Beneficiar:	AUTORITATEA ADMINISTRATIVĂ "AGENȚIA NAȚIONALĂ TRANSPORT AUTO"
Proiect:	*"Cartele tahografice personalizate"*
Ofertant:	CERTSIGN S.A.

Specificaţii tehnice (F4.1)

Numărul licitaţiei:	**21031779 (nr. achizitie comerciala conform platformei achizitii.md) / Anunt participare nr. ANTA: 02/1-1-10804 din 02.12.2020**	Data: **30.12.2020**	Alternativa nr.: **Neaplicabil**
Denumirea licitaţiei:	**Licitatie deschisa pentru "Cartele tahografice personalizate" – cod CPV 30162000-2**	Lot: **Nu este cazul**	Pagina: **_1_din _2_**

Cod CPV	Denumirea bunurilor şi/sau a serviciilor	Modelul articolului	Ţara de origine	Produ-cătorul	Specificarea tehnică deplină solicitată de către autoritatea contractantă	Specificarea tehnică deplină propusă de către ofertant	Standarde de referinţă
1	2	3	4	5	6	7	8
30162000-2	***Cartele tahografice personalizate***	***Cartele tahograf personalizate de următoarele tipuri:*** ▪ *Carduri de conducător auto* ▪ *Carduri de companie* ▪ *Carduri de atelier* ▪ *Carduri de control*	***România***	CERTSIGN S.A.	- ***Tipuri de carduri:*** ***Carduri de conducător auto*** ***Carduri de companie*** ***Carduri de atelier*** ***Carduri de control*** - ***Materialul cardurilor: Policarbonat, pentru a asigura durata de viață de minimum 5 ani în condițiile de utilizare dificile din vehiculele de transport marfă și pasageri, unde pot atinge temperaturi de funcționare de pînă la 80 C*** - ***Dimensiunile: Conforme standardului ISO/IEC 7810:*** ***Lățime: 85,5 mm (ISO 7810, 85,47 – 85,72 mm)*** ***Lungime: 54,0 mm (ISO 7810, 53,92 – 54,03 mm)*** ***Grosime: 0,81 mm (ISO 7810, 0,68 – 0,84 mm)*** - ***Cipurile implementează cerințele formulate în Acordul***	- *Tipuri de carduri:* ▪ *Carduri de conducător auto* ▪ *Carduri de companie* ▪ *Carduri de atelier* ▪ *Carduri de control* - *Materialul cardurilor: Policarbonat, pentru a asigura durata de viață de minimum 5 ani în condițiile de utilizare dificile din vehiculele de transport marfă și pasageri, unde pot atinge temperaturi de funcționare de pînă la 80C*	***ISO/IEC 7810***

S.C. CERTSIGN S.A. certSIGN BUCUREȘTI - ROMÂNIA 2/8

					AETR, Appendix 1B și Commission Regulations No. 1360/2002, Annex 1B - ***Tehnologia de personalizare a cardurilor: Gravare laser, pentru a asigura securitatea cardurilor și durata de viață de minimum 5 ani)***	- *Dimensiunile: Conforme standardului ISO/IEC 7810:* ▪ *Lățime: 85,5 mm (ISO 7810, 85,47 – 85,72 mm)* ▪ *Lungime: 54,0 mm (ISO 7810, 53,92 – 54,03 mm)* ▪ *Grosime: 0,81 mm (ISO 7810, 0,68 – 0,84 mm)* - *Cipurile implementează cerințele formulate în Acordul AETR, Appendix 1B și Commission Regulations No. 1360/2002, Annex 1B* - *Tehnologia de personalizare a cardurilor: Gravare laser, pentru a asigura securitatea cardurilor și durata de viață de minimum 5 ani* *Pentru detalii suplimentare a se vedea capitolele 2.1 Conținutul Ofertei, 2.2 cartele Tahografice ale ofertei tehnice (Specificații Tehnice), și*	

S.C. CERTSIGN S.A. certSIGN BUCUREȘTI - ROMÂNIA

						Anexa 1: Descrierea Tehnică a Cartelelor Tahografice oferite pentru Sistemul Tahograf Digital al Republicii Moldova	
	TOTAL				-	7000 bucați cartele Tahograf personalizate cu respectarea specificațiilor de mai sus	

Semnat:_____ Numele, Prenumele: **Armand-Dragos ROPOT** În calitate de: **Reprezentant imputernicit**

Ofertantul: **CERTSIGN S.A.** Adresa: **Sos. Oltenitei nr. 107A, Cladirea C1, Etaj 1, Camera 16, Sector 4, cod postal 041303, Mun. Bucuresti, Romania**

PROPUNEREA TEHNICĂ

Cuprins

1 Prezentarea ofertantului CERTSIGN S.A.

Prezenta ofertă este depusă de către compania CERTSIGN S.A. din Romania.

CERTSIGN S.A. este producatoarea soluției utilizate în prezent de către ANTA pentru emiterea de cartele tahograf în Republica Moldova. Produsele „persoSAFE" și „tachoSAFE" cu componentele tachoSAFE CIA, tachoSAFE TACHOnet si tachoSAFE CA, sunt dezvoltate de CERTSIGN S.A., fapt demonstrat prin *Certificatul de înregistrare în Registrul Național al Programelor pentru Calculator* emis de către Oficiul Român pentru Drepturile de Autor, ORDA, anexat prezentei oferte.

Prin prezenta ofertă propunem punerea la dispoziția ANTA, întreținerea și actualizarea actualei soluții folosite și în prezent de către ANTA, cu respectarea în totalitate cerințele din documentația de atribuire.

Solutia propusă în prezenta ofertă a fost testată în producție de către beneficiar și și-a dovedit funcționalitatea și fiabilitatea pe parcursul a mai mult de 10 ani. CERTSIGN S.A. a implementat toate cerințele formulate de către ANTA în această perioadă, și în acest moment soluția de furnizare a serviciilor de emitere a cartelelor tahografice personalizate pentru Republica Moldova este o soluție completă, stabilă și customizată comform tuturor cerințelor ANTA.

Această soluție cât și cartelelor tahografice personalizate propuse prin prezenta ofertă respectă în totalitate cerințele din documentația de atribuire și din răspunsurile la întrebările de clarificare.

1.1 CERTSIGN S.A.

CERTSIGN S.A. este o companie care activează în domeniul securității informatice din anul 2006.

CERTSIGN este o firmă certificată conform urmatoarelor standarde:

- **ISO 9001** - Sistemul Managementul al Calității pentru activități în domeniul IT, inclusiv pentru sistemul de personalizare carduri tahograf digital. Certificatul este atașat prezentei oferte;
- **ISO:27001** - Sistemul de Management al Securității Informației, ISMS, inclusiv pentru sistemul de personalizare carduri tahograf digital - cea mai înaltă certificare a Sistemelor de Management al Securității Informatiilor. Certificatul este atașat prezentei oferte;
- **ISO 14001** – pentru Sistemul de Management al Mediului, inclusiv pentru sistemul de personalizare carduri tahograf digital. Certificatul este atașat prezentei oferte;
- **ISO 20000** – managementul Serviciilor IT, inclusiv pentru sistemul de personalizare carduri tahograf digital. Certificatul este atașat prezentei oferte;
- **ISO 18001** – pentru Securitatea si Sanatatea Muncii. Certificatul este atașat prezentei oferte.

- **ISO 37001** - pentru Sistemul de Management Anticoruptie.

Din anul 2006 CERTSIGN este implicată în domeniul sistemului tahografului digital și a dezvoltat propriile soluții pentru sistemul tahografului digital, incluzând:

- Sistemul de înregistrare al aplicanților, emitere și management al cartelelor tahografice pe durata lor de viață, sistem utilizat de autoritatea de emitere cartele tahografice, **CIA** (Card Issuing Authority). Pentru implementarea sistemelor CIA este folosită componenta **tachoSAFE CIA** a produsului software tachoSAFE dezvoltat de CERTSIGN.
- Pachetul de aplicații **tachoSAFE TACHOnet**, componentă a produsului software tachoSAFE dezvoltat de CERTSIGN, folosit pentru conectarea bazei de date a sistemului CIA la bazele de date similare ale celorlalte state Europene și AETR și integrarea în sistemul TACHOnet European, utilizând ca infrastructură de comunicație rețeaua privată la nivelul administrațiilor din statele Uniunii Europene, sTESTA;
- Autoritatea de certificare nationala a sistemului tahografului digital, **CA** (Certification Authority). Pentru implementarea sistemelor CA este folosit produsul software **tachoSAFE CA** dezvoltat de CERTSIGN.
- Centrul de Personalizare, **CP**, care implementează platforma de personalizare carduri **persoSAFE** dezvoltată de CERTSIGN, și folosită și pentru personalizarea cartelelor tahografice.

In Martie 2007, CERTSIGN a semnat contractul cu Autoritatea Rutiera Romana pentru implementarea sistemului tahografului digital in Romania si furnizează cartele tahografice personalizate in Romania incepand cu 1 August 2007. CERTSIGN a dezvoltat și implementat intregul sistem, incluzand:

- Implementarea intregii infrastructuri IT&C pentru sistemul de inregistrare al aplicanților și de management al cartelelor tahograf pe durata lor de viață, RO-CIA, sistemul TACHOnet, autoritatea de certificare națională, RO-CA, și centrul de personalizare al CERTSIGN pentru utilizat pentru personalizarea cardurilor tahografice, RO-CP;
- Elaborarea Politicii de Certificare Nationale si aprobarea acestela la nivel European de către ERCA;
- Certificarea celor 4 tipuri de carduri tahografice la nivel European si obtinerea:
  - Certificatului de Securitate
  - Certificatului de Functionalitate
  - Certificatului de Interoperabilitate
  - Type Approval-ul cardurilor tahografice pentru Republica Moldova
- Migrarea sistemului de emitere și gestiune a cardurilor tahograf, inclusiv a cardurilor, la generatia a doua în anul 2019.

În sistemul tahografului digital Românesc în prezent CERTSIGN are rolurile de:

- Furnizor de servicii de certificare corespunzator autoritatii de certificare a tahografului digital, RO-CA;
- Furnizor de servicii de personalizare pentru cardurile tahografice Romanesti, corespunzator RO-CP;
- Furnizează cartelele tahografice personalizate.

De asemenea, in 2007, CERTSIGN a implementat sistemul tahografului digital in Bulgaria. Deoarece sistemul a fost dezvoltat de specialistii nostri, am fost capabili sa-l adaptam foarte rapid cerintelor Bulgaresti (de ex. suportul pentru caractere chirilice pentru aplicatiile BG-CIA si TACHOnet, etc) si, bazandu-ne pe experienta acumulata din implementarea sistemului Romanesc, am implementat sistemul tahografului digital in Bulgaria, am obtinut toate aprobarile si certificarile Europene si am emis primele carduri tahografice Bulgaresti in 2 luni de la data semnarii contractului.

In Iulie 2010 CERTSIGN a finalizat dezvoltarea si implementarea sistemului de emitere a cardurilor pentru tahograful digital din Ucraina și furnizează cardurile pentru tahograful digital personalizate autorităților ucrainiene.

In Decembrie 2010 CERTSIGN a finalizat dezvoltarea si implementarea sistemului de emitere a cardurilor pentru tahograful digital din Republica Moldova și furnizează cardurile pentru tahograful digital personalizate către ANTA.

In Decembrie 2011 CERTSIGN a finalizat dezvoltarea si implementarea sistemului de emitere a cardurilor pentru tahograful digital din Republica Serbia.

In Decembrie 2013 CERTSIGN a finalizat implementarea Sistemului Tahografului Digital al Republicii Uzbekistan și in prezent emite cartelele tahograf personalizate pentru Uzbekistan.

În 2012 CERTSIGN a implementat sistemul autorității de certificare FI-CA pentru sistemul tahograf digital al Finlandei, și de la 1 Ianuarie 2013 CERTSIGN furnizează certificatele digitale pentru personalizarea cartelelor de tahograf digital ale Finlandei.

În 2013 CERTSIGN a implementat sistemul autorității de certificare NO-CA pentru sistemul tahograf digital al Norvegiei, și din 16 noiembrie 2013 CERTSIGN furnizeaza certificatele digitale pentru personalizarea cartelelor de tahograf digital ale Norvegiei.

In Martie 2015 CERTSIGN a implememntat sistemul autoritatii de certificare pentru Kazakhstan, KZ-CA.

In 2018 CERTSIGN a finalizat implementarea Sistemului Tahografului Digital al Republicii Tajikistan și in prezent emite cartelele tahograf personalizate pentru Tajikistan.

În anul 2018 CERTSIGN S.A. a implementat întregul sistem de emitere a cardurilor pentru tahograful digital în Cipru și din Mai 2019 emite carduri smart tahograf pentru Cipru.

În anul 2018 CERTSIGN S.A. a implementat sistemul autorității de certificare și sistemul de management de chei pentru sistemul de personalizare a cardurilor tahograf digital de generatia a 2-a pentru FNMT-RCM din Spania.

În anul 2019 CERTSIGN S.A. a implementat sistemul autorității de certificare, PT-CA, și sistemul de personalizare al cardurilor tahograf digital de generatia a 2-a, PT-CP, pentru INCM din Portugalia.

În anul 2018 CERTSIGN S.A. a implementat sistemul autorității de certificare de generatia a doua, NL-CA, pentru emiterea cardurilor smart tahograf în Olanda.

În anul 2018 CERTSIGN S.A. a implementat sistemul autorității de certificare de generatia a doua, UK-CA, pentru emiterea cardurilor smart tahograf în Marea Britanie.

În 2019 CERTSIGN a implementat sistemul autorității de certificare B-CA pentru sistemul tahograf digital al Belgiei, și din 2019 CERTSIGN furnizeaza certificatele digitale pentru personalizarea cartelelor de tahograf digital ale Belgiei.

În 2019 CERTSIGN a implementat sistemul autorității de certificare IR-CA pentru sistemul tahograf digital al Irlandei, și din 2019 CERTSIGN furnizeaza certificatele digitale pentru personalizarea cartelelor de tahograf digital ale Irlandei.

În 2019 CERTSIGN a implementat sistemul autorității de certificare DK-CA pentru sistemul tahograf digital al Danemarcei, și din 2019 CERTSIGN furnizeaza certificatele digitale pentru personalizarea cartelelor de tahograf digital ale Danemarcei.

Toate sistemele tahograf digital implementate in Romania, Moldova, Ucraina, Cipru, Uzbekistan, Tajikistan, Finlanda, Norvegia, Belgia, Irlanda, Danemarca sunt sisteme bazate pe servicii, inclusiv servicii de tiparire si personalizare cartele tahograf, furnizate de CERTSIGN.

Compania CERTSIGN este recunoscuta la nivel international ca un furnizor de top de solutii de implementare a sistemelor nationale de tahograf digital. Specialistii CERTSIGN au participat in calitate de experti internationali CORTE la multe workshop-uri internationale dedicate implementarii sistemelor de emitere a cardurilor tahografice (de ex. in Ankara, Tbilisi, Almata, Bucuresti, etc).

Începând din 2009 CERTSIGN furnizează către Autoritatea Rutieră Română cardurile certificat de pregătire profesională pentru conducătorii auto profesioniști, carduri personalizate folosind echipamentele de personalizare din centrul de personalizare al CERTSIGN.

Din anul 2009 CERTSIGN furnizează către Autoritatea Rutieră Română cardurile certificat ADR, carduri personalizate folosind acelasi centru de personalizare al CERTSIGN.

Din anul 2015 CERTSIGN furnizează către Road Trandport Department din Cipru cardurile permis de conducere, carduri personalizate folosind acelasi centru de personalizare al CERTSIGN.

1.2 Avantajele CERTSIGN S.A.

CERTSIGN S.A. ofera avantaje incontestabile in comparatie cu orice alti ofertanti in furnizarea serviciilor de tiparire si personalizare a cartelelor tahografice. Dintre aceste avantaje amintim:

- CERTSIGN a derulat începand cu anul 2010 şi derulează în continuare cu succes contracte în cooperare cu Ministerul Transporturilor şi Infrastructurii Drumurilor şi Autoritatea administrativă „Agenţia Naţională Transport Auto" din Republica Moldova pentru furnizarea de cartele tahografice personalizate;
- Fiabilitatea si functionalitatea soluţiei noastre este dovedita cel mai bine de indeplinirea obligaţiilor contractuale pe parcursul a mai mult de 10 ani in care au fost furnizate aproximativ 30.000 cartele tahografice personalizate în Republica Moldova, în deplina concordanta cu cerintele AETR şi ale reglementarilor Europene in domeniu cat si cu cerintele beneficiarului. Pe parcursul derularii acestor contracte nu a fost inregistrat nici un incident.
- Pe parcursul celor 10 ani în care CERTSIGN S.A. furnizeaza cartelele togograf personalizate pentru Republica Moldova s-a dovedit ca acestea au

cea mai inalta calitate si fiabilitate raportate la nivelul intregului sistem tahograf digital European. Astfel, rata de cartele defecte returnate la nivelul Republicii Moldova este sub 0,4% fata de media Europeana de 5%. Acest nivel inalt de calitate si fiabilitate este oferit și in continuare de catre CERTSIGN, prin prezenta oferta, prin furnizarea de carduri fabricate de acelasi furnizor și personalizate folosind acelasi sistem utilizat și in prezent.

- Solutia propusa de catre CERTSIGN S.A. a fost testata in productie timp de 10 ani, perioada in care au fost implementate toate cerintele autoritatii contractante si au fost corectate toate problemele aparute, deci este o solutie perfect adaptată nevoilor ANTA. Din acest punct de vedere, solutia propusa de CERTSIGN nu prezinta nici un risc pentru autoritatea contractanta. În plus, personalul ANTA cunoaste foarte bine solutia si nu mai are nevoie de o perioada de training si adaptare la o noua solutie.
- Din punctul de vedere al asigurarii continuitatii emiterii de cartele tahografice personalizate, CERTSIGN este unicul ofertant care va putea și va emite prima cartela tahografica personalizata din prima zi a semnarii contractului. Orice alt ofertant, deoarece va trebui sa implementeze un nou sistem, va avea nevoie de o perioadă timp de la semnarea contractului până va putea furniza primele cartele tahografice personalizate certificate la nivel international;
- CERTSIGN este producatorul solutiei propuse, solutie implementata, actualizată si utilizata pe parcursul ultimilor 10 ani pentru furnizarea de cartele tahografice personalizate către Autoritatea Administrativă „Agenția Națională Transport Auto", soluție utilizată și în momentul de fata in derularea actualului contract de furnizare de cartele tahografice personalizare în Republica Moldova. Astfel, putem asigura foarte usor actualizarea solutiei și implementarea tuturor noilor cerinte care pot apare pe plan international si national in domeniul tahografului digital;
- CERTSIGN este membru CORTE si participa activ la evolutia proiectului Tahograf la nivel European si AETR. Specialistii CERTSIGN au participat in calitate de experti internationali CORTE la multe workshop-uri internationale dedicate implementarii sistemelor de emitere a cartelelor tahografice (de ex. in Ankara, Tbilisi, Almata, Bucuresti, Brussels, etc);
- Compania CERTSIGN este recunoscuta la nivel international ca un furnizor de top de solutii de implementare a sistemelor nationale de tahograf digital cât și furnizor de servicii de tiparire, personalizare și certificare cartele tahografice. CERTSIGN are la activ 18 implementari de sisteme nationale de emitere a cartelelor tahografice, în Republica Moldova, Romania, Bulgaria, Ucraina, Serbia, Cipru, Marea Britanie, Finlanda, Norvegia, Olanda, Danemarca, Belgia, Irlanda, Spania, Portugalia, Uzbekistan, Kazakhstan si Tajikistan.

2 Oferta Tehnică

2.1 Conținutul Ofertei

Prin prezenta ofertă tehnică CERTSIGN S.A. se angajează să furnizeze cartele tahografice personalizate către Autoritatea administrativă "Agenția Națională Transport Auto", în continuare ANTA, în deplină conformitate cu toate cerințele din documentația de atribuire cât și cu respectarea normelor și reglementărilor naționale, AETR și ale Uniunii Europene în domeniul tahografului digital, fără întrerupere pe durata contractului, începând din prima zi din care va intra în vigoare contractul.

Prezenta ofertă răspunde în totalitate cerințelor ANTA, inclusiv:

- Cerințelor din Anunțul de participare, și
- Cerințelor din Documentația standard pentru realizarea achizițiilor publice de bunuri cu obiectul achiziției Cartele tahografice personalizate.

Oferta de furnizarea de cartele tahografice personalizate a CERTSIGN include:

- Personalizarea și livrarea cartelelor tahografice conforme reglementarilor AETR si ale Comisiei Europene in vigoare pe toată durata contractului. Detaliile tehnice privind cardurile furnizate se găsesc în capitolul *2.3 Cartele Tahografice* cât și în *Anexa 1: Descrierea Tehnică a Cartelelor Tahografice oferite pentru Sistemul Tahograf Digital al Republicii Moldova* ale prezentei oferte;
- Punerea la dispoziția Autorității Contractante pe întreaga durată a contractului a infrastructurii hardware și software necesară funcționării sistemului tahograf digital la nivel național, pentru emiterea și gestiunea de carduri tahografice în Republica Moldova;
- Operarea întregii infrastructuri hardware și software a sistemului pentru emiterea și gestiunea de carduri tahografice, cu excepția infrastructurii aferente birourilor de înregistrare a solicitărilor de carduri tahografice, care va fi operată de către personalul Autorității administrative "Agenția Națională Transport Auto", cu suportul tehnic oferit de către CERTSIGN.
- Întreținerea și actualizarea tuturor componentelor infrastructurii sistemului pentru emiterea și gestiunea de carduri tahografice pentru a respecta în totalitate cerințele specificate în caietul de sarcini cât și noile cerințe elaborate la nivelul AETR și al Uniunii Europene în acest domeniu. De asemenea, vor fi implementate noile funcționalități cerute de către ANTA pe durata contractului;
- Trainingul și suportul tehnic de la producător, în limba Română, pentru operarea aplicației ANTA la nivelul birourilor de înregistrare cât și pentru întreaga solutie oferită corespunzatoare MD-CIA si pentru toate upgrade-urile efectuate asupra acestela.

CERTSIGN propune prin prezenta ofertă punerea la dispoziția ANTA în vederea utilizării în continuare a sistemului deja implementat și utilizat în prezent cu succes de ANTA pentru emiterea cartelelor tahograf pe teritoriul Republicii Moldova. CERTSIGN, în calitate de producător și implementator al sistemului, va asigura mentenanta, supurtul tehnic, actualizarea și trainingul pentru toate componentele acestui sistem comform cerințelor din prezenta documentatie de atribuire.

Soluția propusă asigură emiterea fără întreruperi a cartelelor tahografice încă din prima zi a intrării în vigoare a contractului cu respectarea în totalitate atât a prevederile naționale cât și a prevederilor internaționale in domeniu, și în special:

- Acordul AETR, Appendix 1B
- Reglementarea (EC) 3821/85;
- Reglementarea (EC) 2135/98;
- Commision Regulation No. 1360/2002, Annex IB;
- Reglementarea (EU) 165/2014;
- Politica de securitate *„National Authority Policy of Republic of Moldova for the Digital Tachograph System"*, aprobata de ERCA;
- Digital Tachograph System European Root Policy Version 2.1.

Prin soluția propusă în prezenta ofertă CERTSIGN S.A. asigură realizarea integrală a obiectivelor autorității contractante, și anume continuitatea procesului de emitere de carduri personalizate pentru tahograful digital în Republica Moldova pentru conducătorii auto, companii, ateliere și organele de control, astfel încât să nu se perturbe activitățile de transport rutier în Republica Moldova și să nu se producă daune companiilor de transport și conducătorilor auto care efectuează transport internațional. CERTSIGN va asigura continuitatea functionarii sistemului de emitere si gestiunea a cartelelor tahografice, cât și emiterea fără intreruperi pe toată durata contractului, începând cu prima zi de la intrarea în vigoare a acestuia, a cartelelor tahografice.

Asigurarea continuității este realizată prin:

- utilizarea acelulasi sistem folosit și in prezent pentru emiterea de cartele tahografice, sistem implementat tot de catre CERTSIGN in anul 2010;
- furnizarea acelorasi tipuri de cartele tahografice furnizate și in prezent, cartele care respecta in totalitate reglementările AETR și ale Uniunii Europene în domeniu, cât și cu cerințele din prezentul caiet de sarcini, fapt demonstrat prin certificările și Type Approval-ul obtinute și anexate prezentei oferte.

Prin punerea la dispoziția ANTA în vederea utilizării pe durata contractului a sistemului folosit și in prezent cât și furnizarea acelorași cartele tahograf, deja certificate, se asigură:

- emiterea primelor carduri personalizate, în conformitate cu toate reglementările AETR și ale Uniunii Europene în domeniu, cât și cu cerințele

din prezentul caiet de sarcini, în termen de **maxim 1 zi** de la data intrării în vigoare a contractului;

- gestiunea tuturor cardurilor tahograf emise în Republica Moldova începînd cu luna Decembrie 2010 şi pană în prezent, cât şi a cardurilor care urmează să fie emise pe durata contractului. Cardurile emise începand cu luna Decembrie 2010 se regasesc deja in baza de date a sistemului, fiind vorba de acelaşi sistem, cu aceeaşi bază de date;
- continuitatea schimbului de informatii cu autoritatile nationale din celelalte state participante in sistemul tahografului digital, prin intermediul serviciului TACHOnet, începând cu data intrării în vigoare a contractului, moment in care vor putea fi livrate si primele cartele tahografice personalizate.
- emiterea neîntreruptă de cartele tahografice personalizate pe toată durata contractului, conform comenzilor transmise de către ANTA, sistemul fiind deja cunoscut şi rodat de catre ANTA prin utilizarea zilnică a acestuia în ultimii 10 ani.

Cardurile tahografice furnizate pe toată durata contractului sunt certificate la nivel European, au acelaşi design ca actualele cartele tahografice emise în Republica Moldova şi sunt conforme specificaţiilor tehnice aprobate pentru Republica Moldova.

Cardurile tahografice furnizate sunt fabricate din acelaşi material, şi anume policarbonat, şi vor fi personalizate prin aceeaşi tehnologie, şi anume gravare laser, folosind acelaşi layout de personalizare utilizat la personalizarea actualelor carduri de tahograf digital. Mai multe detalii despre cardurile tahografice furnizate se gasesc în capitolul *2.3 Cartele Tahografice* cât şi in *Anexa 1: Descrierea Tehnică a Cartelelor Tahografice oferite pentru Sistemul Tahograf Digital al Republicii Moldova* ale prezentei oferte.

Vor fi furnizate toate cele patru tipuri de cartele tahograf, şi anume:

- cartele tahografice pentru conducatorii auto;
- cartele tahografice pentru control;
- cartele tahografice pentru companiile de transport;
- cartele tahografice pentru atelierele acreditate.

Pentru a demonstra faptul ca CERTSIGN poate asigura emiterea neîntreruptă în Republica Moldova a cartelelor tahografice personalizate, certificate la nivel European, cu respectarea tuturor cerinţelor, prezentăm atașate acestei oferte:

- Certificatului de Securitate: *BSI-DSZ-CC-0272-2004 for TCOS tachograph card Version 1.0 Release 2*
- Fogra test report 24509 for type of cards PCS-C-ID1-01A/MDA_eTG/TP97172
- Certificatului de Functionalitate: *Functional Certificate for TCOS Tachograph-AETR for Moldova*

- Certificatului de Interoperabilitate: *Interoperability Certificate Nº. JRC_DTC/AC-040/058/MA01/2010*
- Type Approval-ul cardurilor tahografice pentru Republica Moldova: *Bauartgenehmigung Nr. / Approval No.: e1*209*01*
- mostre de cartele tahografice personalizate funcționale pentru fiecare tip de cartelă, si anume:
  - mostră de cartelă de conducător auto
  - mostră de cartelă de companie
  - mostră de cartelă de control
  - mostră de cartelă de agent economic autorizat împreună cu scrisoarea de PIN aferentă

CERTSIGN S.A. poseda o solutie de disaster recovery utilizată și în prezent pentru toate componentele sistemului de emitere cartele tahografice, și anume: MD-CIA, MD-CA si MD-CP. Soluția de disaster recovery oferită poate prelua activitatea oricarei componente a site-ului principal de productie in mai putin de 24 de ore de la producerea catastrofei. Componentele solutiei de disaster recovery sunt localizate în Constanta, la o distanta de peste 200 km fata de locatia principala de producție din Bucuresti.

CERTSIGN oferă aceeași soluție de disaster recovery, pusă și în prezent la dispoziția ANTA, pentru toate componentele sistemului, care poate prelua activitatea oricărei componente a site-ului principal de producție în mai puțin de 24 de ore de la producerea evenimentului. Soluția de disaster recovery va fi operațională pe întreaga perioadă de derulare a contractului.

CERTSIGN va implementa și opera toate componentele sistemului pus la dispoziția ANTA, respectiv MD-CIA, MP_CA și MD-CP, cu respectarea strictă a tuturor cerințelor de Securitate specificate în politica de securitate *National Authority Policy of Republic of Moldova for the Digital Tachograph System*.

Toate sistemele puse la dispoziția ANTA pe durata contractului vor fi protejate de o infrastructură completă de securitate care asigură respectarea tuturor cerințelor stipulate în:

- politica de securitate *„National Authority Policy of Republic of Moldova for the Digital Tachograph"*, aprobata de ERCA
- politica de securitate a ERCA, *Digital Tachograph System European Root Policy Version 2.1*
- Acordul AETR, appendix IB.

CERTSIGN asigură securitatea complete a soluției propuse, care include:

- securitatea fizică a locațiilor centrelor de date care gazduiesc echipamantele sistemului oferit și a locațiilor de producție în care are loc personalizarea cardurilor
- securitatea tuturor aplicațiilor software ale sistemului, fiind folosite mecanisme puternice de autentificare bazate pe chei criptografice si certificate digitale stocate pe dispositive criptografice hardware și

asigurându-se autenticitatea, integritatea, confidențialitatea datelor vehiculate în sistem,
- securitatea de rețea și comunicații, și
- securitate cibernetica a acestor sisteme ținând cont de noile amenințări cibernetice.

Infrastructura de securitate a CERTSIGN care protejează componentele sistemului autorității de certificare ANTA, MD-CA, include o incintă securizată în interiorul căreia sunt instalate toate serverele și componentele hardware ale sistemului și care este utilizată pentru emiterea certificatelor digitale, semnare, criptare și manipulare chei criptografice, în vederea protecției acestora. Această incintă securizată îndeplinește următoarele cerințe:
- este incinta ecranata, cu o atenuare de minim 55dB in gama 1MHz-1GHz. Atașat prezentei oferte este prezentat raportul de încercări emis de către Laboratorul de Încercări de Joasă și Inaltă Tensiune, conform standardului IEEE STD 299: 2007;
- dispune de sistem de supraveghere video CCTV;
- dispune de sistem de detecție și avertizare în caz de incendiu;
- dispune de sistem de climatizare, în vederea asigurării condițiilor optime de funcționare a echipamentelor;
- dispune de sistem de control acces.

Mai multe detalii despre securitatea soluției și a componentelor care vor fi puse la dispoziția ANTA pot fi gasite în capitolele:
- 2.4.2.4 Securitatea sistemului MD-CIA
- 2.4.3.7 Securitatea sistemului MD-CP
- 2.4.4.4 Securitatea sistemului MD-CA

Mentionam ca CERTSIGN este certificată conform standardului ISO 27001 privind managementul securității informației pentru sistemul de personalizare carduri tahograf digital.

CERTSIGN, în calitate de furnizor de servicii de personalizare de cartele tahografice, a implementat și operează sistemul MD-CP conform codului de practici și proceduri: *„Sistemul de Tahograf Digitale pentru Republica Moldova, Codul de Practici si Proceduri pentru operarea MD-CP"*. Acest cod de practici și proceduri va fi respectat și în continuare, pe toată durata contractului. Documentul *„Sistemul de Tahograf Digitale pentru Republica Moldova, Codul de Practici si Proceduri pentru operarea MD-CP"* este anexat prezentei oferte.

CERTSIGN, în calitate de furnizor de servicii de certificare pentru cartelele tahografice, a implementat și operează sistemul MD-CA conform codului de practici și proceduri: *„Sistemul de Tahograf Digital pentru Republica Moldova, Codul de Practici și Proceduri pentru Implementarea Politicii de Certificare a MD-CA si operarea MD-CA"*. Acest cod de practici și proceduri va fi respectat și în continuare, pe toată durata contractului. Documentul *„Sistemul de Tahograf Digital pentru Republica Moldova, Codul de Practici și Proceduri pentru*

implementarea Politicii de Certificare a MD-CA si operarea MD-CA" este anexat prezentei oferte.

CERTSIGN S.A. va pune la dispoziția autoritatii contractante, pe durata contractului, sistemul de înregistrare, gestiune și emitere de carduri tahograf, tachoSAFE CIA, numită în continuare MD-CIA, inclusiv componanta tachoSAFE TACHOnet a acestuia. CERTSIGN este producătorul acestui sistem, sistem utilizat și în prezent de către ANTA. Echipa de dezvoltare a CERTSIGN va asigura pe durata contractului actualizarea aplicațiilor tachoSAFE CIA si tachoSAFE TACHOnet, iar echipa tehnică va asigura mentenanta și suportul tehnic, în limba Romana, pentru aceste aplicații.

CERTSIGN S.A., in calitate de producatoare a sistemului tachoSAFE, este în masură să asigure și va asigura pe durata contractului upgrade-ul aplicațiilor software ale sistemului pus la dispoziția ANTA comform noilor cerințe care vor fi elaborate la nivel European, AETR și național, cît și a cerințelor Autorității Contractante, fără întreruperea activității de înregistrare și furnizare a cartelelor tahografice de către ANTA și fără costuri suplimentare. Pentru a demonstra calitatea de producător al sistemului pus la dispoziția ANTA și capabilitatea de a asigura upgrade-ul aplicațiilor software ale sistemului, atașăm prezentei oferte Certificatul emis de către Registrul Național al Programelor pentru Calculator corespunzător aplicațiilor tachoSAFE.

CERTSIGN S.A., in calitate de producatoare a sistemului tachoSAFE pus la dispoziția ANTA, inclusiv a aplicatiilor tachoSAFE MD-CIA, este în măsură să asigure și va asigura pe durata contractului mentenanța și suportul tehnic, în limba Română, al sistemului pentru înregistrarea de cereri carduri tahograf digital, emitere carduri și gestiune a cardurilor emise de către ANTA. Pentru a demonstra calitatea de producător al sistemului pus la dispoziția ANTA și capabilitatea de a asigura mentenanța și suportul tehnic de la producător pentru sistem, atașăm prezentei oferte Certificatul emis de către Registrul Național al Programelor pentru Calculator corespunzător aplicațiilor tachoSAFE.

CERTSIGN S.A. va asigura pe durata contractului infrastructura tehnică necesară conectării sistemului gestionat de ANTA la sistemul European TACHOnet prin punctul de acces al unui stat membru UE, respectiv România, la rețeaua privată a Uniunii Europene, sTESTA. Conectarea este deja realizată și ANTA are deja acces la sistemul European TACHOnet prin punctul de acces la rețeaua sTESTA al României folosind sistemul pus la dispoziție de CERTSIGN. CERTSIGN va pune la dispoziția ANTA, pe durata contractului, aceeasi infrastructura tehnică pentru conectarea la TACHOnet.

CERTSIGN S.A., in calitate de producatoar al sistemului tachoSAFE TACHOnet, va asigura pe durata contractului upgrade-ul aplicațiilor software pentru verificarea și validarea cererilor aplicanților la nivel european, prin interfațarea cu sistemul TACHOnet, conform noilor specificații și cerințe care vor fi elaborate la

nivel European. Pentru a demonstra calitatea de producător al sistemului pus la dispoziția ANTA și capabilitatea de a asigura upgrade-ul aplicațiilor software ale sistemului TACHOnet național, atașăm prezentei oferte Certificatul emis de către Registrul Național al Programelor pentru Calculator corespunzător aplicațiilor tachoSAFE.

CERTSIGN S.A., în calitate de producatoar al sistemului tachoSAFE TACHOnet, va asigura pe durata contractului mentenanța și suportul tehnic, în limba Română, al aplicațiilor software pentru verificarea și validarea cererilor aplicanților la nivel european, prin interfațarea cu sistemul TACHOnet. Pentru a demonstra calitatea de producător al sistemului pus la dispoziția ANTA și capabilitatea de a asigura mentenanța și suportul tehnic de la producător al acestor aplicații software, atașăm prezentei oferte Certificatul emis de către Registrul Național al Programelor pentru Calculator corespunzător aplicațiilor tachoSAFE.

CERTSIGN S.A. va pune la dispoziția autoritatii contractante și va opera, pe durata contractului, sistemul Autorității de Certificare, tachoSAFE CA, numit în continuare și MD-CA. CERTSIGN este producătorul acestui sistem, sistem utilizat și în prezent de către ANTA. Echipa de dezvoltare a CERTSIGN va asigura pe durata contractului actualizarea aplicațiilor tachoSAFE CA, iar echipa tehnică va asigura mentenanta și suportul tehnic, în limba Romana, pentru aceste aplicații.

Deoarece în perioada de derulare a Acordului cadru (2017-2021) la nivelul Uniunii Europene va fi introdusă noua generație de tahografe digitale și noua generație de carduri pentru tahograful digital care vor include noi mecanisme criptografice și o structură modificată a sistemului de fișiere, CERTSIGN va upgrada sistemul pentru emiterea de carduri tahograf pentru republica Moldova și va realiza tranziția la noua generație de carduri tahografice, fără a depăși termenele impuse de Acordul AETR și Reglementările Europene în acest sens.

Pentru a realiza tranziția la noua generație de carduri tahografice, CERTSIGN va:

- dezvolta cardurile tahografice de generația a doua pentru Republica Moldova și va obține și prezinta Autorității Contractante Type Approval-ul pentru aceste carduri în termenele impuse de Acordul AETR și Reglementările Europene.
- actualiza sistemul actualei autorități de certificare, MD-CA a ANTA, pentru a implementa noile mecanisme criptografice stabilite pentru sistemul tahograf digital, și a asigura compatibilitatea cu actualele tahografe digitale și carduri tahograf pe perioada de tranziție în care ambele mecanisme criptografice vor fi folosite;
- actualiza sistemul centrului de personalizare, MD-CP, pentru personalizarea cardurilor tahografice de generatia a doua;
- actualiza politica de securitate *National Authority Policy of Republic of Moldova for the Digital Tachograph System* conform noilor cerințe impuse de tranziția la generația a doua a tahografului digital și conform noii Politici

de Securitate a ERCA care va fi emisă pentru generația a doua a sistemului tahograf digital.

CERTSIGN S.A., in calitate de producatoare a actualului sistem tachoSAFE CA, este în masură să asigure și va asigura actualizarea, pe durata contractului, a aplicatiilor software ale autoritatii de certificare MD-CA conform noilor cerinte care vor fi elaborate la nivel elaborate la nivel European și AETR în această perioadă. Implementarea noilor cerințe în sistemul ANTA se va realiza cu respectarea strictă a termenelor impuse de AETR și reglementările Europene în acest sens, fără întreruperea activității de furnizare a cardurilor tahografice și fără costuri suplimentare pentru Autoritatea Contractantă.

Pentru a demonstra calitatea de producător al sistemului tachoSAFE CA pus la dispoziția ANTA și capabilitatea de a asigura actualizarea aplicațiilor software ale autorității de certificare ANTA, atașăm prezentei oferte Certificatul emis de către Registrul Național al Programelor pentru Calculator corespunzător aplicațiilor tachoSAFE.

CERTSIGN S.A., in calitate de producatoare a solutiei propuse, va asigura suport tehnic pentru aplicatiile MD-CIA, TACHOnet și MD-CA printr-un serviciu de help-desk in limba Romana 24 de ore din 24, 7 zile pe saptamana, 365 zile pe an si interventie on-site in timpul programului de lucru, fara nici o limitare in numarul de interventii.

CERTSIGN oferă ANTA dreptul de utilizare a aplicatiilor software ale MD-CIA, TACHOnet si MD-CA, inclusiv asupra tuturor actualizarilor aplicatiilor MD-CIA, TACHOnet si MD-CA realizate, pe durata contractului, pentru a-si putea indeplini sarcinile de inregistrare, emitere si management al cartelelor tahografice.

2.2 Cartele Tahografice

2.2.1 Introducere

CERTSIGN va furniza următoarele tipuri de carduri tahografice:

- Carduri de conducător auto
- Carduri de companie
- Carduri de atelier
- Carduri de control

Cardurile tahografice oferite sunt identice cu cardurile furnizate și in prezent de catre CERTSIGN. Cardurile sunt produse de catre Trüb AG din Elveția, in prezent o companie Gemalto, sunt conforme cu toate cerintele AETR, Appendix 1B si

Commission Regulations No. 1360/2002, Annex 1B şi cu toate cerintele din anuntul de participare si documentatia fde atribuire, cu specificaţiile tehnice *Design & Layout Personalizare Cartele Tahografice* si au obtinut toate certificarile necesare la nivel european si anume:

- certificatele de securitate pentru cipuri si softul cipurilor cartelelor oferite,
- certificatul de functionalitate,
- certificatul de interoperabilitate,
- type approval-ul bazat pe aceste certificate.

În vederea implementarii cerintei de a asigura continuitatea emiterii de cartele tahografice de catre ANTA si asigurarea continuitatii functionarii sistemului de emitere si gestiune a cartelelor tahografice in Republica Moldova, CERTSIGN va asigura un stoc de cartele nepersonalizate şi toate consumabilele necesare care să acopere necesarul pentru cel puţin 2 luni de producţie.

Având în vedere faptul că specificaţiile cartelelor tahograf au fost modificate de către Uniunea Europeana şi urmează ca modificarile respective să fie implementate şi la nivelul AETR, CERTSIGN va asigura tranziţia la noua generaţie de cartele tahografice conform graficului de implementare ataşat, fără a depăşi termenele care vor fi impuse de reglementarile AETR şi cele europene in acest sens. Pentru noua generaţie de carduri tahografice CERTSIGN va obtine in acest termen toate certificatele necesare, şi anume certificatul de securitate, certificatul de funcţionalitate şi certificatul de interoperabilitate, şi pe baza acestora va obţine Type Approval-ul pe care îl va prezenta ANTA.

Pe lângă elementele tehnice prezenate în continuare, mai multe detalii despre cardurile tahograf furnizate de CERTSIGN pot fi gasite în documentul *Anexa 1 – Descrierea Tehnică a Cartelelor Tahografice oferite pentru Sistemul Tahograf Digital al Republicii Moldova* ataşat prezentei oferte.

2.2.2 Tipuri de carduri

CERTSIGN va furniza următoarele tipuri de carduri tahografice:

- Carduri de conducător auto
- Carduri de companie
- Carduri de atelier
- Carduri de control

2.2.3 Materialul cartelelor

Pentru a asigura durata de viaţă de minimum 5 ani în condiţiile de utilizare dificile din vehiculele de transport marfă şi pasageri, unde pot atinge temperaturi de funcţionare de pînă la 80 C, cartelele furnizate sunt fabricate din policarbonat.

Policarbonatul are calitaţi superioare multor materiale sintetice oferind o înaltă rezistenţă mecanică, chimică şi termică. Este insensibil la influeţele mediului înconjurător; atât datele ştiinţifice cât şi experienţa practica indica un timp de viaţă de aproximativ 7-10 ani.

Catelele furnizate sunt realizate din mai multe straturi de material policarbonat şi sunt apoi laminate în conditii speciale de presiune si temperatură fără a folosi adezivi. Această tehnologie reduce riscul desfacerii cartelelor în scopul falsificării oricărei componente din cartelă.

2.2.4 Dimensiunea cartelelor

Dimensiunile cartelelor tahografice furnizate sunt conforme standardului ISO/IEC 7810, şi anume:

- Lăţime: 85,5 mm (ISO 7810, 85,47 – 85,72 mm)
- Lungime: 54,0 mm (ISO 7810, 53,92 – 54,03 mm)
- Grosime: 0,81 mm (ISO 7810, 0,68 – 0,84 mm)

2.2.5 Cipurile cartelelor

Cip-urile cartelelor tahografice furnizate implementează cerinţele formulate în Acordul AETR, Appendix 1B şi Commission Regulations No. 1360/2002, Annex 1B. Acest fapt este dovedit de certificările obţinute pentru cele 4 tipuri de carduri tahografice la nivel European, atașate prezentei oferte, si anume:

- Certificatului de Securitate
- Certificatului de Functionalitate
- Certificatului de Interoperabilitate
- Type Approval-ul cardurilor tahografice pentru Republica Moldova

2.2.6 Tehnologia de personalizare

Pentru a asigura un nivel înalt de securitate poza, semnatura si celelalte date variabile corespunzatoare fiecarui posesor de card tahograf vor fi personalizate prin gravare laser. În plus, anumite câmpuri vor fi personalizate cu caractere tactile.

Descrierea layout-ului de personalizare a fiecărula din cele 4 tipuri de carduri tahograf furnizate este prezentat în documentul *Anexa 1 – Descrierea Tehnică a Cartelelor Tahografice oferite pentru Sistemul Tahograf Digital al Republicii Moldova* atașat prezentei oferte.

2.2.7 Descrierea grafică

Descrierea grafică a cartelelor tahografice oferite şi elementele de securitate incluse sunt prezentate, pentru fiecare tip de cartelă, în *Anexa 1: Descrierea*

Tehnică a Cartelelor Tahografice oferite pentru Sistemul Tahograf Digital al Republicii Moldova ataşat prezentei oferte. Designul cartelelor tahograf şi elementele de securitate implementate sunt in concordanţă cu specificaţiile AETR şi cu directivele UE, cât şi cu cerinţele beneficiarului, fiind aprobat de catre laboratoarele specializate din uniunea Europeana in cadrul procedurii pentru obtinerea Type Approval-ului.

2.3 Sistemul National de Emitere și Gestiune a Cartelelor Tahografice

Sistemul propus de catre CERTSIGN respecta in totalitate prevederile acordului AETR, prevederile europene in domeniu tahografului digital, si anume reglementarile (EC) 3821/85, (EC) 2135/98, (EC) 1360/2002, (EU) 165/2014 cit si politicile, normele si specificatiile aferente. In acelasi timp sunt respectate toate prevederile legale nationale in domeniu.

Sistemul tahografului digital la nivel national va avea urmatoarele componente:

- **MD-A** = Autoritatea statului responsabila de implementarea reglementarilor AETR in Republica Moldova. Functia MD-A este asigurata de Ministerul Transporturilor și Infrastructurii Drumurilor.
- **MD-CA** = Incepând din 2010, functia MD-CA este asigurata de catre ANTA, care functioneaza conform AETR si a politicii de securitate *„National Authority Policy of Republic of Moldova for the Digital Tachograph System"*, aprobata de ERCA. CERTSIGN este desemnată ca service agency pentru MD-CA și opereaza sistemul autorității de certificare. Autoritatea de certificare propusa de CERTSIGN indeplineste toate conditiile necesare si este declarata oficial ca MSCA in cadrul UE, cheile sale publice fiind certificate de ERCA.
- **MD-CP** = Autoritatea de personalizare a cartelelor tahografice. Incepând din 2010, functia MD-CP este asigurata de catre ANTA, care functioneaza conform AETR si a politicii de securitate *„National Authority Policy of Republic of Moldova for the Digital Tachograph System"*, aprobata de ERCA. CERTSIGN S.A. este desemnată ca service agency pentru MD-CP și opereaza sistemul centrului de personalizare. Centrul de personalizare al CERTSIGN indeplineste toate conditiile necesare si este declarat oficial ca CP in cadrul UE, comform documentului anexat prezentei oferte tehnice.
- **MD-CIA** = Autoritatea de inregistrare si emitere cartele tahografice digitale. Functia MD-CP este asigurata de catre ANTA, care functioneaza conform AETR si a politicii de securitate *„National Authority Policy of Republic of Moldova for the Digital Tachograph System"*. Infrastructura MD-CIA este operata de catre CERTSIGN, cu exceptia birourilor de inregistrare, operate de către ANTA.

2.3.1 Arhitectura Sistemului

In figura 3.1.a este prezentata arhitectura sistemului national de emitere si gestiune a cartelelor pentru tahografele digitale.

Arhitectura componentelor sistemului national este prezentata in sectiunile dedicate componentelor respective.

MD-A este autoritatea administrativa care stabileste normele si procedurile de lucru pentru unitatile operative, exercita activitatea generala de control si mentine legatura cu organelle legislative ale Uniunii Europene. MD-A este organismul de contact in relatia cu autoritatea de certificare root Europeana, ERCA.

Fluxul de emitere a unei cartele tahografice personalizate este urmatorul:

1. Solicitantul pentru a aplica pentru o cartela tahografica (de sofer, companie, control sau atelier) se prezinta la un birou al MD-CIA unde prezinta documentatia necesara, si impreuna cu operatorul MD-CIA completeaza cererea de emitere a cartelei, pe care o semneaza
2. Operatorul MD-CIA verifica datele solicitantului pe baza documentatiei si inregistreaza cererea in baza de date.
3. Sistemul MD-CIA verifica automat datele solicitantului atat la nivel national in baza de date MD-CIA, cat si la nivel European, prin TACHOnet, daca verificarile interne au fost in regula. Daca toate verificarile s-au desfasurat cu succes, cererea solicitantului este validata (marcata ca valida in baza de date a MD-CIA)
4. Un operator MD-CIA cu rolul de supervizor selecteaza cererile valide din baza de date a MD-CIA si le trimite spre executie la MD-CP. Date necesare personalizarii cardurilor sunt trimise folosind o conexiune securizata (semnate, marcate temporal si criptate) la MD-CP.
5. MD-CP verifica cererile primate de la MD-CIA, genereaza cererile de certificate corespunzatoare si le trimite la MD-CA pentru a obtine certificatele corespunzatoare
6. MD-CA receptioneaza cererile de certificate de la MD-CP, genereaza certificatele corespunzatoare si le trimite la MD-CP;
7. MD-CP personalizeaza cartela tahografica atat vizual cat si electric (cip-ul), iar pentru cartelele de atelier genereaza si PIN-ul si il tipareste intr-un plic special pentru a fi expediat catre aplicant
8. MD-CP trimite cardurile personalizate si ambalate la MD-CIA pentru a fi eliberate solicitantilor.
9. Solicitantul se prezinta la biroul MD-CIA pentru asi ridica cartela tahografica personalizata.

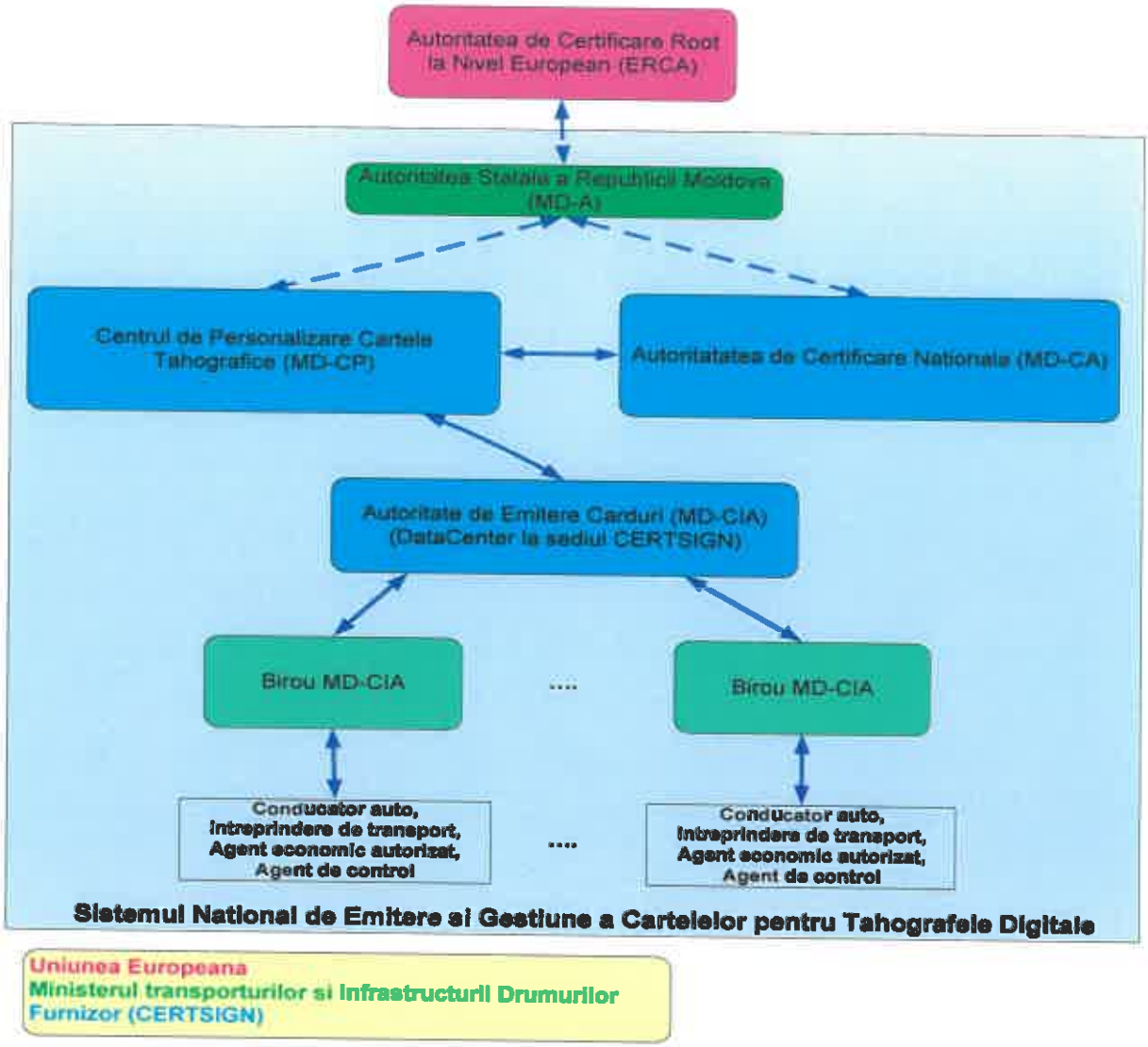


Figura 3.1.a: *Arhitectura sistemului national de emitere si gestiune a certelelor pentru tahografele digitale*

2.3.2 MD-CIA

Autoritatea de inregistrare, emitere si gestiune a cartelelor tahografice pe durata ciclului lor de viata, MD-CIA, dezvoltata si implementata de catre CERTSIGN in anul 2010 si actualizată în perioada 2010 – 2020, realizeaza urmatoarele functii:

- Informeaza toti utilizatorii asupra cerintelor care trebuie indeplinite in scopul obtinerii unui card tahografice. Pentru aceasta sunt publicate pe un site web urmatoarele:
  - Lista documentelelor cu care trebuie sa se prezinte la birourile MD-CIA pentru obtinerea unei cartele tahografice sau pentru declararea modificarii starii acestela

- Cererile de emitere de cartele tahografice, cu optiunea de tiparire, pentru: conducatorii auto, organele de control, companiile de transpoort si atelierele acreditate
- legislatia nationala, la nivelul AETR si la nivelul Uniunii Europene privitoare la sistemul tahografului digital
- orice alte informatii publice legate de sistemul tahografului digital, la cererea beneficiarului

- Inregistreaza cererile de emitere, reinnoire, schimb a cartelelor tahografice. Aceste operatiuni se realizeaza de catre operatorii birourilor de inregistrare si emitere a cartelelor tahografice ale MD-CIA folosind aplicatia web de operare a MD-CIA, componentă a sistemului tachoSAFE CIA;
- Verifica daca toate cerintele necesare obtinerii unei cartele tahografice sunt indeplinite. Verificarea corectitudinii datelor furnizate de catre aplicanti si a legalităţii emiterii cartelei tahografice se va face in 3 etape:
  - manual, de catre operatorii MD-CIA, prin verificarea actelor aferente (buletin de identitate, permis de conducere, etc) la inregistrarea cererilor;
  - automat, la nivel national, prin verificarea datelor disponibile pe serverul de baze de date al MD-CIA. Aceasta verificare este realizata de catre modulul de verificare a datelor aplicantilor;
  - automat, la nivel european, de catre aplicatia de interfatare, comunicare si notificare cu sistemul TACHOnet, se verifica daca persoana care a solicitat cartela mai are o alta cartela tahografica emisa in alt stat, prin utilizarea serviciului TACHOnet;
- Genereaza cererile de cartele tahografice si asigura trimiterea datelor strict necesare emiterii cartelelor tahografice corespunzatoare la MD-CP, in conditiile de securitate cerute, cu ajutorul aplicatiei de interfatare si comunicare cu MD-CP;
- Asigura transmiterea PIN-ului cartelelor de atelier persoanei autorizate. Scrisorile care contin PIN-ul sunt primite de la MD-CP separat de cardurile corespunzatoare (in alt plic);
- Realizeaza stocarea si gestiunea datelor cu caracter personal folosind baza de date Oracle a MD-CIA si aplicatia web de operare a MD-CIA;
- Asigura managementul cartelelor tahografice pe intreaga durata a ciclului lor de viata folosind baza de date Oracle a MD-CIA si aplicatia web de operare a MD-CIA;
- Inregistreaza declararea pierderii, furtului, defectarii sau suspendarii cardului tahografic folosind aplicatia web de operare a MD-CIA;
- Stochează istoricul fiecarui card in baza de date si actualizează, in functie de evenimentele raportate, starea fiecarui card emis.
- Se interfateaza si comunica cu sistemul TACHOnet folosind aplicaţiile de interfatare, comunicare si notificare cu TACHOnet ale sistemului tachoSAFE oferit;
- Se interfateaza si comunica cu MD-CP folosind o conexiune securizata prin care trimite automat cererile de cartele tahografice si datele necesare

personalizarii acestora la MD-CP si primeste de la MD-CP starea cererilor si cartelelor corespunzatoare folosind aplicatia de interfatare si comunicare cu MD-CP;

- Informeaza MD-A si MD-CA despre toate incidentele de securitate.
- Asigura confidentialitatea datelor obtinute in urma inregistrarii de la persoanele fizice si juridice. In acest scop doar operatorii aplicatiei web de operare a MD-CIA au acces la aceste informatii si doar prin intermediul aplicatiei, la care trebuie sa se autentifice mutual pe baza certificatului digital. Toate accesarile si actiunile efectuate de catre orice entitate (operator sau aplicatie) sunt logate in fisiere speciale de audit. Pentru comunicatii se folosesc doar conexiuni securizate;
- Permite realizarea backup-ului periodic a bazei de date a MD-CIA cat si a fisierelor speciale de audit.
- Toate interfețele aplicațiilor software ale sistemului autorității de inregistrare, emitere si gestiune a cartelelor tahografice pe durata ciclului lor de viata, MD-CIA, sunt în limba Română.

Din punct de vedere software, sistemul MD-CIA contine urmatoarele componente:

- Baza de date a MD-CIA
- Aplicatia Web de operare a MD-CIA
- Aplicatia de interfatare, comunicare si notificare cu sistemul TACHOnet
- Aplicatia de interfatare si comunicare cu MD-CP
- Modulul de validare automata a datelor aplicantilor
- Modulul de logare si notificare

Arhitectura este una distribuita, fiecare dintre modulele componente putand rula pe masini diferite. Acest lucru permite aplicarea unor politici de securitate diferite pentru fiecare dintre sistemele hardware pe care ruleaza modulele aplicatiei.

Aplicatia web de operare a MD-CIA este singura aplicatie care permite operatorilor MD-CIA sa interactioneze cu sistemul, celelalte aplicatii/module au doar rolul de a efectua operatii automate pe baza mesajelor primite in baza de date de la aplicatia web, aplicatia de interfatare, comunicare si notificare cu TACHOnet si MD-CP prin intermediul aplicatiei de interfatare si comunicare cu MD-CP.

Punctul central de stocare a datelor este serverul de baze de date, iar comunicarea intre modulele aplicatiei se realizeaza prin intermediul acestuia.

2.3.2.1 Arhitectura MD-CIA

Arhitectura sistemului autoritatii de emitere si gestiune a cartelelor tahografice, MD-CIA, este prezentata in figura 3.2.1.a.

Sistemul MD-CIA contine 2 zone distincte: o zona centrala, numita in continuare Data Center-ul MD-CIA, care consta intr-un mediu securizat in care sunt amplasate serverele MD-CIA si echipamentele aferente, situat la sediul

CERTSIGN, si o zona descentralizata care cuprinde toate birourile de inregistrare si emitere a cartelelor tahografice ale MD-CIA din teritoriu, astfel:

- Zona centrala - data center – sediul CERTSIGN
  - Serverul de baze de date
    - Serverul de baze de date Oracle, baza de date a MD-CIA si baza de date a a aplicatiei de auto enrolment
    - Aplicatia de interfatare si comunicare cu MD-CP
    - Modulul de administrare si monitorizare
  - Server-ul WEB
    - Aplicatia WEB de inregistrare a aplicantilor si gestiune a cartelelor tahografice, numita si aplicatia web de operare a MD-CIA
    - Modulul de administrare si monitorizare, care este integrat in aplicatia web de operare a MD-CIA
    - Aplicatia de interfatare&validare/notificare cu serviciul TACHOnet
    - Aplicatia de validare automata a datelor solicitantilor de cartele tahografice cu baza de date a MD-CIA
  - Consola pentru administratorii de aplicatii, DB, securitate
    - Aplicatii de administrare/monitorizare

- Zona descentralizata – birourile de inregistrare MD-CIA ale ANTA din teritoriu
  - Statie de lucru pentru operatori cu interfetele necesare conectarii token-ului criptografic, scanner-ului si padului de semnatura
    - Browser WEB
    - Aplicatie pentru scanarea si formatarea semnaturii si a fotografiei aplicantului
  - Scanner pentru scanarea semnaturii si/sau a fotografiei aplicantului
  - Modulul pentru verificarea si vizualizarea datelor de pe cartelele tahografice.

Serverul de baze de date din DataCenter-ul MD-CIA are sistemul de operare Suse Linux Enterprise Server si gazduieste serverul de baze de date Oracle Database Standard One.

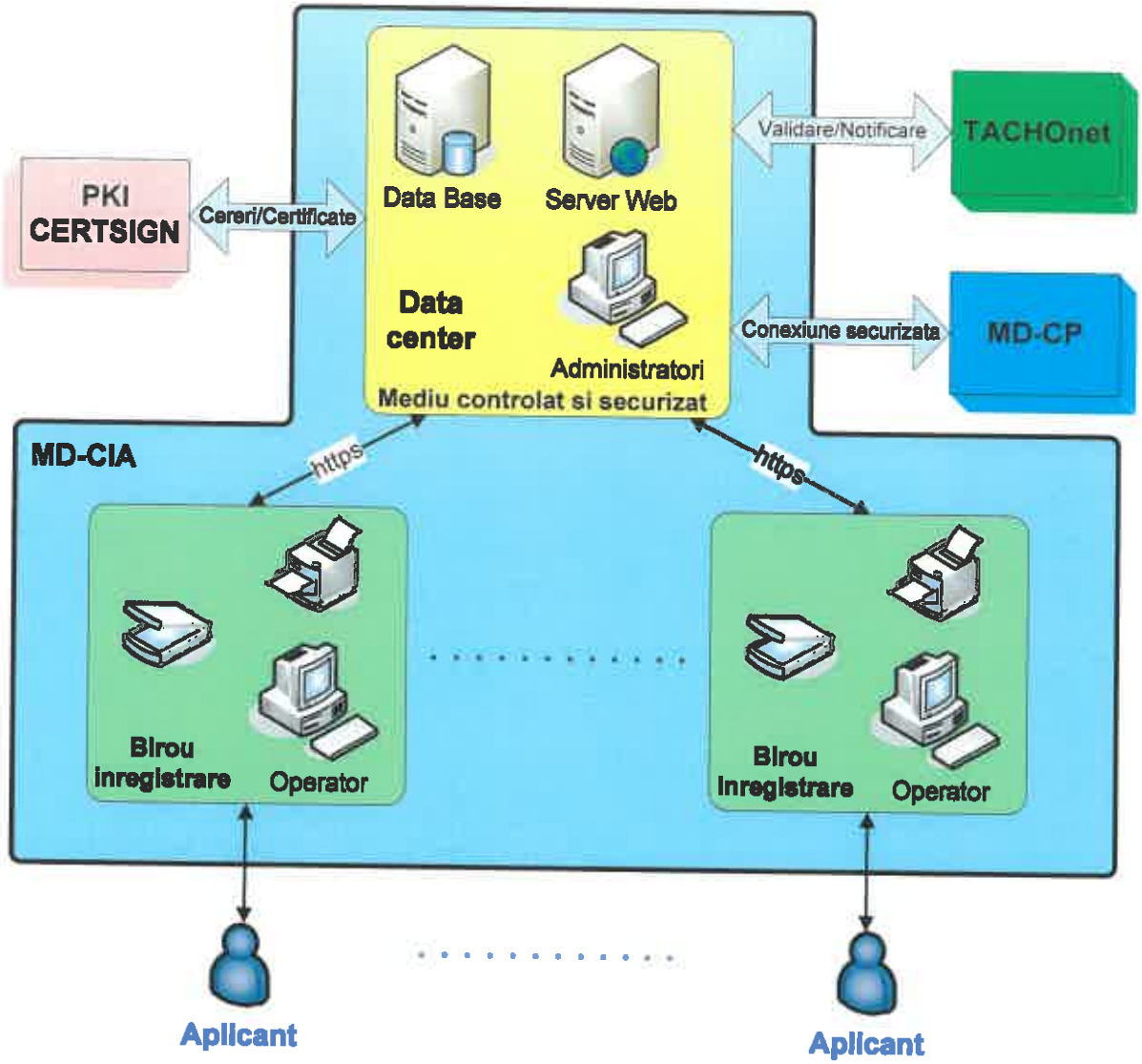


Figura 3.2.1.a: *Arhitectura MD-CIA*

Serverul web din DataCenter-ul MD-CIA foloseşte sistemul de operare Suse Linux Enterprise Server si gazduieşte serverul web Apache inclus in distributia sistemului de operare.

In zona descentralizata pot opera un numar oricat de mare de birouri de inregistrare si eliberare cartele fara a afecta performantele sistemului.

Arhitectura descrisa permite mentinerea datelor de productie pe termen lung.

2.3.2.2 Procese MD-CIA

Principalele procese care se desfasoara in cadrul sistemului de inregistrare si emitere a cartelelor tahografice, MD-CIA, sunt:

- Inregistrarea cererilor de emitere a cartelelor tahografice
- Validarea cererilor de emitere a cartelelor tahografice
- Aprobarea si lansarea in executie a cererilor de emitere a cartelelor tahografice

2.3.2.2.1 Procesul de inregistrare a cererilor

Inregistrarea cererilor de emitere a cartelelor tahografice se efectueaza la birourile MD-CIA. Inregistrarea unei cereri se face de catre operatorul MD-CIA in prezenta solicitantului.

Pentru acest lucru se va utiliza aplicatia web de operare a MD-CIA care pune la dispozitia operatorului un set de formulare specifice fiecarui tip de cartela. Acesta va completa formularele pe baza informatiilor puse la dispozitie de catre solicitant si va verifica autenticitatea acestora.

Procesul de inregistrare a unei cereri cuprinde urmatorii pasi:

- operatorul MD-CIA verifica datele solicitantului pe baza documentelor pe care acesta trebuie sa le prezinte la ghiseu (buletin de identitate, actele firmei de transport, permis de conducere, etc), in functie de tipul de cartela tahografica pentru care depune cererea;
- operatorul MD-CIA completeaza formularele din interfata web a aplicatiei;
- pentru cartelele de conducator auto si agent de control se scaneaza si se formateaza poza pentru a corespunde cerintelor MD-CP pentru personalizarea cartelelor;
- se scaneaza si se formateaza semnatura olografa a solicitandului pentru a corespunde cerintelor MD-CP pentru personalizarea cartelelor;
- se poate tipari din interfata web a aplicatiei cererea de cartela tahografica, ale carei sectiuni vor fi completate automat cu datele introduse de catre operator. Aceasta cerere trebuie semnata de catre solicitant. Daca solicitantul se prezinta cu cererea deja completata, folosind formularul pus la dispozitie pe site-ul web, nu mai este necesara tiparirea de catre operator a acestuia;
- se inregistreaza efectiv cererea in baza de date si i se aloca un cod unic de inregistrare.

Inregistrarea efectiva a cererii in baza de date semnifica faptul ca procesul de inregistrare s-a finalizat, si urmeaza ca respectiva cerere sa fie validate la nivel national si international, aprobata pentru executie si trimisa la MD-CP pentru emiterea cartelei tahografice.

2.3.2.2.2 Procesul de validare a cererilor

Validarea cererilor de emitere a cartelelor tahografice se efectueaza in 3 pasi, si anume:

- Validarea manuala, realizata de catre personalul ANTA din teritoriu. La inregistrarea cererii operatorul MD-CIA va solicita actele necasare identificarii solicitantului (buletin de identitate, actele firmei, permisul de conducere, etc) in functie de tipul cartelei tahografice pentru care face cererea, si va verifica corectitudinea datelor introduse in cerere. In acest moment se realizeaza identificarea solicitantului cartelei tahografice, motiv pentru care acesta trebuie sa se prezinte personal la agentia ANTA;

- Validarea la nivel national se realizeaza automat dupa introducerea in sistem a datelor corespunzatoare cererii. Datele respective sunt validate folosind informatiile stocate in baza de date a MD-CIA;
- Daca validarea la nivel national s-a realizat cu success, se continua cu validarea cererii la nivel international, folosind sistemul TACHOnet, pentru a asigura faptul ca solicitantul nu mai are alt card tahografic valid emis in alt stat.

In final, daca procesul de validare a cererii aplicantului s-a realizat cu success, cererea respectiva poate fi aprobata pentru personalizare, folosind interfata web a aplicatiei MD-CIA, de catre un operator cu rolul de supervisor. Acesta va putea vizualiza lista cererilor care trebuiesc aprobate, si va decide pentru fiecare dintre ele daca o aproba sau nu.

Aprobarea unei cereri sau a unui grup de cereri se va realiza prin generarea unei note de comanda care poate fi tiparita si semnata pe hartie sau poate fi semnata digital folosind certificatul digital al operatorului respectiv, certificat furnizat de CERTSIGN si stocat pe tokenul criptografic al operatorului.

In momentul aprobarii se genereaza o comanda de cartele tahografice in format electronic, comanda care contine toate datele necesare personalizarii cartelelor la MD-CP. Datele sunt impachetate intr-un format XML, sunt transmise printr-un canal de comunicatie securizat la central de personalizarea al CERTSIGN, MD-CP pentru personalizarea cartelelor tahografice solicitate.

2.3.2.2.3 Procesul de eliberare cartela tahografica

Eliberarea unei cartele se face de catre operatorii MD-CIA dupa primirea cartelelor tahografice personalizate de la MD-CP (CERTSIGN).

Fiecare plic livrat de CERTSIGN contine o scrisoare insotitoare a cartelei tahografice cu instructiuni sumare de utilizarea a acesteia, personalizata cu datele destinatarului. Cartela este atasata de scrisoarea insotitoare si apoi este impliculta in plicuri special personalizate cu insemnele ANTA. In fereastra plicului, pe langa informatiile corespunzatoare posesorului cartelei, este vizibil si numarul cartelei tahografice. Numarul cartelei poate fi introdus de catre operator intr-o pagina speciala din interfata web a aplicatiei MD-CIA pentru a vizualiza informatiile despre posesorul cartelei. Pe baza acestor informatii operatorul MD-CIA poate programa o intalnire cu solicitantul cartelei in vederea inmanarii acesteia.

In momentul inmanarii cartelei catre solicitant, acesta va trebui sa semneze un document de primire impreuna cu operatorul MD-CIA, iar acesta din urma va trebui sa seteze in interfata web noua stare a cartelei tahografice, care va deveni "Inmanata".

2.3.2.2.4 Procesul de modificare stare cartela tahografica

Modificarea starii unei cartele tahografice este necesara in una din urmatoarele situatii:

- în momentul expirării cartelei
- în momentul reînnoirii cartelei

- în momentul confiscării cartelei
- în momentul suspendării temporare a cartelei
- în momentul reținerii de către o autoritate competentă a cartelei
- în momentul schimbării cartelei
- în momentul declarării pierderii cartelei
- în momentul declarării furtului cartelei
- în momentul defectării (nefuncționării corespunzătoare) a cartelei
- în momentul predării unei cartele pierdute sau furate

In functie de tipul modificarii starii cartelei, se identifica urmatoarele variante ale procesului:

Procesul de expirare a unei cartele se desfasoara astfel:

1) Un modul software automat verifica periodic validitatea cartelelor tahografice inregistrate in system;
2) Pentru cartelele care urmeaza sa expire intr-un interval de timp mai mic decit o valoare configurabila (de ex. 1 luna) modulul software respectiv va notifica pe e-mail posesorul (daca acesta a oferit o adresa de e-mail la inregistrare) si, optional, notifica pe e-mail un operator MD-CIA, daca se va dori contactarea posesorului cartelei in scopul notificarii acestuia;
3) Pentru cartelele care deja au expirat de la ultima verificare, modulul software respectiv setează starea cartelei pe valoarea "Expired" în baza de date a MD-CIA şi trimite un mesaj de notificare asupra modificării stării cartelei către serverul central al TACHOnet.

Procesul de reînnoire a unei cartele tahografice.

1) Pentru ca o cartela tahografica sa treaca in starea "Renewed" trebuie ca posesorul acesteia sa se prezinte la un ghiseu MD-CIA inainte de expirarea cartelei si sa completeze o cerere de reinnoire. Cererea de reinnoire poate fi depusa doar daca datele de inregistrare ale posesorului nu s-au schimbat de la emiterea anterioara;
2) Se valideaza din nou datele solicitantului atat la nivel national cat si european;
3) Se trimite cererea la MD-CP pentru emiterea noii cartele;
4) Se primeste noua cartela de la MD-CP;
5) Solicitantul se prezinta la ghiseul MD-CIA, preda operatorului vechia cartela pentru a fi distrusa si primeste noua cartela. Simultan se actualizeaza in baza de date a MD-CIA starea cartelei.

Procesul de confiscare a unei cartele se efectuează astfel:

1) Un controlor, in urma confiscarii unei cartele, va raporta datele despre cartela confiscată unui operator MD-CIA. De asemenea, daca controlorul utilizeaza aplicatia de validare in trafic a starii cartelelor tahografice

furnizata de CERTSIGN, raportarea confiscarii se poate face automat utilizand aceasta aplicatie, fara a mai fi necesara interventia unui operator MD-CIA;

2) Operatorul va utiliza aplicatia web de operare a MD-CIA pentru a gasi cartela respectivă şi a-i seta starea pe valoarea "Confiscata";
3) Aplicatia web de operare a MD-CIA va actualiza in baza de date a MD-CIA starea cartelei si va plasa, de asemenea, o cerere de notificare TACHOnet;
4) Aplicatia de interfatare, comunicare si validare cu TACHOnet va prelucra cererea de notificare gasita in baza de date si va trimite un mesaj de informare asupra modificării stării cartelei către serverul central al TACHOnet.

Procesul de suspendarea temporară a unei cartele se efectuează astfel:

1) Posesorul unei cartele va raporta datele despre cartela care doreşte să fie suspendată unui operator MD-CIA;
2) Operatorul va utiliza aplicatia web de operare a MD-CIA pentru a gasi cartela respectivă şi a-i seta starea pe valoarea "Suspendata";
5) Aplicatia web de operare a MD-CIA va actualiza in baza de date a MD-CIA starea cartelei si va plasa, de asemenea, o cerere de notificare TACHOnet;
3) Aplicatia de interfatare, comunicare si validare cu TACHOnet va prelucra cererea de notificare gasita in baza de date si va trimite un mesaj de informare asupra modificării stării cartelei către serverul central al TACHOnet.

Procesul de retragere a unei cartele se efectuează astfel:

1) Un operator MD-CIA poate decide sa retraga o cartela tahografica din diferite motive, cum ar fi: datele de personalizare a cartelei au fost gresite, posesorul cartelei nu mai are dreptul sa detina cartela respectiva, etc.
2) Operatorul va utiliza aplicatia web de operare a MD-CIA pentru a gasi cartela respectivă şi a-i seta starea pe valoarea "Retrasa";
3) Aplicatia web de operare a MD-CIA va actualiza in baza de date a MD-CIA starea cartelei si va plasa, de asemenea, o cerere de notificare TACHOnet;
4) Aplicatia de interfatare, comunicare si validare cu TACHOnet va prelucra cererea de notificare gasita in baza de date si va trimite un mesaj de informare asupra modificării stării cartelei către serverul central al TACHOnet.

Procesul de schimbare a unei cartele se efectuează astfel:

1) Posesorul unei cartele se va prezenta la un birou MD-CIA unde va inregistra o cerere de schimbare a cartelei. Pentru aceasta va prezenta documentele care dovedesc modificarea datelor de inregistrare a solicitantului;
2) Operatorul va utiliza aplicatia web de operare a MD-CIA pentru a gasi cartela respectivă şi îi va seta starea pe valoarea „In schimbare";

3) Operatorul MD-CIA va inregistra o cerere de schimbare a cartelei. Procesul de inregistrare cerere schimbare cartela este similar procesului de inregistrare a unei cereri de prima eliberare, cu diferenta ca de data aceasta campurile cererii vor fi precompletate cu datele vechi ale solicitantului, iar operatorul va putea actualiza aceste date;
4) Aplicatia web de operare a MD-CIA va actualiza in baza de date a MD-CIA starea cartelei si va plasa, de asemenea, o cerere de notificare TACHOnet;
5) Aplicatia de interfatare, comunicare si validare cu TACHOnet va prelucra cererea de notificare gasita in baza de date si va trimite un mesaj de informare asupra modificării stării cartelei către serverul central al TACHOnet;
6) In momentul în care noua cartelă a ajuns în starea "Inmanata", starea vechii cartele se va modifica automat pe valoarea "Schimbata" şi se va trimite un nou mesaj de informare asupra modificării stării cartelei către serverul central al TACHOnet.

Procesul de declararea a pierderii unei cartele se efectuează astfel:

1) Posesorul unei cartele va raporta datele despre cartela pe care a pierdut-o sau, dacă nu cunoaşte respectivele date, va raporta datele de identificare ale sale către un operator MD-CIA;
2) Operatorul va utiliza aplicatia web de operare a MD-CIA pentru a gasi cartela respectivă şi a-i seta starea pe valoarea "Pierduta";
3) Aplicatia web de operare a MD-CIA va actualiza in baza de date a MD-CIA starea cartelei si va plasa, de asemenea, o cerere de notificare TACHOnet;
4) Aplicatia de interfatare, comunicare si validare cu TACHOnet va prelucra cererea de notificare gasita in baza de date si va trimite un mesaj de informare asupra modificării stării cartelei către serverul central al TACHOnet.

Procesul de declararea a furtului unei cartele se efectuează astfel:

1) Posesorul unei cartele va raporta datele despre cartela care i-a fost furată sau, dacă nu cunoaşte respectivele date, va raporta datele de indetificare ale sale către un operator MD-CIA;
2) Operatorul va utiliza aplicatia web de operare a MD-CIA pentru a gasi cartela respectivă şi a-i seta starea pe valoarea "Furata";
3) Aplicatia web de operare a MD-CIA va actualiza in baza de date a MD-CIA starea cartelei si va plasa, de asemenea, o cerere de notificare TACHOnet;
4) Aplicatia de interfatare, comunicare si validare cu TACHOnet va prelucra cererea de notificare gasita in baza de date si va trimite un mesaj de informare asupra modificării stării cartelei către serverul central al TACHOnet.

Procesul de declararea a defectării unei cartele se efectuează astfel:

1) Posesorul se va prezenta la un ghiseu MD-CIA cu cartela respectiva si pentru a raporta defectarea si a preda cartela. Operatorul MD-CIA poate verifica cartela folosind modului de vizualizare a datelor cartelelor tahografice integrat in aplicatia de operare a MD-CIA;
2) Operatorul va utiliza aplicatia web de operare a MD-CIA pentru a gasi cartela respectivă şi a-i seta starea pe valoarea "Malfunctioning";
3) Aplicatia web de operare a MD-CIA va actualiza in baza de date a MD-CIA starea cartelei si va plasa, de asemenea, o cerere de notificare TACHOnet;
4) Aplicatia de interfatare, comunicare si validare cu TACHOnet va prelucra cererea de notificare gasita in baza de date si va trimite un mesaj de informare asupra modificării stării cartelei către serverul central al TACHOnet.
5) Dacă posesorul cartelei doreşte ca aceasta să fie înlocuită, atunci operatorul MD-CIA va introduce o cerere de inlocuire cartelă (vezi procesul de înregistrare a cererilor de emitere cartele);
6) Cartela raportata ca defecta va fi trimisa la MD-CP pentru verificare;
7) Daca se dovedeste ca respectiva cartela nu este defecta, solicitantul va trebui sa plateasca taxa pentru emiterea unei noi cartele;
8) In momentul în care noua cartelă a ajuns în starea "Inmanata", starea vechii cartele se va seta pe valoarea "Inlocuita" şi se va trimite un mesaj de informare asupra modificării stării cartelei către serverul central al TACHOnet.

Procesul de predare a unei cartele pierdute sau furate se desfasoara astfel:

1) În momentul găsirii unei cartele pierdute sau furate şi predarii acesteia către autorităţi, agentul care a preluat cartela va trebui să raporteze către un operator MD-CIA primirea cartelei;
2) Operatorul va utiliza aplicatia web de operare a MD-CIA pentru a identifica cartela respectivă şi a-i seta starea pe valoarea "Inlocuita" dacă între timp s-a emis o nouă cartelă care să o înlocuiască, sau pe "Predata" dacă între timp nu s-a emis o nouă cartelă care să o înlocuiască;
5) Aplicatia web de operare a MD-CIA va actualiza in baza de date a MD-CIA starea cartelei si va plasa, de asemenea, o cerere de notificare TACHOnet;
3) Aplicatia de interfatare, comunicare si validare cu TACHOnet va prelucra cererea de notificare gasita in baza de date si va trimite un mesaj de informare asupra modificării stării cartelei către serverul central al TACHOnet

Diagrama tranziţiilor stărilor cartelelor tahografice in cadrul sistemului propus de CERTSIGN este prezentata in figura 3.2.2.4.a. Aceasta diagrama de stari respecta intru totul specificaţiile definite in documentul "TACHOnet - XML Messaging Reference Guide, V1.5".

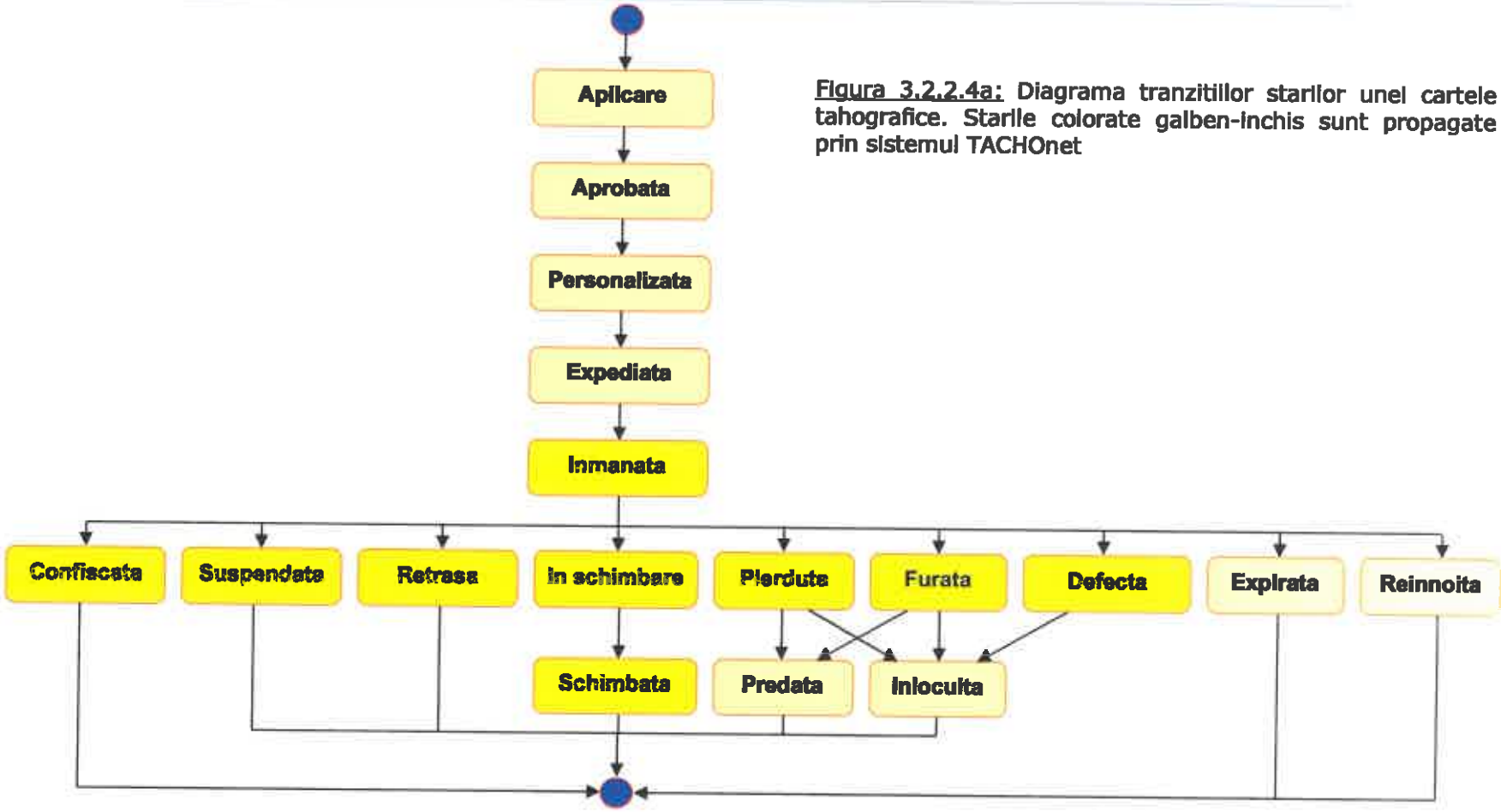


Figura 3.2.2.4a: Diagrama tranzitiilor starilor unei cartele tahografice. Starile colorate galben-inchis sunt propagate prin sistemul TACHOnet

2.3.2.3 Aplicatiile software MD-CIA

Din punct de vedere software, sistemul MD-CIA contine urmatoarele componente:

- Baza de date a MD-CIA
- Aplicatia Web de operare a MD-CIA
- Aplicatia Web de inregistrare on-line a cererilor de cartele tahografice (auto enrolement)
- Aplicatia de interfatare, comunicare si notificare cu sistemul TACHOnet
- Aplicatia de interfatare si comunicare cu MD-CP
- Modulul de validare automata a datelor aplicantilor
- Modulul de logare si notificare
- Modulul de administrare si monitorizare
- Aplicatia de backup

Punctul central de stocare a datelor este serverul de baze de date, iar comunicarea intre modulele aplicatiei se realizeaza prin intermediul acestuia.

Fiecare aplicatie are propriile fisiere de configurare in format XML, care permit administratorilor configurarea si administrarea facila a fiecarei aplicatii sau modul de aplicatie din sistem.

Fiecare aplicatie utilizeaza o componenta de logare si notificare care permite inregistrarea log-urilor de audit si erori in fisiere special de audit si permite trimiterea de mesaje de e-mail la aparitia unor evenimente critice in sistem.

Pentru backup se va folosi aplicatia Legato Networker.

2.3.2.3.1 Aplicatia web de operare a MD-CIA

Aplicatia web de operare MD-CIA este cea care permite operatorilor MD-CIA sa interactioneze cu sistemul. Aceasta este o aplicatie web-based cu interfata in limba Romana care poate fi accesata cu un browser de Internet. Operatorii vor putea accesa aplicatia doar prin autentificare mutuala bazata pe certificate digitale emise de catre CERTSIGN. In acest scop fiecare operator are un token criptografic pe care sunt stocate certificatele si cheile necesare.

Aplicatia ofera urmatoarele functii:

- Administrarea operatorilor si a rolurilor acestora;
- Inregistrarea cererilor de emitere cartele tahografice, prin:
  - Preluarea datelor necesare personalizarii cartelelor tahografice ale conducatorilor de vehicule, organelor de control, firmelor de transport si atelierelor acreditate, inclusiv imaginea faciala si semnatura in format electronic;
  - Verificarea corectitudinii datelor si a legalitatii emiterii cartelelor tahografice utilizatorilor respectivi;

- Înregistrarea on-line a cererilor de cartele tahografice prin modului web de inregistrare on-line pus la dispozitie de către sistemul MD-CIA;
- Dacă utilizatorul şi-a precompletat datele prin modului web de inregistrare on-line pus la dispozitie de către sistemul MD-CIA, operatorul va prelua aceste date din baza de date a modului web de inregistrare on-line, va valida aceste date pe baza documentelor prezentate de catre utilizator şi va completa aceste date prin scanarea pozei si semnaturii de pe cererea pentru obtinerea cartelei tahografice.

- Vizualizarea informatiilor despre starea curenta a cartelei si posesorul acesteia;
- Inregistrarea declaratiilor de modificare a starii cartelei: furtul, pierderea, defectarea, confiscarea, retragerea, etc;
- Operatii de cautare, listare si vizualizare detalii conducatori auto, controlori, companii si ateliere auto;
- Vizualizarea datelor de personalizare ale cartelelor tahografice;
- Generarea de rapoarte de activitate si de statistici;
- Inregistrare, cautare, listare si vizualizare loguri pentru operatiile effectuate;
- Logare mesaje de audit, eroare si debug si trimitere de notificari prin e-mail.

Accesul la aplicatie se face folosind numai protocolul HTTPS pe conexiuni SSL cu autentificare multuala.

Fiecare incercare de accesare a aplicatiei, reusita sau nu, va fi logata intr-un fisier special de audit.

Server-ul web utilizat este Apache oferit de sistemul de operare SuSE Linux Enterprise Server care este instalat pe masina corespunzatoare serverului web.

Accesarea interfeţei web se face în *"sesiuni"*. O sesiune se lucru este reprezentată de o fereastră a browser-ului şi începe în momentul în care utilizatorul se autentifică folosind certificatul digital şi se termină în momentul în care utilizatorul a inchis fereastra browser-ului sau sesiunea a expirat.

Durata de viata a unei sesiuni este configurabila si reprezinta intervalul maxim de timp care poate trece de la ultima accesare a aplicatiei de catre operator. Astfel, daca durata de viata a unei sesiuni este de 10 minute si utilizatorul nu a accesat nici o functie a aplicatiei atunci sesiunea este inchisa automat. Apoi la urmatoarea functie accesata se va crea automat o noua sesiune si se va verifica iarasi certificatul operatorului.

Aplicatia web de operare a MD-CIA foloseste in paralel doua mecanisme de logare.

Primul dintre ele este comun si celorlalte aplicatii si permite logarea de mesaje de audit si eroare si trimiterea de notificari prin e-mail la aparitia anumitor

evenimente in utilizarea aplicatiei. Acesta este descris in sectiunea " Aplicatia de logare si notificare".

Cel de-al doilea mecanism de logare, specific acestei aplicatii, are rolul de a inregistra in baza de date anumite operatii efectuate de catre operatorii MD-CIA.

Aceste loguri contin urmatoarele informatii:

- tipul operatiei efectuate
- operatorul care a efectuat operatia
- data la care s-a efectuat operatia
- alte informatii (specifice fiecarui tip de operatie)

Scopul acestui mecanism de logare este de a inregistra istoricul operatiilor efectuate in sistem si de a permite operatorilor cu roluri speciale (auditor) vizualizarea acestora. Astfel, se poate monitoriza fiecare operatie de inregistrare, modificare stare cartela, interogare stare cartela, etc., efectuata de fiecare operator. Deasemeni, se poate vizualiza lista tuturor operatiilor efectuate asupra unei cartele pentru a detecta eventualele erori ale operatorilor umani.

Aplicatia este instalata pe serverul web din data center-ul CERTSIGN si poate fi accesata de operatorii situati in birourile de preluare cereri ai ANTA. Accesul se face prin conexiuni securizate SSL cu autentificare mutuala, care realizeaza canale criptate de comunicatie.

Configurarea aplicatiei se realizeaza utilizand fisiere speciale de configurare, accesibile doar administratorului sistemului. Acestea sunt incarcate la pornirea aplicatiei (a serverului web).

2.3.2.3.1.1 Managementul rolurilor operatorilor

Fiecare operator este caracterizat de un "rol de acces". Aplicatia limiteaza drepturile operatorilor in aplicatie conform rolurilor asignate. Rolul de acces permite operatorului respectiv să efectueze numai anumite operaţii, de exemplu: sa administreze sistemul, sa primeasca cererile de carduri, sa inregistreze modificari ale starilor cardurilor, sa initializeze trimiterea cererilor de carduri catre central de personalizare, MD-CP, etc.

Aplicatia ofera o interfata de management a operatorilor care au dreptul sa acceseze aplicatia. Aceasta interfata permite:

- adaugare operator
- modificare operator
- adaugare rol operator
- invalidare rol operator
- invalidare operator

Modulul de management a operatorilor CIA permite folosirea a patru roluri dupa cum urmeaza:

- administrator - administreaza sistemul, atribuie roluri pentru operatori

- operator - primeste cereri de carduri, inregistreaza modificari ale starii cardurilor (pierdere, furt, deteriorare, etc)

- supervisor - initializeaza trimiterea cererilor de carduri la CP pe baza cererilor strinse si validate in baza CIA pina la acel moment

- auditor – Poate decripta si verifica fisierele speciale de audit

Pentru fiecare rol pe care un operator il indeplineste, trebuie sa detina un certificat digital emis de catre CERTSIGN. Certificatul digital al operatorului contine o extensie privata care defineste unul din "rolurile de acces". Astfel, la accesare de catre un operator a aplicatiei web, certificatul acestuia va fi verificat si daca certificatul este valid si emis de catre autoritatea de certificare corespunzatoare se trece la faza a doua a autentificarii operatorului si anume a determinarii rolului pe care acesta il are in cadrul aplicatiei pentru a permite accesul doar in zonele corespunzatoare rolului pe care il detine. In cazul in care operatorul nu detine acces se va afisa un mesaj corespunzator si accesul la functiile aplicatiei va fi interzis. Fiecare accesare a sistemului de catre un operator se consemneaza in fisierele de audit corespunzatoare.

Aplicatia nu permite folosirea de catre un operator a unui singur certificat digital pentru mai multe roluri. Astfel, daca se doreste ca un operator sa indeplineasca mai multe roluri in aplicatie, acesta trebuie sa detina cate un certificat pentru fiecare rol in parte. In cazul in care un operator detine mai multe certificate si unul din certificate este revocat sau ii este anulat rolul (corespunzator certificatului) din aplicatie, el nu se va mai putea accesa aplicatia cu certificatul respectiv, deci in numele rolului respectiv. In schimb, va putea accesa aplicatia in numele rolurilor pentru care inca are un certificat operational si este inregistrat in aplicatie cu ajutorul certificatului respectiv.

Daca un operator este autentificat in aplicatie cu un anumit rol, pentru a accesa o zona specifica unui alt rol, el va trebui sa inchida sesiunea curenta si sa se autentifice iar in aplicatie, dar de data asta sa foloseasca certificatul digital corespunzator celuilalt rol.

Aplicatia de management a operatorilor poate fi accesata doar de catre un utilizator care are rolul de "administrator". Administratorul este cel care poate adauga noi operatori in sistem.

2.3.2.3.1.2 Inregistrarea cererilor de cartele tahografice

Aplicatia web de operare a MD-CIA permite inregistrarea cererilor de cartele tahografice pentru toare cele 4 tipuri de cartele:

- Cartela de Conducator Auto
- Cartela de Controlor
- Cartela de Companie
- Cartela de Atelier Auto

Inregistrarea cererilor de cartele tahografice se poate face doar de catre utilizatorii aplicatiei cu rolul de "operator". Solicitantii pot completa si tipari de

acasa cererile, folosind site-ul web al ANTA pe care sunt disponibile pentru tiparire formularele tipizate de cereri, sau pot furniza datele necesare direct la ghiseul MD-CIA.

In functie de fiecare tip de cartela, operatorul trebuie sa introduca in formularul de inregistrare anumite date, inclusiv semnatura olografa scanata si formatata corespunzator, iar in cazul cererilor pentru carduri de conducatori auto si organe de control si poza posesorului scanata si formatata corespunzator. Scanarea si formatarea semnaturii si a pozei se poate face tot de catre operatorul MD-CIA cu ajutorul modulului de scanare si formatare inclus in aplicatia web a MD-CIA.

Dupa completarea formularului cu informatiile furnizate de catre solicitant, aplicatia ofera optiunea de tiparire la imprimanta a cererii astfel completate, optiune ce poate fi folosita in cazul in care solicitantul nu vine cu cererea deja completata. Cererile trebuie semnate in prezenta operatorului MD-CIA, pentru a se asigura autenticitatea semnaturii.

Operatorul verifica datele furnizate in baza documentelor pe care solicitantul este oblicat sa le prezinte la inregistrare (buletin de identitate, pasaport, permis de conducere, etc). Dupa ce datele au fost verificate si cererea a fost semnata, operatorul MD-CIA o va inregistra in sistem.

Dupa inregistrarea cererii de emitere cartela tahografica in sistem urmeaza 2 etape de verificare automate, transparente pentru operator:

- se verifica la nivel national datele solicitantului, prin verificarea datelor disponibile pe serverul de baze de date al MD-CIA. Aceasta verificare este realizata de catre modulul de verificare a datelor aplicantilor;
- se verifica la nivel european, de catre aplicatia de interfatare, comunicare si notificare cu TACHOnet, daca persoana care a solicitat cardul mai are o cartela tahografica emisa in alt stat membru, prin conectarea la reteaua TACHOnet.

Daca toate verificarile se realizeaza cu success cererea se marcheaza ca valida in baza de date a MD-CIA, in caz contrar fiind marcata ca invalida. Daca cererea este invalidata, in baza de date va fi inregistrat si motivul invalidarii.

Operatorul va putea verifica daca cererile inregistrate au fost validate sau invalidate, iar in caz de invalidare va putea sa vada si motivul pentru care cererea a fost invalidata.

Pentru a fi trimisa la MD-CP pentru emiterea cartelei tahografice cererea validata trebuie aprobata catre executie de un operator MD-CIA cu rolul de "supervisor". Aceasta aprobare se poate face pe mai multe cereri valide in acelasi timp (in mod normal aceasta operatie se executa o data pe zi), si are ca rezultat trimiterea cererilor cu datele necesare emiterii cartelelor tahografice la MD-CP prin intermediul aplicatiei de interfatare si comunicare cu MD-CP si, optional, trimiterea unui e-mail semnat si marcat temporal de catre supervizorul respectiv la MD-CP, e-mail in care se solicita emiterea cartelelor tahografice respective autoritatii MD-CP.

2.3.2.3.1.3 Modulul de achiziție date biometrice

Actiunea de preluare a imaginii faciale si a semnaturii olografe in format electronic este realizata in cadrul operatiei de inregistrare a cererilor de cartele tahografice din cadrul aplicatiei web de operare a MD-CIA cu ajutorul modulului de achiziție date biometrice.

La inregistrarea unei cereri de cartela tahografica de conducator auto sau organ de control aplicatia permite operatorului sa realizeze achizitia imaginii faciale a viitorului posesor a cartelei prin scanarea fotografiei cu care acesta trebuie sa se prezinte la ghiseu.

Dimensiunea imaginii faciale pe cartelele tahografice va fi 18 mm x 23 mm. Aceasta dimensiune poate fi modificata la cererea beneficiarului intre anumite limite, astfel incat sa nu afecteze structura vizuala a cartelei tahografice.

La inregistrarea cererilor de cartele tahografice aplicatia permite operatorului sa realizeze achizitia semnaturii olografe in format electronic a solicitantului prin scanarea acesteia.

Dimensiunea imaginii semnaturii olografe pe cartelele tahografice va fi 23 mm x 7 mm. Aceasta dimensiune poate fi modificata la cererea beneficiarului intre anumite limite, astfel incat sa nu afecteze structura vizuala a cartelei tahografice.

Imaginile scanate pot fi decupate, scalate si formatate pentru a putea fi aduse la caracteristicile necesare tiparirii pe cartela tahografica. Aceaste imagini sunt integrate in cererile de cartele tahografice automat.

In cazul in care operatorul observa ca imaginea pozei sau semnaturii nu este de calitate, are posibilitatea actualizarii acesteia reluand actiunea de achizitie.

Achizitia imaginii faciale si a semnaturii se realizeaza utilizand un scanner.

Pentru achizitia semnaturii in format electronic aplicatia va putea utiliza si un pad de semnatura, daca beneficiarul va cere acest lucru.

2.3.2.3.2 Aplicația de interfațare cu sistemul TACHOnet

Aplicatia de interfațare și comunicare cu sistemul TACHOnet are rolul de a permite operatorilor MD-CIA sa verifice starea unei cartele tahografice in tarile membre ale Uniunii Europene sau de a informa autoritatile CIA corespunzatoare despre modificarea starii unei cartele pe teritoriul Republicii Moldova.

Aceasta consta intr-un program server care ruleaza fara intervenția operatorului uman si ofera urmatoarele functionalitati principale:

- preia din baza de date a MD-CIA mesajele de interogare postate de catre aplicatia web de operare a MD-CIA si le trimite catre sistemul TACHOnet
- raspunde la interogarile venite din sistemul TACHOnet pe baza informatiilor stocate in baza de date a MD-CIA
- proceseaza raspunsurile venite din sistemul TACHOnet si actualizeaza corespunzator baza de date a MD-CIA

Comunicarea cu Aplicatia de Interfata Web se realizeaza prin intermediul bazei de date a MD-CIA. Deasemeni, crearea mesajelor de raspuns care se vor trimite

ca raspuns la interogarile venite de la serverul TACHOnet se realizeaza pe baza informatiilor existente in baza de date MD-CIA.

Comunicatia cu serverul TACHOnet se realizeaza prin intermediul retelei sTESTA. ANTA este responsabilă de realizarea protocolului de cooperare cu ARR pentru asigurarea accesul la rețeaua sTESTA. Protocolul de comunicatie utilizat este HTTPS, autentificarea si securizarea canalului de comunicatie realizandu-se mutual cu ajutorul certificatelor digitale. Pentru obtinerea certificatelor digitale necesare conectarii la serverul TACHOnet este folosita procedura descrisa in documentul "TACHOnet - Network and Security Reference Guide, V1.10".

Aceasta aplicatie foloseste modulul de logare si notificare care permite logarea de mesaje de audit si eroare si trimiterea de notificari prin e-mail la aparitia evenimentelor critica in rularea aplicatiei. Acest modul este descris in sectiunea "Modulul de logare si notificare".

Aplicatia de comunicare cu sistemul TACHOnet este compusa din trei componente principale, acestea ruland in paralel, lucru care garanteaza utilizarea eficienta a resurselor hardware disponibile si asigurarea unui raspuns in timp real la cererile pe care trebuie sa le proceseze. Cele trei componente sunt:

- Componenta de preluare mesaje
- Componenta de procesare mesaje
- Componenta de trimitere mesaje

Componenta de preluare mesaje are rolul de a primi mesajele de interogare de tipul TCN2MS_*_Req sau mesaje de raspuns de tipul TCN2MS_*_Res venite de la sistemul TACHOnet. Acest lucru se realizeaza prin initializarea unui server care primeste conexiuni HTTPS pe portul standard 443. In cazul preluarii unui mesaj de interogare de tipul TCN2MS_*_Req acesta va fi stocat in baza de date pentru o procesare ulterioara de catre componenta de procesare mesaje. In cazul preluarii unui mesaj de raspuns de tipul TCN2MS_*_Res, acesta va fi decodificat si interpretat (de exemplu: se va actualiza starea unei cartele, se va permite continuarea procesului de emitere cartela, etc.).

Componenta de procesare mesaje are rolul de a scana periodic baza de date pentru a gasi mesaje noi neprocesate. Acestea mesaje sunt fie interogari venite din sistemul TACHOnet, pentru care va compune un mesaj de raspuns XML de tipul MS2TCN_*_Res pe care il va stoca in baza de date, fie mesaje de interogare de la aplicatia web de operare a MD-CIA, pentru care va trebui sa compuna mesajele XML de tipul MS2TCN_*_Req pe care il va stoca in baza de date.

Componenta de trimitere mesaje are rolul de a verifica in baza de date daca exista mesaje care trebuiesc trimise catre sistemul TACHOnet. Acestea sunt de tipul MS2TCN_*_Req si MS2TCN_*_Res. In cazul gasirii unui mesaj, se va initializa o conexiune HTTPS cu serverul central al TACHOnet si i se va trimite mesajul respectiv.

Fiecare dintre cele trei componente ale aplicatiei sunt configurabile, pentru fiecare dintre ele existand o sectiune dedicata in fisierul de configurare global al aplicatiei. Acest fisier este de tipul XML, si permite configurarea urmatorilor parametri:

- intervalele de timp la care se verifica existenta unei cereri care trebuie procesata
- numarul de thread-uri de lucru ale fiecarei componente
- certificatele si cheile private pentru realizarea autentificarii mutuale cu serverul central al TACHOnet

Acesti parametri de configurare permit ajustarea aplicatiei pentru utilizarea optima a resurselor hardware disponibile. Pe un sistem de lucru cu resurse hardware modeste aceasta aplicatie poate procesa peste 10 cereri pe secunda.

Aplicatia de comunicare cu sistemul TACHOnet respecta in totalitate specificatiile stipulate in urmatoarele documente:

- "TACHOnet - XML Messaging Reference Guide, V1.5"
- "TACHOnet - Network and Security Reference Guide, V1.10"
- "TACHOnet – Global Business Analysis, V01_30"
- "TACHOnet – Software Requirements Specifications, V01_00"

Prin prezenta ofertă CERTSIGN propune utilizarea aplicatii de interfaţare şi comunicare cu sistemul TACHOnet utilizată şi în prezent. Astfel se asigura continuitatea schimbul de informatii cu autoritatile nationale din celelalte state participante in sistemul tahografului digital prin intermediul serviciului TACHOnet încă din prima zi după intrarea în vigoare a contractului.

CERTSIGN va realiza pe durata contractului upgrade-ul aplicatiilor software pentru verificarea si validarea cererilor aplicantilor la nivel european prin interfatarea cu sistemul TACHOnet, prin implementarea tuturor noilor specificatii elaborate la nivel European.

Produsul „tachoSAFE" incluzând şi componenta TACHOnet este dezvoltat de CERTSIGN, fapt demonstrat prin certificatul de înregistrare al acestui produs la ORDA, anexat prezentei oferte. CERTSIGN fiind dezvoltatorul soluției este perfect capabil sa asigure upgrade-ul aplicatiilor software pentru verificarea si validarea cererilor aplicantilor la nivel european, prin interfatarea cu sistemul TACHOnet.

2.3.2.3.3 Aplicatia de interfatare si comunicare cu MD-CP

Avand in vedere ca cele doua autoritati MD-CIA si MD-CP se gasesc in locatii fizice diferite si apartin de institutii diferite se foloseste un canal de comunicatie securizat care asigura transmiterea datelor in ambele sensuri: de la CIA catre CP si de la CP catre CIA.

Pentru realizarea acestui obiectiv la MD-CIA ruleaza aplicatia de interfatare si comunicatie intre MD-CIA si MD-CP (Comm_CIA_CP), iar la MD-CP ruleaza o

aplicatie similara, numita aplicatia de interfatare si comunicatie intre MD-CP si MD-CIA (Comm_CP_CIA).

Pentru a asigura securizarea schimbului de date dintre MD-CIA si MD-CP cele doua aplicatii de comunicare si interfatare de la MD-CIA si MD-CP realizeaza criptarea canalului de comunicatie si se autentifica mutual una la cealalta. In acest scop aplicatiile de la MD-CIA, respectiv MD-CP, utilizează certificate digitale emise de catre infrastructura PKI a CERTSIGN.

Aplicatia Comm_CIA_CP realizeaza urmatoarele functii:

- Extrage din baza de date a MD-CIA cererile de emitere de cartele tahografice personalizate validate si aprobate pentru executie de catre MD-CIA. Sunt preluate din baza de date doar datele strict necesare personalizarii cartelelor tahografice;
- Impacheteaza datele intr-un format acceptat de canalul de comunicatie;
- Aplica o semnatura digitala si o marca temporala asupra datelor inainte de a fi trimise. Marca temporala este obtinuta folosind serverul de timestamp al infrastructurii PKI de support.
- Creaza un canal de comunicatie sigur intre CIA si CP prin crearea unei conexiuni SSL;
- Transmite datele semnate electronic pe canalul de comunicatie creat in prealabil de la CIA catre CP (transmiretea cererilor);
- Asteapta un timp limitat (configurabil) raspunsul de confirmare de la CP si daca s-a primit un mesaj de eroare sau nu s-a receptionat mesajul de confirmare in intervalul de timp prestabilit, se retransmite mesajul. Retransmiterea poate fi incercata de un numar maxim configurabil de ori, dupa care se genereaza un mesaj de notificare catre administratorii de system.
- Accepta conexiuni SSL (securizate) in urma autentificarii mutuale cu aplicatia Comm_CP_CIA
- Verifica integritatea datelor primite de la CP prin verificarea semnaturii digitale aplicate datelor
- Analizeaza datele primite de la MD-CP si actualizeaza corespunzator baza de date a MD-CIA daca este cazul (etapa de procesare a cererilor, starea cardurilor corespunzatoare, mesaje de confirmare, etc);
- Trimite la MD-CP un mesaj de confirmare a primirii mesajului in care se specifica si succesul sau esecul receptionarii mesajului si in caz de esec un cod de eroare.
- Toate mesajele de transmis pe canal sunt semnate digital si marcate temporal inainte de a fi trimise.
- La mesajele de confirmare nu se raspunde cu alt mesaj de confirmare.

Astfel, acest modul va asigura transmiterea in ambele sensuri CIA->CP si CP->CIA a datelor necesare personalizarii cartelelor si monitorizarii starii cererilor de

emitere cartele personalizate cit si a starii cartelelor corespunzatoare, asigurand integritatea si confidentialitatea acestor date.

Toate operatiile si tranzactiile efectuate de aceasta aplicatie vor fi logate in fisiere speciale de audit folosind modulul de logare si notificare ce va fi integrat in aplicatie. Vor fi, de asemenea, logate toate eventualele erori.

Prezenta logurilor are ca scop oferirea de informatii de accounting administratorului sistemului precum si informatii de debug daca acestea vor fi necesare in fazele de implementare si support tehnic. Informatiile logate vor fi intr-un format customizabil si in mare parte vor fi conforme cu formatele de logare ale principalelor aplicatii cunoscute pe Linux.

2.3.2.3.4 Modulul de logare si notificare

Modulul de logare si notificare este o componenta comuna utilizata de catre toate aplicatiile MD-CIA si ofera urmatoarele functionalitati:

- permite logarea de mesaj de audit
- permite logarea de mesaje de eroare
- permite logarea de mesaje de debug
- permite trimitere mesaje e-mail de notificare administratorilor in cazul evenimentelor critice

Mesajele cu logurile de audit, erori si debug sunt stocate in fisiere de pe disc. Pentru asigurarea confidentialitatii, aceste fisiere pot fi criptate utilizand cheile publice ale certificatelor auditorilor si accesul la ele este permis numai acestora. Pentru asigurarea integritatii, aceste fisiere pot fi semnate utilizand cheia privata a aplicatiei respective.

Mesajele continute in aceste fisiere sunt in limba Romana.

Fisierele de audit inregistreaza toate operatiile efectuate si rezultatele lor. Acestea contin: numele (ID-ul) operatorului, tipul de operatie efectuata si codul de succes sau eroare corespunzator si data la care a efectuat operatia. Prin configurare, modulul poate loga orice alte informatii, la cererea beneficiarului.

Fisierele de eroare inregistreaza numai mesajele de eroare aparute in urma operatiilor efectuate. Acestea contin: numele (ID-ul) operatorului, codul de eroare si mesajul text care descrie motivul si locul unde a aparut eroarea si data la care a efectuat operatia. Prin configurare, modulul poate loga orice alte informatii specifice erorii, la cererea beneficiarului.

Fisierele de debug inregistreaza informatii suplimentare necesare in faza de testare si implementare la beneficiar. In plus, acestea sunt utilizate in cazul interventiilor tehnicienilor CERTSIGN la interventiile de suport tehnic. Fisierele de debug nu sunt create de catre aplicatie decat pe perioada interventiei tehnice.

Componenta de logare utilizeaza un mecanism de rotatie a log-urilor care permite ca la un interval de timp predefinit fisierele cu logurile curente sa fie

arhivate, semnate, criptate si mutate manual sau automat pe un mediu de stocare extern (CD, DVD, NAS, FTP, etc.).

Functionalitatea de trimitere mesaje de notificare permite aplicatiilor care utilizeaza modulul de logare sa trimita un e-mail sau SMS atunci cand s-a detectat un anumit eveniment in sistem. Acest mecanism permite alertarea administratorilor de securitate despre incidentele de securitate si a administratorilor de sistem despre eventualele erori sau cazuri exceptionale aparute in functionarea aplicatiei pentru a permite interventia rapida a acestora.

Componenta de logare si notificare este configurabila, parametrii de functionare fiind cititi dintr-un fisier de pe disc in format XML. Acestia specifica:

- locatia fisierelor de audit (logare) de pe disc
- intervalul de rotatie a fisierelor de audit (logare)
- certificatele auditorilor cu care sunt criptate fisierele audit (logare)
- scenariile care duc la inserarea de inregistrari in fisierele speciale de audit
- continutul inregistrarilor de audit pentru fiecare situatie in parte
- filtrele de notificari

Solutia propusă asigură backup-ul fisierelor speciale de audit.

Solutia propusă asigură integritatea și autenticitatea fisierelor speciale de audit prin semnatură digitală.

2.3.2.4 Securitatea sistemului MD-CIA

2.3.2.4.1 Securitate aplicații

Securitatea aplicatiei web de operare a MD-CIA, numita si aplicatia web de inregistrare, emitere si gestiune a cartelelor tahografice, se realizeaza prin:

- Folosirea conexiunilor criptate (SSL) intre clientii aplicatiei (browserele web) si serverul web din datacenter-ul MD-CIA;
- Autentificarea mutuala pe baza de certificate digitale intre operatorii aplicatiei si serverul web;
- Implementarea unui sistem de management a operatorilor si rolurilor acestora in cadrul aplicatiei. S-a stabilit o politica stricta de roluri la nivelul aplicatiei bazata pe certificate digitale. Astfel utilizatorul logat in aplicatie cu un certificat corespunzator unui anumit rol va avea acces numai la functionalitatile specifice rolului respective;
- Logarea in fisiere speciale de audit a tuturor incercarilor de accesare aplicatiei si a tuturor actiunilor desfasurate in cadrul aplicatiei de catre utilizatori, si notificarea administratorilor prin email si/sau SMS in cazul evenimentelor deosebite. In acest scop se foloseste modulul de logare si notificare.

Astfel, la nivelul accesului operatorilor si administratorilor la aplicatie, se foloseste un sistem de chei publice şi de certificate digitale X.509 asigurat de catre infrastructura PKI a CERTSIGN. Operatorii birourilor de inregistrare accesează aplicaţia web a MD-CIA de pe statiile de lucru autentificandu-se utilizand certificate digitale stocate pe token-uri criptografice USB. Token-ul criptografic este utilizat ca mecanism de autentificare pe baza a doi factori: ceva ce utilizatorul poseda – token-ul criptografic pe care se afla certificatul digital, si ceva ce utilizatorul cunoaste – codul de acces la tokenul criptografic. Pentru a accesa aplicaţia web a MD-CIA utilizatorul deschide sesiunea pe statia de lucru iar atunci cand i se solicita sa se autentifice foloseste token-ul criptografic, pentru a prelua automat de pe statia de lucru informatiile de sesiune, a semna electronic, folosind certificatul digital aflat pe dispozitiv, si transmite catre sistemul de autentificare un identificator al sesiunii pe baza caruia, dupa verificarea informatiilor primite si a certificatului digital, este permis accesul în aplicaţie de pe staţia de lucru.

De asemenea, si serverul web are un certificat digital de server necesar criptarii conexiunii si autentificarii la client.

Pentru desfasurarea activitatilor specifice MD-CIA, operatorii birourilor MD-CIA, se conecteaza la aplicatie folosind doar autentificarea mutuala cu certificatele digitale stocate pe token-urile criptografice.

Fiecare operator este caracterizat de un "rol de acces". Aplicatia limiteaza drepturile operatorilor in aplicatie conform cu rolurile definite. Rolul de acces permite operatorului respectiv să efectueze numai anumite operaţii, de exemplu: sa administreze sistemul, sa primeasca cererile de carduri, sa inregistreze modificari ale starilor cardurilor, sa initializeze trimiterea cererilor de carduri catre CP, etc.

2.3.2.4.2 Securitate retea

Securitatea la nivel de retea este realizata prin utilizarea unui echipament din noua generatie de platforme Unified Threat Management (UTM); acesta asigura functii avansate de **firewall/switching/routing** , putand fi extins (optional) cu functionalitati de tip **intrusion prevention** ,antivirus, antispam sau **content filtering**.

Echipamentul folosit este un Juniper SRX210 (Juniper Networks) care asigura o arhitectura modulara si ofera optiunea de adaugare module WAN (ISDN, ADSL, E1) pe langa interfetele standard (8x10/100 Mbps, 2x10/100/1000 Mbps).

SRX210 asigura functionalitati avansate pentru securizarea unei retele precum protectie atacuri de retea, protectie DoS si DDoS, reasamblare TCP pentru protectia pachetelor fragmentate, protectie la atacuri tip forta bruta, protectie SYN cookie, protectie IP spoofing bazata pe zone, protectie la pachete malformate, suport pentru tunele VPN IPSec (criptare DES, 3DES, AES si hashing MD5, SHA1).

Legatura intre MD-CIA si MD-CP se realizeaza prin tunel criptat VPN IPSec. Atat echipamentul SRX210 cat si echipamentele de comunicatii din locatia MD-CP ofera suport pentru gestionare traficului (Guaranteed bandwidth, Maximum bandwidth, Priority-bandwidth utilization, DiffServ stamp), fiind posibila

rezervarea unei latimi de banda pentru interconectarea MD-CIA cu MD-CP, sau MD-CIA cu reteaua de conectare in sTESTA.

Sistemul MD-CIA este monitorizat continuu prin intermediul unei infrastructuri de monitorizare. Sistemul de monitorizare interogheaza sistemele MD-CIA in mod activ pentru a asigura o functionare in conditii optime atat a sistemelor de operare cat si a aplicatiilor specifice care ruleaza pe acestea. Sunt monitorizati o serie de parametrii ai sistemului de operare cum ar fi: memoria RAM, incarcarea pe sistem, numarul de procese din sistem, utilizarea disk-ului dar si aplicatiile specifice platformei MD-CIA.

Atacurile informatice sau problemele de functionare constituie incidente care trebuie tratate corespunzator. Fiecare incident este inregistrat intr-un registru de incidente electronic, inregistrandu-se pentru fiecare incident urmatoarele tipuri de informatii: numarul incidentului, data incidentului, descrierea incidentului, cauza, solutia, masuri corective, data solutionarii si in functie de severitatea acestuia, entitatile instiintate (de exemplu MD-A).

2.3.2.4.3 Securitate fizica

Echipamentele dedicate sistemului MD-CIA sunt localizate în data center-ul CERTSIGN, într-un mediu de producţie special amenajat, pentru a oferi cele mai bune condiţii de funcţionare şi administrare, atât din punct de vedere operaţional şi din punct de vedere al securităţii.

Centrul de date se află în sediul CERTSIGN aflat în Bulevardul Tudor Vladimirescu, nr. 29 A, AFI Tech Park 1, Sector 5, Bucureşti, România, CP 050881. Spaţiul este corespunzator din punct de vedere al iluminatului, aerisirii, climatizării şi alimentării electrice.

Politicile de acces în incinta utilizate pentru echipamentele MD-CIA sunt gestionate separat şi sunt diferite de politicile de acces în celelalte spaţii.

Spaţiul se află într-o clădire care este amplasată într-un perimetru închis cu gard şi dotat cu echipamente de control acces pentru autovehicule, având ca dispozitiv de blocare bariere auto. Accesul autovehiculelor se face prin control dual, cartele de proximitate si agenti de paza. Accesul pietonal este de asemenea controlat la intrarea în perimetru de catre agentii de paza. Toate caile de acces catre locatia ocupata de certSIGN sunt controlate dual, cu echipamente de control acces si cu agenti de paza.

Spaţiul alocat CERTSIGN este prevazut cu agenţi de pază proprii şi este organizat pe trei nivele de securitate:

- la primul nivel are acces tot personalul CERTSIGN, pe bază de cartele de proximitate, purtand fotografia angajatului si datele de identificare ale firmei (aria delimitată este de tip „zonă administrativă");
- al doilea nivel este destinat „zonelor tehnice";
- al treilea nivel este format de „zonele de securitate-clasă 2". Accesul in aceste zone este permis pe baza acelorasi cartele de proximitate.

Incintele astfel definite, unde se instalează echipamentele de procesare date sau se păstrează documente, sunt protejate la intruziune prin instalarea de dispozitive de detecţie adecvate, care fac parte dintr-un subsistem de detecţie la efracţie. Accesul în fiecare zona de securitate este permis numai persoanelor autorizate de administratorul de securitate, prin programarea corespunzatoare a sistemului de acces fizic.

În vederea asigurării unui control complet al circulaţiei personalului propriu şi al vizitatorilor, punctele de control acces în zonele de securitate sunt supravegheate cu ajutorul unui subsistem de TVCI, care permite vizualizarea în timp real a imaginilor culese, înregistrarea acestora, căutarea şi redarea imaginilor de la anumite momente de timp.

Conform reglementărilor în vigoare, toate încăperile şi holurile de circulaţie fac obiectul detecţiei la incendiu, detectie asigurata printr-un sistem de detecţie şi semnalizare. Accesul grupelor de intervenţie la incendiu va fi permis şi supervizat de personalul firmei de pază, cu anunţarea administratorului de securitate al CERTSIGN.

Sistemul de securitate pentru cladirile centrului de personalizare cuprinde: un sistem de control al accesului, un sistem CCTV (pentru supraveghere video), proceduri de a monitoriza si raporta incidentele CCTV, sisteme aritiefractie si antiincendiu.

Aplicatia de management a securităţii sistemului fizic contine o baza de date in care se înregistreaza toate evenimentele din sistem (intrari/iesiri, alarme). Aplicatia contine un modul de rapoarte, utilizat de catre administratorul de securitate (sau de catre o persoana autorizata de acesta), dupa cum urmeaza :

- rapoarte de prezenta (listeaza perioadele de timp petrecute in interiorul obiectivului pentru fiecare persoana in parte, cu posibilitatea de filtrare pe departamente/persoane si pe o anumita perioada de timp (zile/saptamani/luni);
- rapoarte de evenimente de acces, de tipul "cine, când, unde", cu posibilitatea de selectie pe anumite filtre şi într-o anumita perioada de timp ;
- rapoarte cu tentativele de acces nepermise, referitoare la situatiile cand anumite persoane incearca sa acceseze un anumit filtru la care nu au dreptul sau cand se folosesc alte cartele decat cele introduse in sistem ; acestea se asociază cu imaginile înregistrate de subsistemul de TVCI .

În scopul asigurării pazei şi securităţii bunurilor existente şi a informaţiilor există un post de pază permanent, 24/24 ore, asigurat cu agent de pază, amplasat la intrarea obiectivului, în interiorul acestuia, cu misiunea de a permite accesul autorizat în incintă a salariaţilor si a vizitatorilor. În cazul unui incident, după declansarea alarmei sosesc in maximum 30 de secunde echipajele de interventie.

Accesul în obiectiv este controlat printr-un sistem electronic prevăzut cu uşi cu broaşte electromagnetice ce pot fi acţionate de către cititoarele de cartele de proximitate. Cartelele de proximitate sunt personalizate prin inscripţionarea unei serii unice personalizarea acestora fiind cotrolată de administratorul de securitate.

2.3.2.4.4 Securitate cibernetică

Evaluarea vulnerabilităţilor

CERTSIGN va realiza Evaluarea Vulnerabilitatilor sistemului MD-CIA, proces in cadrul caruia se va evalua nivelul de risc cu privire la fiecare vulnerabilitate identificata si se vor face recomandari de remediere.

Serviciile de evaluarea vulnerabilităţilor ofertate în prezentul document vor fi livrate de către experţi în acest domeniu. Acest serviciu presupune realizarea mai multor tipuri de acţiuni în mod recurent, respectiv: identificarea sistemelor informatice ce trebuie scanate, prioritizarea acestora, scanarea, revizuirea rezultatelor obţinute, evalurea vulnerabilităţilor identificate şi acordarea unui indice de risc, formularea de recomandări de remediere, retestare.

În livrarea serviciului se vor utiliza instrumente automate de scanare a sistemelor MD-CIA. Aplicatiile si metodele de realizare a evaluarii sunt de ultima generatie si sunt cotate ca tehnologii de varf. Modul in care se va derula evaluarea nu va impacta in niciun fel performantele sistemelor informatice evaluate si va permite descoperirea de vulnerabilitati la nivel de: sistem de operare, retea LAN, aplicatii, aplicatii web, baze de date, etc.

Ultima etapă din fiecare iteraţie a serviciului de evaluării de vulnerabilităţi va fi formularea de recomandări care să permită realizarea corecţiilor necesare pentru remedierea breşelor de securitate.

Teste de penetrare

CERTSIGN va livra servicii de tipul Penetration Testing pentru sistemul MD-CIA, care permit testarea nivelului de securitate al infrastructurii tinta prin identificarea şi validarea vulnerabilităţilor la nivel de reţea, sistem de operare, aplicaţii, inclusiv cele web servicii.

Testele de penetrare se vor derula cu ajutorul unor specialişti certificaţi, care vor utiliza aplicaţii comerciale dedicate de ultimă generaţie.

De asemenea, CERTSIGN desfăşoară testele de penetrare în baza unor proceduri ce au fost concepute prin respectarea standardelor şi recomandărilor în domeniu (SANS, NIST, ENISA, etc.).

În cadrul metodologiei de lucru cu privire la serviciile de penetration test au fost cuprinse următoarele etape:

- realizarea unui penetration test plan, care va stabili tipul de pentest care se va realiza (black box – din exteriorul reţelei, white box – din interiorul reţelei), sistemele care vor fi cuprinse în iteraţia respectivă de pentest, prioritizarea

acestora, intervalul de realizare al testelor și durata acestora, strategia de comunicare în cadrul echipei de lucru, etc. De asemena, planul de penetration test va mai include o analiză de proiect la nivelul echipei CERTSIGN în care se va stabili: membrii echipei de pentest, scenariile de testare, tool-urile utilizate.

- stabilirea modului în care se va face gestionarea datelor/informațiilor sensibile ce vor fi descoperite cu privire la infrastructura MD-CIA, respectiv: colectarea datelor și stocarea lor într-o formă sigură.

Fiecare pentest in parte se va incheia cu intocmirea unui raport in cadrul carula vor fi cuprinse toate vulnerabilitatile identificate si recomandari pentru remedierea acestora.

Asigurarea reacției la atacuri informatice

CERTSIGN va livra pentru sistemul MD-CIA, servicii de reactie la atacuri informatice prin intermediul unor specialisti dedicati acestei activitati care vor realiza:

- Confirmarea atacului informatic
- Analiza probelor colectate
- Stabilirea cauzelor
- Evaluarea pagubelor
- Identificarea tuturor victimelor in reteau compromisa
- Sanitizarea retelei
- Formularea unui raport de incident

Activitatile de raspuns la incident au drept scop eradicarea unei infectii din cadrul retelei intr-un timp optim astfel incat sa fie diminuate pagubele.

Serviciile ofertate vor fi livrate conform unor proceduri de lucru interne care au fost concepute prin respectarea recomandărilor (SANS) și standardelor în domeniu (NIST Special Publication 800-137) astfel încât să se poată furniza un timp de reacție redus pentru a iniția răspunsul la potențialele incidente de securitate cibernetică.

Monitorizarea sistemelor

CERTSIGN va asigura servicii de monitorizare a sistemelor, furnizate prin intermediul unor experți specializați (analiști de securitate) în acest domeniul. Serviciul va realiza identificarea în mod proactiv și eficient a potențialelor amenințări informatice prin monitorizarea proactivă și continuă a activității care impacteaza sistemele informatice protejate ale MD-CIA.

Serviciile CERTSIGN respectă standardele si recomandările în domeniu impuse de organisme recunoscute precum: ENISA, SANS, Trusted Introducer (CERTSIGN este membră acreditată a comunității), NIST.

Prin mecanisme dedicate se va realizeaza corelarea evenimentelor astfel încât să determine generarea unor alerte/alarme cu privire la amenințările identificate in cadrul sistemului MD-CIA.

2.3.3 MD-CP

Una din componentele de bază ale sistemului national de emitere de cartele tahografice este centrul de personalizare, MD-CP. Sistemul centrului de personalizare, corespunzator MD-CP, este deținut de CERTSIGN S.A. Acestsa se află în sediul CERTSIGN din Bulevardul Tudor Vladimirescu, nr. 29 A, AFI Tech Park 1, Sector 5, București, România, CP 050881.

Serviciul de personalizare a cartelelor tahografice va fi furnizat de catre Asociere. Autoritatea de personalizare a cartelelor tahografice, MD-CP, va fi operată de către CERTSIGN. Procesul de personalizare al cartelelor tahografice se desfășoara integral în centrul de personalizare al CERTSIGN.

Stocarea, gestiunea si personalizarea efectiva a cartelelor tahografice se face in cadrul centrului de personalizare MD-CP a carui descriere functionala este facuta in acest capitol.

Sistemul centrului de personalizare a cartelelor tahografice al CERTSIGN respecta in totalitate cerintele AETR și ale Reglementarii Comisiei Europene (CE) 1360/2002, Anexa IB cat și toate celelalte cerinte si reglementari Europene in domeniu. Infrastructura informatica a MD-CP constă intr-un mediu securizat in care sunt amplasate serverele si calculatoarele centrului de personalizare și toate echipamentele aferente incluzând și echipamentele de personalizare carduri.

Principalele functionalitati acoperite de solutia de MD-CP propusa in cadrul acestei oferte sunt urmatoarele:

- Interfatarea cu sistemul tachoSAFE CIA a MD-CIA pentru a prelua cererile de personalizare a cartelelor tahografice;
- Interfatarea cu sistemul tachoSAFE CA a MD-CA implementat si gazduit de catre CERTSIGN pentru certificarea cheilor criptografice care sunt folosite pentru personalizarea cartelelor tahografice;
- Personalizarea efectiva a cartelelor tahografice din punct de vedere optic si electric (chip), pe baza cererilor primite din partea MD-CIA
- Generarea si gestiunea securizata a cheilor criptografice destinate cartelelor tahografice;
- Generarea si gestiunea securizata a informatiilor de PIN destinate cartelelor tahografice de workshop;
- Controlul calitatii cartelelor tahografice personalizate;
- Gestionarea stocurilor de materiale necesare personalizarii cartelelor tahografice (cartele blank, cartele defecte, consumabile, etc.);
- Gestiunea tuturor informatiilor despre cartelele tahografice personalizate, in curs de persoanlizare sau care urmeaza a fi personalizate;

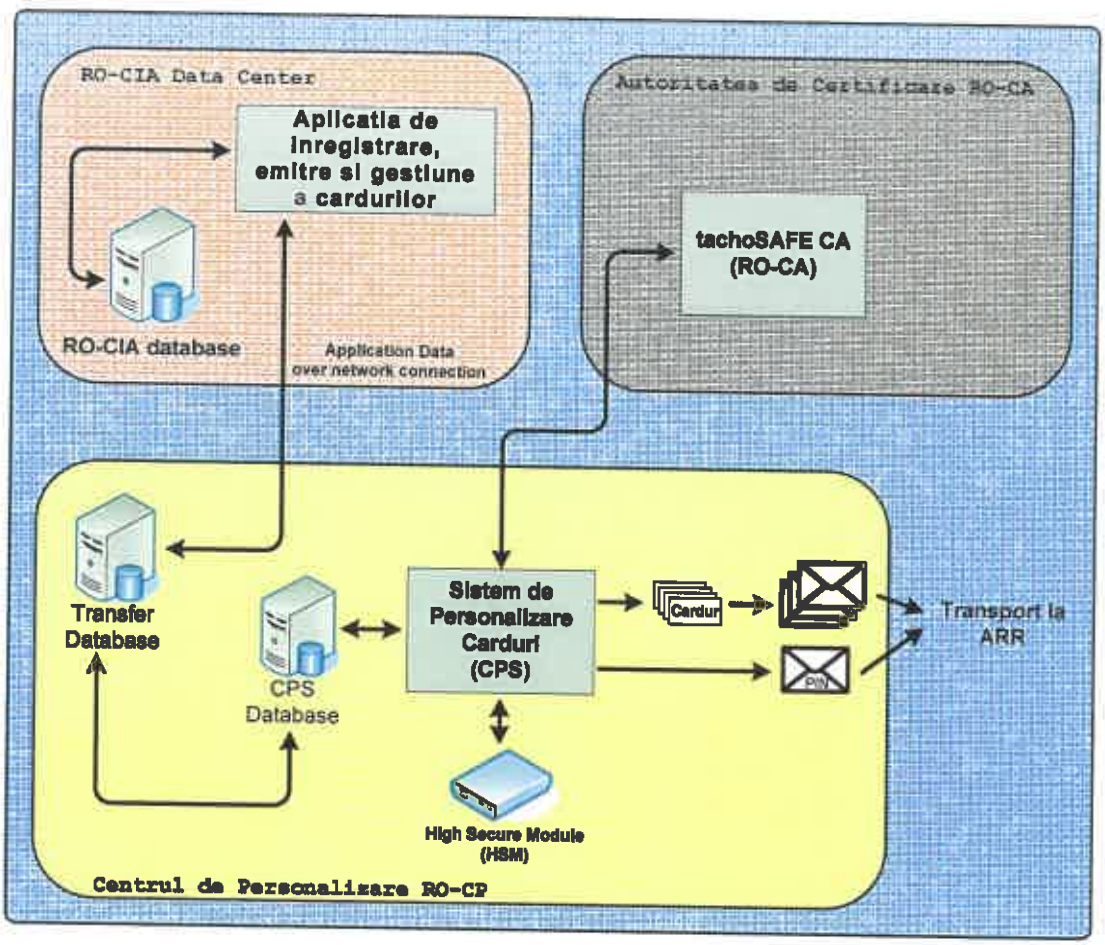
- Furnizarea de statistici si rapoarte despre cartelele tahografice personalizate sau in curs de personalizare;
- Asigurarea tuturor conditiilor de functionare optima, din punct de vedere al securitatii fizice si logice necesare in cadrul procesului de personalizare a cartelelor tahografice.
- Asigura stergerea securizata a datelor personale ale posesorilor de carduri din baza de date la o perioada de timp configurabila, implicit setata la 30 de zile de la primirea acestora de la MD-CIA.

CERTSIGN va asigura personalizarea cartelelor tahografice corespunzătoare comenzilor ANTA în maxim 2 zile lucratoare de la primirea datelor de personalizare de la MD-CIA.

Având in vedere faptul că în perioada de derulare a contractului, 2015-2019, la nivelul Uniunii Europene va fi introdusă noua generație de tahografe digitale și noua generație de carduri pentru tahograful digital care vor include noi mecanisme criptografice și o structura modificata a sistemului de fisiere, CERTSIGN va upgrada sistemul centrului de personalizare, fără costuri suplimentare pentru autoritatea contractantă, pentru a răspunde noilor cerințe ale Uniunii Europene și a fi capabilă să personalizeze noua generație de cartele pentru tohograful digital. Acest upgrade se va face fără a afecta procesul de producție și personalizare a cartelelor tahograf, CERTSIGN asigurând personalizarea și livrarea fără întrerupere a cartelelor tahografice personalizate către ANTA pe toată durata contractului.

2.3.3.1 Arhitectura MD-CP

Din punct de vedere arhitectural, sistemul de emitere de cartele tahografice este descris de figura urmatoare:



Fluxul de personalizare a cartelelor tahografice contine urmatoarele operatiuni:

1. **Primirea cererilor de la MD-CIA**. Cererile de personalizare sunt primite de MD-CIA, o data pe zi. Cererile sunt preluate in mod bulk si sunt stocate intr-o baza de date intermediara, de transfer intre MD-CIA si MD-CP. În momentul primirii cererii de al ANTA aplicația MD-CP de import (Import Client) verifică validitatea datelor de personalizare primate și în cazul în care există erori in datele trimise, CERTSIGN notifică ANTA în maxim 1 zi lucratoare de la primirea datelor de la MD-CIA pentru a putea fi corectate în timp util.
2. **Pregatirea datelor** pentru personalizarea cartelelor tahografice, process care include urmatoarele etape:
   a. Datele de personalizare sunt stocate intr-o baza de date centrala a sistemului de personalizare;
   b. Se efectueaza verificarea cererilor primite de la MD-CIA din punct de vedere al corectitudinii datelor si formatelor;

c. Genereaza chelle RSA pentru cartelele tahografice, utilizand un dispozitiv criptografic hardware de tip HSM, acreditat FIPS 140-2 level 3;
d. Genereaza cereri de certificate catre MD-CA prin intermediul aplicatiei de interfatare cu MD-CA. Primeste certificatele corespunzatoare de la MD-CA;
e. Genereaza un mesaj de confirmare catre MD-CIA confirmand catre acesta ca datele primite sunt gata de a fi personalizate pe cartelele tahografice;
f. Pentru cartelele de workshop, genereaza intr-un mod securizat PIN – urile. Pentru acest lucru utilizeaza dispozitivul HSM, acreditat FIPS 140-2 level 3.
g. Pregateste forma finala a lotului de date care urmeaza a fi personalizate pe cartelele tahografice.

3. **Personalizarea** cartelelor tahografice. In acest pas este realizata personalizarea optica si electrica a cartelelor tahografice. Pentru aceasta operatie, aplicatia de personalizare se interfateaza printr-un modul dedicat cu masinile de personalizare (imprimantele de carduri) care realizeaza perosonalizarea atat din punct de vedere grafic (optic) prin gravare laser, cat si personalizarea electrica (logica) a cipului cartelelor.
4. **Controlul calitatii.** Dupa parcurgerea pasului de personalizare optica si electrica a cartelelor tahografice, are loc un pas special de verificare a calitatii cartelelor personalizate. Se foloseste o componenta software speciala numita "QA Client" a sistemului de personalizare "TrackStar" care include atat echipamente hardware, cum ar fi cititoare de carduri cat si software. Aceasta componenta permite, la detectarea unor neconformitati asupra unei cartele personalizate, marcarea acesteia ca fiind defecta si, de asemenea, notificarea in baza de date a sistemului de personalizare pentru a fi efectuata apoi o re-personalizare a informatiilor respective utilizand o alta cartela tahografica. Procedura de verificare a calitatii cartelelor tahografice personalizate se realizeaza pentru fiecare cartela livrata.
5. **Sortarea cartelelor**. Sistemul de personalizare sorteaza toate cartelele conform unor reguli definite la startarea procesului de personalizare. Astfel, la finalul procesului de personalizare a unui set de cartele, acestea se regasesc deja sortate comform criteriilor stabilite de ANTA.
6. **Tiparirea plicurilor si impachetarea.** Odata cu procesul efectiv de personalizare a cartelelor tahografice, sistemul de personalizare creaza in paralel, utilizand o imprimanta dedicata pentru acest lucru, scrisorile insotitoare ale cartelelor, scrisori personalizate cu datele destinatarului cartelei. Cartelele personalizate sunt atasate de aceste scrisori si apoi implicuite in plicuri special personalizate cu insemnele ANTA. Procedura este urmatoarea:
   a. Cartelele tahografice sunt personalizate intr-o anumita ordine, conform unui criteriu de sortare definit la inceputul procesului de personalizare;

b. Scrisorile insotitoare de care vor fi atasate cartelele sunt tiparite in aceeasi ordine. Numarul de identificare al cartelelor, necesar in procesul de sortare, este tiparit de asemenea pe scrisori si va fi vizibil prin fereastra transparent a plicului;
c. Cartelele sunt introduse manual in plicurile corespunzatoare.
d. Plicurile cu cartelele personalizate sunt ordonate dupa criteriile stabilite de ANTA.

7. **Tiparirea PIN-urilor** pentru cartelele de workshop. Sistemul de personalizare pregateste de asemenea scrisorile speciale de PIN pe care sunt tiparite informatiile de PIN asociate cu cartelele de workshop. Caracterele care alcatuiesc PIN-ul efectiv sunt tiparite pe o hartie speciala cu capabilitati de ascundere a informatiilor, de tipul celor utilizate din cazul cardurilor bancare.

Cartelele tahografice personalizate, ataşate scrisorilor însoţitoare şi împlicuite în plicurile special personalizate cu însemnele ANTA, cât şi scrisorile de PIN corespunzătoare cartelelor de workshop împlicuite în acelaşi tip de plicuri special personalizate cu însemnele ANTA, vor fi livrate la sediul ANTA din Republica Moldova mun. Chişinău str. Aleea Gării, 6. In fereastra plicului, pe langa informatiile corespunzatoare posesorului cartelei sau a PIN-ului, este vizibil si numarul cartelei tahografice cat si agentia ANTA unde trebuie sa ajunga.

Pentru fiecare din acesti pasi, se face jurnalizarea actiunilor efectuate astfel incat sa se poata asigura urmarirea pasilor in procesul de personalizare precum si realizarea de statistici si raportari. De asemenea, jurnalele sunt semnate digital utilizand o cheie privata speciala pentru acest scop, asigurandu-se astfel integritatea si autenticitatea acestora in vederea auditarii.

De asemnea exista prevazut mecanism de backup pentru datele critice din sistem. Periodic, se face backup la datele din baza de date interna a MD-CP. Fisierele de backup sunt transportate in mod securizat catre locatia de disaster-recovery. Acestea sunt semnate digital asigurandu-se integritatea si autenticitatea acestor fisiere. Astfel, este asigurata 24 din 24 de ore disponibilitatea datelor din sistem.

2.3.3.2 Gestiunea cheilor criptografice la MD-CP

Scopul sistemului de la MD-CP este asigurarea procesului de personalizare optica si electrica a cartelelor tahografice pentru cererile de personalizare primite de la MD-CIA.

Conform specificatiilor din Reglementarea Comisiei Europene (CE) 1360/2002, Anexa IB, procesul de personalizare a cartelelor tahografice realizeaza:

- generarea perechilor de chei asimetrice RSA destinate cartelelor tahografice pe un dispozitiv HSM, acreditat FIPS 140-2 level 3;

- obtinerea de la MD-CA a certificatelor pentru cartelele tahografice;
- personzalizarea cartelelor cu cheia privata RSA si certificatul asociat;
- obtinerea de la MD-CA a cheii simetrice (KmWC) pentru cartelele de workshop;
- personalizarea cartelelor de workshop cu cheia simetrica (KmWC);
- personzalizarea cartelelor cu MD.C si EUR.PK

Pentru asigurarea managementului cheilor si operatiilor criptografice implicate de procesul de personalizare, sistemul de personzalizare al CERTSIGN utilizeaza un dispozitiv dedicat de tip HSM (Hardware Secure Module), acreditat FIPS 140-2 level 3. Astfel, toate operatiile criptografice sunt executate in interiorul acestui HSM.

In cadrul sistemului de personzalizare al CERTSIGN, perechile de chei RSA destinate cartelelor tahografice sunt generate extern cartelelor, pe dispozativul hardware de tip HSM, acreditat FIPS 140-2 level 3. Pentru fiecare cartela tahografica care se personalizeaza este generata o singura pereche de chei RSA. Perechile de chei sunt pe 1024 de biti si sunt conforme cu cerinte CSM_003, CSM_014 din Reglementarea Comisiei Europene (EC) 1360/2002, Anexa IB, Appendix 11. Cheile publice sunt certificate prin intermediul sistemului autoritatii de certificare tachoSAFE CA al MD-CA dezvoltat, implementat si gazduit in conditiile de securitate cerute prin caietul de sarcini, de catre CERTSIGN. Algoritmul de hash folosit la generarea certificatelor cu care se vor personaliza cartelele tahografice este SHA-1.

Cheia simetrica de workshop (KmWC) este de tip 3DES, de forma (Ka, Kb, Ka), si este conforma cu cerintele Reglementarii Comisiei Europene (EC) 1360/2002, Anexa IB, Appendix 11, cerintele CSM_005, CSM_015, CSM_037. Cheia simetrica de workshop este obtinuta de la MD-CA utilizand protocolul de transport al cheilor simetrice descris de Politica de Certificare a ERCA, versiunea 2.1. Cheia de transport este generata in sistemul de la MD-CP utilizand dispozitivul HSM. Aplicatia de la MD-CP genereaza un Key Distribution Request (KDR) catre MD-CA. Formatul acestei cereri este descris, de asemenea in Politica de Certificare a ERCA, versiunea 2.1, Anexa D. Acesta contine cheia publica de transport a cheii simetrice pentru cartelele de workshop. Dupa ce se obtine raspunsul de la MD-CA, acesta:

- contine un Key Distribution Message (KDM), in formatul descris de Anexa D a Politicii de Certificare a ERCA;
- este decriptat utilizand dispozitivul HSM si cheia privata de transport stocata in HSM;
- cheia simetrica KmWC este stocata in mod securizat pe HSM pentru a fi utilizata apoi la personalizarea cartelelor tahografice.

Informatia de PIN destinata cartelelor tahografice de workshop este generata utilizand tot dispozitivul HSM.

Procesul de personalizare presupune de asemenea inserarea pe cartelele tahografice a informatiei de certificat a MD-CA (MD.C) si chele publica a ERCA

(EUR.PK). Aceste informatii sunt obtinute de la MD-CA fiind stocate in cadrul sistemului de personalizare in mod securizat.

2.3.3.3 Personalizarea cartelelor de test

In scopul obtinerii acreditarilor si certificarilor necesare pentru producerea de cartele tahografice (type approval), sistemul de personalizare propus este capabil sa faca personalizarea cartelelor si in modul „TEST". Sistemul de personzalizare va comunica sistemului tachoSAFE CA de la MD-CA, in cererile de certificate destinate acestor tipuri de cartele, faptul ca trebuie sa obtina certificate de test (semnate cu cheia privata de test a MD-CA) sau certificate de producţie.

2.3.3.4 Interfatarea cu MD-CIA

Avand in vedere ca cele doua sisteme corespunzatoare MD-CIA si MD-CP se gasesc in locatii fizice diferite si apartin de institutii diferite se foloseste un canal de comunicatie securizat care asigura transmiterea datelor in ambele sensuri: de la CIA catre CP si de la CP catre CIA.

Pentru realizarea acestui obiectiv la MD-CP ruleaza aplicatia de interfatare si comunicatie intre MD-CP si MD-CIA (Comm_CP_CIA), iar la MD-CIA ruleaza o aplicatie similara, numita aplicatia de interfatare si comunicatie intre MD-CIA si MD-CP (Comm_CIA_CP).

Pentru a asigura securizarea schimbului de date dintre MD-CP si MD-CIA cele doua aplicatii de comunicare si interfatare de la MD-CP si MD-CIA realizeaza criptarea canalului de comunicatie si se autentifica mutual una la cealalta. In acest scop aplicatiile de la MD-CP si MD-CIA utilizeaza cate un certificat digital X.509, certificatul corespunzator aplicatiei de la MD-CIA fiind emis de catre infrastructura PKI a CERTSIGN.

Aplicatia Comm_CP_CIA realizeaza urmatoarele functii:

- Accepta conexiuni SSL (securizate) in urma autentificarii mutuale cu aplicatia Comm_CIA_CP;
- Verifica integritatea datelor primite de la CIA prin verificarea semnaturii digitale aplicate datelor;
- Analizeaza si valideaza datele primite de la MD-CIA si actualizeaza corespunzator baza de date a MD-CP;
- Trimite la MD-CIA un mesaj de confirmare a primirii mesajului in care se specifica si succesul sau esecul receptionarii mesajului si in caz de esec un cod de eroare;
- Verifica periodic repository-ul MD-CP pentru a gasi modificarile de stare ale cererilor de emitere de cartele tahografice personalizate si ale cartelelor tahografice corespunzatoare. Modificarile gasite sunt trimise catre MD-CIA;
- Impacheteaza datele intr-un format acceptat de canalul de comunicatie;

- Creaza un canal de comunicatie sigur intre intre CP si CIA prin crearea unei conexiuni SSL;
- Transmite datele semnate electronic pe canalul de comunicatie creat in prealabil de la CP catre CIA;
- Asteapta un timp limitat (configurabil) raspunsul de confirmare de la CIA si daca s-a primit un mesaj de eroare sau nu s-a receptionat mesajul de confirmare in intervalul de timp prestabilit, se retransmite mesajul. Retransmiterea poate fi incercata de un numar maxim configurabil de ori, dupa care se genereaza un mesaj de notificare catre administratorii de sistem;
- Toate mesajele de transmis pe canal sunt semnate digital si marcate temporal inainte de a fi trimise;
- La mesajele de confirmare nu se raspunde cu alt mesaj de confirmare.

Astfel, acest modul asigura transmiterea in ambele sensuri CIA→CP si CP→CIA a datelor necesare personalizarii cartelelor si monitorizarii starii cererilor de emitere cartele personalizate cit si a starii cartelelor corespunzatoare, asigurand integritatea si confidentialitatea acestor date.

Toate operatiile si tranzactiile efectuate de aceasta aplicatie sunt logate in fisiere speciale de audit folosind modulul de logare si notificare integrat in aplicatie. De asemenea sunt logate toate erorile care vor apare.

Prezenta logurilor are ca scop oferirea de informatii de accounting administratorului sistemului precum si informatii de debug daca acestea sunt necesare in fazele de implementare si support tehnic. Informatiile sunt logate intr-un format customizabil si sunt conforme cu formatele de logare ale principalelor aplicatii cunoscute pe Linux.

2.3.3.5 Interfatarea cu MD-CA

La nivelul sistemului de MD-CP propus exista o componenta dedicata pentru interfatarea cu sistemul tachoSAFE CA al MD-CA. Prin intermediul acestei componente se emit cereri de certificare catre MD-CA si se primesc certificatele emise de acesta. Componenta de interfatare cu MD-CA comunica cu o componenta similara de la nivelul MD-CA (descrisa in capitolul dedicat pentru MD-CA). Functionalitatile acestei componente sunt identice cu a celei de la nivelul MD-CA.

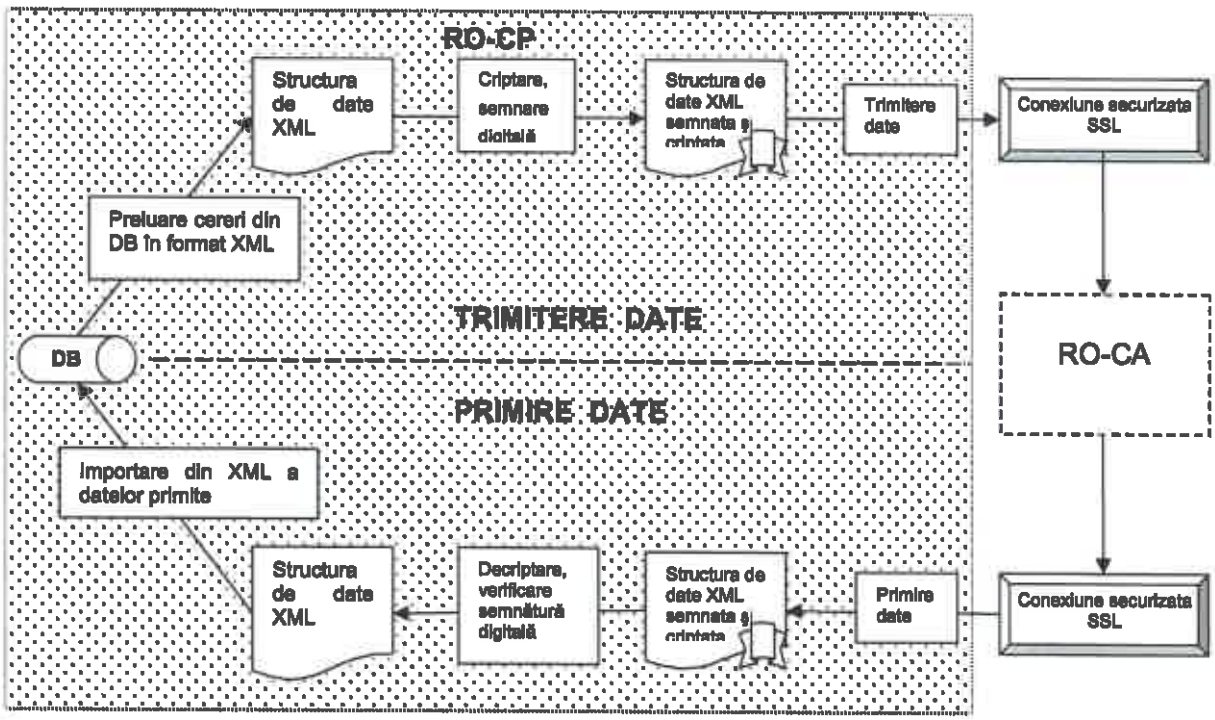
Astfel, avand in vedere ca sistemele celor doua autoritati MD-CA si MD-CP se gasesc in locatii fizice diferite se foloseste un canal de comunicatie securizat SSL cu autentificare mutuala bazata pe certificate digitale care asigura transmiterea datelor in ambele sensuri: de la CA catre CP si de la CP catre CA.

Securizarea schimbului de date dintre MD-CA si MD-CP este realizat de catre cele doua aplicatii de comunicare si interfatare de la MD-CA si MD-CP astfel:

- Semneaza datele de transmis cu cheia privata proprie;

- Cripteaza datele de transmis cu cheia publica a celeilalte aplicatii;
- Comunica prin folosind un canal de comunicatie securizat SSL cu autentificare muluala.

In figura urmatoare este prezentat fluxul de date corespunzator aplicatiei de interfatare cu MD-CA:



Fluxul operatiilor aplicaţiei de intefaţare şi comunicare cu MD-CA este urmatorul:

- Preia cererile de certificate pentru cartelele tahografice din baza de date a MD-CP si le exporta în structuri de date XML. Aceste cereri de certificate vor contine toate datele necesare emiterii certificatului;
- Semneaza structurile XML care conţin cererile de certificate folosind cheia privata proprie;
- Cripteaza structurile XML semnate care conţin cererile de certificate cu cheia publica a aplicatiei corespondente de la MD-CA;
- Impacheteaza structurile de date XML semnate si criptate intr-un format acceptat de canalul de comunicatie realizat prin intermediul dispozitivului hardware de separare zone;
- Transmite datele astfel impachetate către MD-CA utilizând dispozitivul hardware de separare de zone;

- Receptioneaza structuri de date XML semnate si criptate de catre aplicatia corespondenta de la MD-CA. Aceste structuri de date contin certificatele emise de catre MD-CA, in baza cererilor primite de la MD-CP;
- Extrage si reasambleaza datele receptionate de la MD-CA;
- Decripteaza datele primite de la MD-CA;
- Verifica integritatea datelor primite de la MD-CA prin verificarea semnăturii acestora;
- Verificarea structura si consistenta datelor continute in structurile XML receptionate;
- Daca toate verificarile au fost realizate cu success datele receptionate sunt inserate in baza de date a MD-CP pentru a fi folosite la personalizarea cartelelor tahografice.

În structura mesajelor XML schimbate între MD-CP si MD-CA există un câmp care identifică daca cererea de certificat, respectiv certificatul, este de test sau de producţie. Certificatele de test sunt necesare personalizării cartelelor tahografice de test necesare executarii testelor pentru „type approval".

Pentru toate transferurile de date intre MD-CP si MD-CA se genereaza jurnalizari in fisierele speciale de audit folosind modulul de logare si notificare. Sunt logate momentul de timp al evenimentului, id-uri de cereri pentru care s-a realizat transferul, rezultatul transferului (success sau fail), eventualele probleme legate de operatiile criptografice (criptare, semnare, verificare semnatura), erorile de comunicaţie, de integritate a datelor.

2.3.3.6 Masinile de personalizare cartele tahografice

Masinile de personalizare propuse in cadrul acestei oferte sunt Sistemele de Personalizare Desktop Muehlbauer CLP54 şi Muehlbauer Hyprint 50. Vor fi utilizate 2 maşini CLP54 şi o maşină Hyprint 50.

Caracteristicile principale ale unei astfel de masini de personalizare carduri, care fac din aceasta o alegere foarte buna pentru sistemul de personalizare cartele tahografice, sunt urmatoarele:

- o solutie de personalizare smart carduri de ultima generatie propusa de Muhlbauer;
- calitate excelenta la personalizarea (printarea) optica a cardurilor, mai ales pe suprafete de policarbonat, bazata pe tehnologia printarii cu laser cu capabilitati de gravare;
- detine modul dedicat pentru personalizarea electrica a cardurilor cu contacte (personalizarea chipului);
- pentru cartelele tahografice care necesita cele mai multe procesari, capacitatea de printare este de peste 500 carduri / 8 ore (photo, semnatura, text, chip);
- magazie de intarare de pana la 200 carduri;
- magazie de iesire de pana la 200 carduri;

- optimizarea procesului de personalizare prin procesarea simultana a trei carduri;
- conectare la surse de date prin retea pe baza protocolului TCP/IP.

2.3.3.7 Securitatea sistemului MD-CP

CERTSIGN va asigura serviciile de personalizare pentru cartelele tahografice in aceleasi conditii de maximă securitate ca in prezent. Conditiile de securitate sunt comforme politicii de securitate *„National Authority Policy of Republic of Moldova for the Digital Tachograph"*, aprobata de ERCA, si reglementarii Comisiei Europene nr. 1360/2002, fapt confirmat prin rapoartele de audit ale sistemului tahografului digital national, incluzand sistemul centrului de personalizare MD-CP, desfasurate in anii 2009 şi 2012 de catre Ministerul Transporturilor, in calitate de MD-MSA. Sumarele de audit corespunzătoare au fost acceptate şi publicate pe site-ul ERCA: http://dtc.jrc.ec.europa.eu/dtc_audit_report_status.php.

Securizarea sistemului MD-CP se face pe mai multe nivele. Astfel, exista asigurate elemente de securitate la nivelul aplicatiilor, la nivel de retea si la nivel fizic.

2.3.3.7.1 Securitate aplicatii

Securitatea la nivelul aplicatiilor este data de urmatoarele elemente:

- Accesul operatorilor la aplicatiile de personalizare se face pe baza de smartcarduri. Dupa autentificarea, fiecare operator are asociat un rol in cadrul aplicatiei care limiteaza accesul si operarea aplicatiei de catre acesta;
- Cheile criptografice (asimetrice si simetrice) sunt gestionate in mod securizat prin intermediul unui dispozitiv hardware criptografic de tip HSM, acreditat FIPS 140-2 level 3;
- Generarea PIN-urilor se face tot prin intermediul dispozitivului HSM;
- Securitatea comunicaţiei între MD-CP şi MD-CIA este asigurată de utilizarea unei legaturi SSL dublu autentificata (autentificare mutuala de ambele parti), bazata pe certificate digitale.
- Securitatea comunicaţiei între MD-CP şi MD-CA este asigurată de Aplicaţia de interfaţare şi comunicare cu MD-CA, astfel:
  - *La nivelul de comunicatie* securitatea este asigurata prin utilizarea unei legaturi SSL dublu autentificata (autentificare mutuala de ambele parti), bazata pe certificate digitale;
  - *La nivel software* securitatea este asigurată prin mijloace criptografice. Aplicatia dispune de propriul certificat digital si cheia privata corespunzatoare cat si de certificatul digital al aplicatiei corespondente de la MD-CA. Folosind aceste certificate aplicaţia de interfaţare va semna datele de transmis dupa care le va cripta pentru aplicatia corespondenta. La receptie aplicatia decripteaza datele si

verifica semnatura aplicata de aplicatia corespondenta. Astfel sunt asigurate conditiile de confidentialitate, autenticitate si integritate a datelor vehiculate intre MD-CA si MD-CP. Astfel, orice alterare a informaţiei pe traseul dintre cele două zone va fi detectată imediat şi va fi urmată de notificări specifice către administratorii de system folosind modulul de logare si notificare

- Toate mesajele de jurnalizare (loguri) destinate auditarii sunt semnate digital pentru asigurarea integritatii si autenticitatii acestora;
- Accesul personalului in locatia de lucru a sistemului MD-CP se face controlat si este restrictionat numai pentru personalul autorizat.

2.3.3.7.2 Securitate retea

Securitatea la nivel de retea pentru MD-CP este asigurata prin masurile implementate la nivelul centrului de date care gazduieste infrastructura hardware MD-CP. In acest sens este utilizata o solutie multilayer ce asigura protectia pe mai multe nivele.

Primul nivel de protectie este asigurat de echipamentele de rutare utilizate pentru interconectare la retele publice de date Intener. Aceste echipamente asigura suplimentar fata de functionalitatile de rutare si functionalitati precum filtrare traficului prin intermediul listelor de contol al accesului, protectie DoS si spoofing.

Urmatorul nivel este asigurat prin protectie firewall stateful realizata prin echipamente dedicate ce asigura functionalitati specifice precum protectie atacuri de retea, protectie DoS si DDoS, reasamblare TCP pentru protectia pachetelor fragmentate, protectie la atacuri tip forta bruta, protectie SYN cookie, protectie IP spoofing bazata pe zone, protectie la pachete malformate.

Toate echipamentele de comunicatii si serverele din data center sunt monitorizate permanent asigurandu-se interventia rapida in caz de atacuri informatice sau probleme de functionare.

Conexiunea intre MD-CP si MD-CIA cat si intre MD-CP si MD-CA este protejata prin utilizarea conexiunilor securizate SLL cu autentificare mutuala.

Sistemul de monitorizare interogheaza sistemele MD-CP in mod activ pentru a asigura o functionare in conditii optime atat a sistemelor de operare cat si a aplicatiilor specifice care ruleaza pe acestea. Sunt monitorizati o serie de parametrii ai sistemului de operare cum ar fi: memoria RAM, incarcarea pe sistem, numarul de procese din sistem, utilizarea disk-ului, dar si aplicatiile specifice platformei de personalizare carduri.

Atacurile informatice sau problemele de functionare constituie incidente care trebuie tratate corespunzator. Fiecare incident este inregistrat intr-un registru de incidente electronic, inregistrandu-se pentru fiecare incident urmatoarele tipuri de informatii: numarul incidentului, data incidentului, descrierea incidentului, cauza, solutia, masuri corective, data solutionarii si in functie de severitatea acestuia, entitatile instiintate (de exemplu MD-MSA, ERCA).

2.3.3.7.3 Securitate fizica

Activităţile ce ţin de personalizarea logică şi fizică a cartelelor tahografice se desfăşoară într-un mediu de producţie special amenajat pentru a oferi cele mai bune condiţii de operare, atât din punct de vedere al sarcinilor ce trebuiesc îndeplinite zilnic cât şi din punct de vedere al securităţii.

Spaţiul de producţie se află în sediul CERTSIGN aflat în Bulevardul Tudor Vladimirescu, nr. 29 A, AFI Tech Park 1, Sector 5, Bucureşti, România, CP 050881. Spaţiul este mai mare de 100 de metri pătraţi, este compartimentat în mai multe camere dintre care una este utilizată pentru centrul de personalizare corespunzător MD-CP. Spaţiul este corespunzator din punct de vedere al iluminatului, aerisirii şi climatizării.

În afară de personalizarea cartelelor tahografice în acest spaţiu funcţioneaza si sistemul MD-CA şi sunt păstrate în siguranţă bazele de date ale sistemului, toate acţiunilor care implica emiterea de certificate, semnare, criptare, generare şi manipulare de chei criptografice, initializare si personalizare logica si vizuala de cartele desfăşurându-se în mediul de productie special securizat.

Politicile de acces în incintele utilizate pentru activităţile MD-CP sunt gestionate separat şi sunt diferite de politicile de acces în celelalte spaţii.

Spaţiul se află într-o clădire care este amplasată într-un perimetru închis cu gard şi dotat cu echipamente de control acces pentru autovehicule, având ca dispozitiv de blocare bariere auto. Accesul autovehiculelor se face prin control dual, cartele de proximitate si agenti de paza. Accesul pietonal este de asemenea controlat la intrarea în perimetru de catre agentii de paza. Toate caile de acces catre locatia ocupata de certSIGN sunt controlate dual, cu echipamente de control acces si cu agenti de paza.

Spaţiul alocat CERTSIGN este prevazut cu agenţi de pază proprii şi este organizat pe trei nivele de securitate:

- la primul nivel are acces tot personalul CERTSIGN, pe bază de cartele de proximitate, purtand fotografia angajatului si datele de identificare ale firmei (aria delimitată este de tip „zonă administrativă");
- al doilea nivel este destinat „zonelor tehnice";
- al treilea nivel este format de „zonele de securitate-clasă 2". Accesul in aceste zone este permis pe baza acelorasi cartele de proximitate.

Incintele astfel definite, unde se instalează echipamentele de procesare date sau se păstrează documente, sunt protejate la intruziune prin instalarea de dispozitive de detecţie adecvate, care fac parte dintr-un subsistem de detecţie la efracţie. Accesul in fiecare zona de securitate este permis numai persoanelor autorizate de administratorul de securitate, prin programarea corespunzatoare a sistemului de acces fizic.

În vederea asigurării unui control complet al circulaţiei personalului propriu şi al vizitatorilor, punctele de control acces în zonele de securitate sunt

S.C. CERTSIGN S.A.

supravegheate cu ajutorul unui subsistem de TVCI, care permite vizualizarea în timp real a imaginilor culese, înregistrarea acestora, căutarea şi redarea imaginilor de la anumite momente de timp.

Conform reglementărilor în vigoare, toate încăperile şi holurile de circulaţie fac obiectul detecţiei la incendiu, detectie asigurata printr-un sistem de detecţie şi semnalizare. Accesul grupelor de intervenţie la incendiu va fi permis şi supervizat de personalul firmei de pază, cu anunţarea administratorului de securitate al CERTSIGN.

Sistemul de securitate pentru cladirile centrului de personalizare cuprinde: un sistem de control al accesului, un sistem CCTV (pentru supraveghere video), proceduri de a monitoriza si raporta incidentele CCTV, sisteme aritiefractie si antiincendiu.

Aplicatia de management a securităţii sistemului fizic contine o baza de date in care se înregistreaza toate evenimentele din sistem (intrari/iesiri, alarme). Aplicatia contine un modul de rapoarte, utilizat de catre administratorul de securitate (sau de catre o persoana autorizata de acesta), dupa cum urmeaza :

- rapoarte de prezenta (listeaza perioadele de timp petrecute in interiorul obiectivului pentru fiecare persoana in parte, cu posibilitatea de filtrare pe departamente/persoane si pe o anumita perioada de timp (zile/saptamani/luni);
- rapoarte de evenimente de acces, de tipul "cine, când, unde", cu posibilitatea de selectie pe anumite filtre şi într-o anumita perioada de timp ;
- rapoarte cu tentativele de acces nepermise, referitoare la situatiile cand anumite persoane incearca sa acceseze un anumit filtru la care nu au dreptul sau cand se folosesc alte cartele decat cele introduse in sistem ; acestea se asociază cu imaginile înregistrate de subsistemul de TVCI .

În scopul asigurării pazei şi securităţii bunurilor existente şi a informaţiilor există un post de pază permanent, 24/24 ore, asigurat cu agent de pază, amplasat la intrarea obiectivului, în interiorul acestuia, cu misiunea de a permite accesul autorizat în incintă a salariaţilor si a vizitatorilor. În cazul unui incident, după declansarea alarmei sosesc in maximum 30 de secunde echipajele de interventie.

Accesul în obiectiv este controlat printr-un sistem electronic prevăzut cu uşi cu broaşte electromagnetice ce pot fi acţionate de către cititoarele de cartele de proximitate. Cartelele de proximitate sunt personalizate prin inscripţionarea unei serii unice personalizarea acestora fiind cotrolată de administratorul de securitate.

2.3.3.7.4 Securitate cibernetică

Evaluarea vulnerabilităţilor

CERTSIGN va realiza Evaluarea Vulnerabilitatilor sistemului MD-CP, proces in cadrul caruia se va evalua nivelul de risc cu privire la fiecare vulnerabilitate identificata si se vor face recomandari de remediere.

Serviciile de evaluarea vulnerabilităţilor ofertate în prezentul document vor fi livrate de către experţi în acest domeniu. Acest serviciu presupune realizarea mai multor tipuri de acţiuni în mod recurent, respectiv: identificarea sistemelor informatice ce trebuie scanate, prioritizarea acestora, scanarea, revizuirea rezultatelor obţinute, evalurea vulnerabilităţilor identificate şi acordarea unui indice de risc, formularea de recomandări de remediere, retestare.

În livrarea serviciului se vor utiliza instrumente automate de scanare a sistemelor MD-CP. Aplicatiile si metodele de realizare a evaluarii sunt de ultima generatie si sunt cotate ca tehnologii de varf. Modul in care se va derula evaluarea nu va impacta in niciun fel performantele sistemelor informatice evaluate si va permite descoperirea de vulnerabilitati la nivel de: sistem de operare, retea LAN, aplicatii si baze de date, etc.

Ultima etapă din fiecare iteraţie a serviciului de evaluării de vulnerabilităţi va fi formularea de recomandări care să permită realizarea corecţiilor necesare pentru remedierea breşelor de securitate.

Teste de penetrare

CERTSIGN va asigura servicii de tipul Penetration Testing pentru sistemul MD-CP, care testaază nivelului de securitate al infrastructurii tinta prin identificarea şi validarea vulnerabilităţilor la nivel de reţea, sistem de operare, aplicaţii si servicii.

Testele de penetrare se vor derula cu ajutorul unor specialişti certificaţi, care vor utiliza aplicaţii comerciale dedicate de ultimă generaţie.

De asemenea, CERTSIGN desfăşoară testele de penetrare în baza unor proceduri ce au fost concepute prin respectarea standardelor şi recomandărilor în domeniu (SANS, NIST, ENISA, etc.).

În cadrul metodologiei de lucru cu privire la serviciile de penetration test au fost cuprinse următoarele etape:

- realizarea unui penetration test plan cu privire la: tipul de pentest care se va realiza (black box – din exteriorul reţelei, white box – din interiorul reţelei), sistemele care vor fi cuprinse în iteraţia respectivă de pentest, prioritizarea acestora, intervalul de realizare al testelor şi durata acestora, strategia de comunicare în cadrul echipei de lucru, etc. De asemena, planul de penetration test va mai include o analiză de proiect la nivelul echipei CERTSIGN în care se va stabili: membrii echipei de pentest, scenariile de testare, tool-urile utilizate.
- stabilirea modului în care se va face gestionarea datelor/informaţiilor sensibile ce vor fi descoperite cu privire la infrastructura MD-CP, respectiv: colectarea datelor şi stocarea lor într-o formă sigură.

Fiecare pentest in parte se va incheia cu intocmirea unui raport in cadrul caruia vor fi cuprinse toate vulnerabilitatile identificate si recomandari pentru remedierea acestora.

Asigurarea reactiei la atacuri informatice

CERTSIGN va asigura pentru sistemul MD-CP, servicii de reactie la atacuri informatice prin intermediul unor specialisti dedicati acestei activitati care vor realiza:

- Confirmarea atacului informatic
- Analiza probelor colectate
- Stabilirea cauzelor
- Evaluarea pagubelor
- Identificarea tuturor victimelor in reteau compromisa
- Sanitizarea retelei
- Formularea unui raport de incident

Activitatile de raspuns la incident au drept scop eradicarea unei infectii din cadrul retelei intr-un timp optim astfel incat sa fie diminuate pagubele.

Serviciile ofertate vor fi livrate conform unor proceduri de lucru interne care au fost concepute prin respectarea recomandărilor (SANS) și standardelor în domeniu (NIST Special Publication 800-137) astfel încât să se poată furniza un timp de reacție redus pentru a iniția răspunsul la potențialele incidente de securitate cibernetică.

Monitorizarea sistemelor

CERTSIGN va monitoriza sistemele MD-CP, folosind experți specializați (analiști de securitate) în acest domeniul. Monitorizarea va realiza identificarea în mod proactiv și eficient a potențialelor amenințări informatice prin monitorizarea proactivă și continuă a activității care impacteaza sistemele informatice protejate ale MD-CP.

Serviciile CERTSIGN respectă standardele si recomandările în domeniu impuse de organisme recunoscute precum: ENISA, SANS, Trusted Introducer (CERTSIGN este membră acreditată a comunității), NIST.

Prin mecanisme dedicate se va realizeaza corelarea evenimentelor astfel încât să determine generarea unor alerte/alarme cu privire la amenințările identificate in cadrul sistemului MD-CP.

2.3.3.8 Infrastructura de comunicatii a MD-CP

In cladirea unde este localizat centrul de date care gazduieste platforma MD-CP este realizata o cablare structurata de date si voce ce respecta standardele: ISO-IEC 11801, EN50173, EN50167/68/69, EIA/TIA568A, EIA/TIA 568A-5, TSB67.

Toate echipamentele sunt produse in conformitate cu standardul calitatii ISO9001.

Sistemul de cablare structurata este de categorie 5 complet modulară, având la bază conceptele actuale de cablare structurată, cu conexiuni individuale pentru fiecare post de lucru (telefon sau calculator) la tablouri de conexiuni şi repartiţie (patch panel-uri), şi apoi către echipamente centrale (switch-uri, respectiv centrala telefonică). Reteaua este de tip switching Ethernet, cu rate de transfer de 10/100/1000 Mbps.

Centrul de date are 2 legaturi de mare viteza la Internet care sunt folosite intr-o arhitectura redundanta si de balansare a incarcarii. La nivelul echipamentelor active se aplica politici de management si prioritizare a traficului asigurandu-se astfel un nivel de servicii predeterminat.

Cladirea centrul de date detine toate dotarile necesare unui centru informatic modern (climatizare, alimentare electrica, generator de curent, sistem de control acces, paza si protectie, supraveghere video).

Tot aici este localizat si Centrul de Monitorizare (NOC – Network Operation Center) prin intermediului carula se asigura servicii de monitorizare si management in timp real al echipamenetelor active de retea precum si a serverelor.

2.3.3.9 Gestiunea stocurilor de consumabile

În vederea implementarii cerintei de a asigura continuitatea personalizării şi emiterii de cartele tahografice de către ANTA pe toată durata contractului, CERTSIGN va asigura un stoc de cartele nepersonalizate şi toate consumabilele necesare care să acopere necesarul pentru cel puţin 2 luni de producţie.

Solutia propusa de catre CERTSIGN are la baza un lant de aprovizionare securizat, cu inventar si control de audit complet, care poate fi urmarit pentru fiecare element in parte in orice faza a productiei, astfel:

1. **Aprovizionare:**
   - stabilirea unui plan de achizitii care sa tina cont de comenzile estimate a fi primite din partea clientului, de termenele de productie si livrare ale furnizorilor, precum si de mentinerea unui stoc tampon necesar unei productii medii aferente unei luni calendaristice; astfel se asigura toate materialele consumabile aferente echipamentelor din centrul de personalizare, care permit productia fara intreruperi a cartelelor tahografice;
   - semnarea contractelor cu furnizorii conform procedurilor de achizitie interne;
   - lansarea comenzilor de achizitie conform planului de achizitie si a update-urilor perioadice facute de catre Project Manager ca urmare a monitorizarii istoricului comenzilor primite din partea clientului si a nevoilor de productie;

S.C. CERTSIGN S.A.

- livrarea comenzilor de achizitie de catre furnizori(cu transport securizat acolo unde este cazul), vamuirea marfurilor (acolo unde este cazul) si introducerea lor in gestiune in baza documentelor specifice;
- operatiunile aferente procesului de aprovizionare sunt inregistrate in software-ul ERP (Enterprise Resource Planning) precum si in aplicatii specifice conexe conform procedurilor si politicilor interne, oferind in orice moment trasabilitate, monitorizare, si control astfel procesul este auditabil.

2. Gestiune:

- Introducerea marfurilor in gestiune conform documentelor specifice de catre gestionarul companiei, in urma verificarilor cantitative si calitative a loturilor de marfa primite;
- Identificarea rebuturilor de fabricatie si demararea procedurilor de notificare a furnizorului si de inlocuire a acestor rebuturi prin deschiderea unor operatiuni de export-import temporar;
- Iansarea cererii de scoatere din gestiune in baza reperelor comandate de catre client;
- efectuarea descarcarii de gestiune si predarea marfurilor spre productie in baza documentelor specifice;
- efectuarea reconcilierii stocurilor la sfarsitul fiecarei zile;
- lunar, sunt intocmite balante de verificare a stocurilor;
- anual, la 31 decembrie, se realizeaza inventarul faptic si scriptic al stocurilor;
- anual, are loc auditul financiar-contabil extern al stocurilor;
- operatiunile aferente procesului de gestiune sunt inregistrate in software-ul ERP (Enterprise Resource Planning) precum si in aplicatii specifice conexe conform procedurilor si politicilor interne, oferind in orice moment trasabilitate, monitorizare si control astfel procesul este auditabil.

3. Productie:

- primirea comenzi din partea clientului;
- introducerea marfurilor in procesul de productie;
- efectuarea controlului de calitate;
- depistarea rebuturilor de productie si intocmirea documentelor specifice pentru scoaterea din functiune si distrugerea acestora, conform procedurilor interne;
- pregatirea marfurilor pentru livrarea catre client.

4. Distributie:

- Livrarea printr-o metodă securizată a cartelelor la sediul ANTA din Republica Moldova mun. Chișinău str. Aleea Gării, 6 în baza documentelor însoțitoare conform contractului;
- predarea cartelelor de către personalul ANTA în baza proceselor verbale de predare-primire;
- In cazul in care clientul semnaleaza, ulterior livrarii, existenta unor cartele defecte din vina furnizorului, acestea sunt inlocuite in garantie, cu

intocmirea documentelor necesare predarii-primirii acestor cartele, verificarii defectelor, scoaterii din functiune si distrugerii lor.

Plicurile cu cartelele personalizate vor fi livrate la sediul ANTA din Republica Moldova mun. Chișinău str. Aleea Gării, în cel mult 7 zile calendaristice de la transmiterea comenzii de către ANTA.

Procesul special de gestionare a cartelelor tahograf asigura:

1. accesul limitat in gestiune, atat faptic cat si scriptic, de catre persoana desemnata de catre companie sa indeplineasca rolul de gestionar, astfel:
   - faptic: stocurile sunt depozitate intr-o zona special determinata acestui scop, iar accesul se face securizat numai de catre persoane autorizate;
   - scriptic: toate activitatile de gestiune sunt inregistrate in software-ul ERP (Enterprise Resource Planning) al companiei, in module determinate functie de rolul fiecarei persoane, accesul in software efectuandu-se in baza unui user ID si a unei parole;
   - astfel, in orice moment procesul ofera trasabilitate, monitorizare si control si este auditat;
2. procedura de control corespunzator al stocurilor pentru toate componentele utilizate in productia cartelelor tahografice si tiparirea scrisorilor special cu PIN-ul cartelelor de atelier, astfel:
   - verificarea cantitativa si calitativa a marfurilor in momentul receptiei;
   - reconcilierea zilnica a stocurilor in urma intrarilor si iesirilor de gestiune;
   - lunar, sunt intocmite balante de verificare a stocurilor;
   - anual, la 31 decembrie, se realizeaza inventarul faptic si scriptic al stocurilor;
   - anual, are loc auditul financiar-contabil extern al stocurilor;
3. reconciliere la sfarsitul zilei cu privire la intrarile, respectiv iesirile din gestiune a marfurilor
4. parole si coduri de acces pentru fiecare operatie, asa cum este evidentiat mai sus
5. identificarea persoanelor care au aprobat si efectuat diferite operatii, asa cum este evidentiat mai sus

DataCenter-ul MD-CP detine infrastructura necesara asigurarii următoarelor categorii de functionalitati:

- Gestioneaza stocurile de materiale (cartele blank, cartele defecte, consumabile, etc.) si alerteaza operatorii asupra situatiilor critice, asa cum este evidentiat la punctele CP1 si CP2, prin utilizarea software-ului ERP (Enterprise Resource Planning) precum si a unor aplicatii specifice conexe, in baza procedurilor si politicilor interne in vigoare;
- Furnizeaza statistici si rapoarte pentru cartelele tahografice procesate sau in curs de procesare prin utilizarea software-ului ERP (Enterprise

Resource Planning) precum si a unor aplicatii specifice conexe, in baza procedurilor si politicilor interne in vigoare.

2.3.4 MD-CA

Sistemul MD-CA propus de catre CERTSIGN, sistem utilizat și în prezent, este una dintre componentele de baza ale sistemului national de emitere a cartelelor tahografice. Sistemului MD-CA este bazat pe produsul tachoSAFE CA și a fost dezvoltat, implementat, găzduit, administrat, operat și întreținut de către CERTSIGN începând cu anul 2007.

Sistemul tachoSAFE CA este responsabil cu emiterea certificatelor digitale care sunt inserate in cipurile celor patru tipuri de cartelele tahografice emise.

Sistemul tachoSAFE CA, corespunzator MD-CA, Implementeaza un serviciu PKI de emitere a certificatelor digitale pentru cartelele tahografice. In acest sens tachoSAFE CA Implementeaza toate cerintele reglementarilor (EC) 3281/85, (EC) 2135/98, (EC) 1360/2002 cu privire la un astfel de sistem, cât și cerințele de securitate specificate prin Politica ERCA vresiunea 2.1 și *„National Authority Policy of Republic of Moldova for the Digital Tachograph"* aprobată de catre ERCA.

Sistemul MD-CA propus de catre CERTSIGN a fi folosit în continuare, a trecut deja cu succes toate auditurile realizate de către MT In calitate de MD-MSA din anii 2009 și 2012, si MD-MSA a trimis la ERCA rezultatele auditurilor.

În continuare CERTSIGN va asigura pe durata contractului toate condițiile necesare în vederea auditării cu succes a MD-CA.

CERTSIGN, in calitate de service agency pentru MD-CA este deja declarat oficial ca MSCA prin politica de securitate a *„National Authority Policy of Republic of Moldova for the Digital Tachograph"* aprobata de catre ERCA.

Sistemul MD-CA a organizat deja 5 ceremonii ale cheilor, prin care s-au emis perechile de chei RSA necesare, chei care au fost certificate de ERCA, conform reglementarii (EC) 1360/2002 si a politicilor ERCA si *„National Authority Policy of Republic of Moldova for the Digital Tachograph"* aprobata de catre ERCA.

Pe durata contractului CERTSIGN va organiza toate ceremoniile cheilor necesare pentru a asigura continuitatea furnizarii de servicii de certificare pentru cartelele tahografice Romanesti.

CERTSIGN va asigura găzduirea, administrarea, operarea, mentenanța și actualizarea sistemului autoritatii de certificare nationale, MD-CA, in aceleasi conditii ca in prezent. Conditiile de securitate sunt comforme politicii de securitate *„National Authority Policy of Republic of Moldova for the Digital Tachograph"*, aprobata de ERCA si reglementarii Comisiei Europene nr. 1360/2002, fapt confirmat prin rapoartele de audit ale sistemului tahografului digital national, incluzand sistemul centrului de personalizare MD-CP, desfasurate in anii 2009 și 2012 de catre Ministerul Transporturilor, in calitate de MD-MSA. Sumarele de audit corespunzătoare au fost acceptate și publicate pe site-ul ERCA:

http://dtc.jrc.ec.europa.eu/dtc_audit_report_status.php.

De asemenea, asigurarea conditiilor de securitate corespunzatoare pentru sistemul autoritatii de certificare nationale, MD-CA, este certificată si prin

S.C. CERTSIGN S.A.

rapoartele de audit ISO 27001 pentru sistemului de management al securitatii informatiilor obtinute de catre CERTSIN.

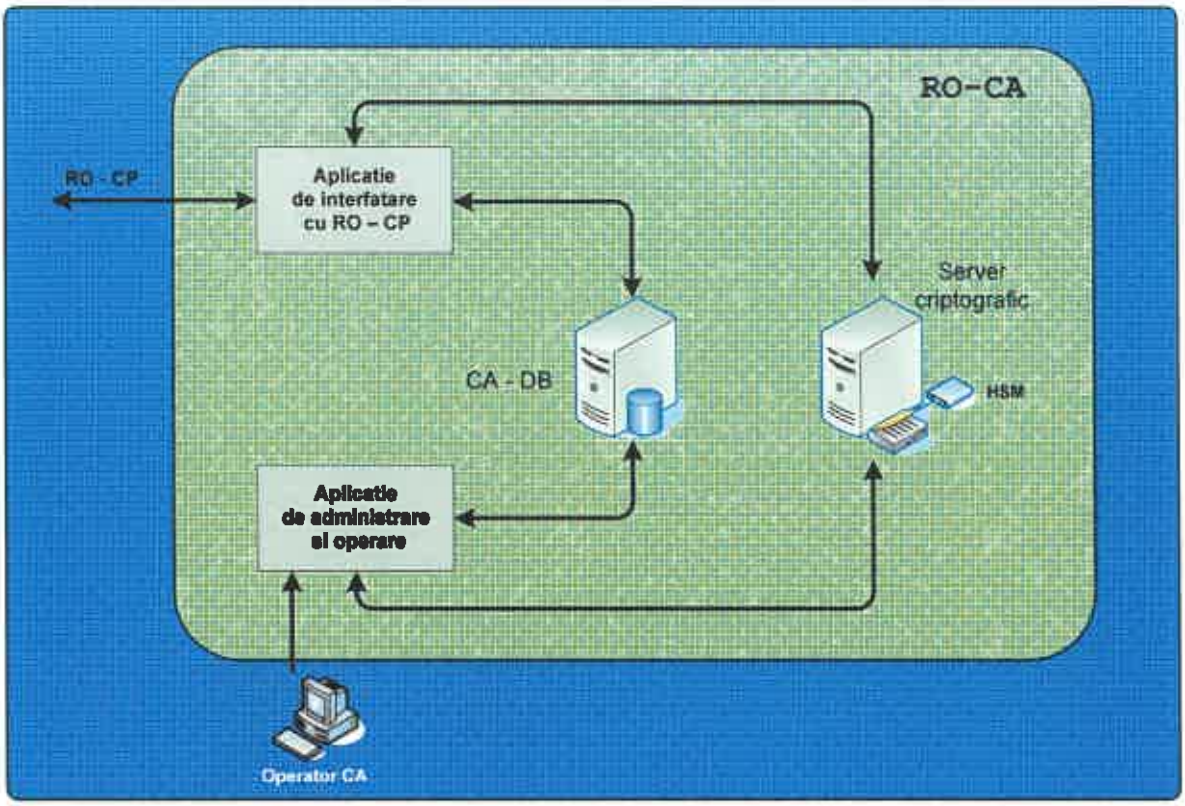
Solutia propusa implementează pe lângă infrastructura PKI de producţie utilizată pentru emiterea certificatelor digitale pentru personalizarea cartelelor tahografice destinate ANTA, şi o infrastructura PKI de test bazata pe perechea de chei de test la nivel european si o pereche de chei de test la nivelul Romaniei, a carei cheie publica este certificata cu chela privata de test Europeana, conform cerintei CSM_011 din reglementarea comisiei europene (EC) 1360/2002, Anexa IB, Appendix 11. Infrastructura PKI de test este necesara emiterii de certificate de test pentru cartelele tahografice care urmeaza sa fie certificate în vederea obţinerii Type Approval-ului.

În situaţia în care specificaţiile criptografice ale sistemului tahograf digital vor fi actualizate sau modificate de Uniunea Europeană pe durata contractului CERTSIGN va actualiza sistemul actualei autoritati de certificare, tachoSAFE CA, pentru a implementa noile cerinţe şi specificaţii criptografice, si va asigura şi compatibilitatea cu actualele tahografe digitale si carduri tahograf pe perioada de tranzitie in care ambele mecanisme criptografice vor fi folosite. Implementarea noilor cerinte în sistemul MD-CA se va face în termen de maximum 30 zile de la publicarea acestora, fără costuri suplimentare pentru ANTA şi fără a intrerupe activitatea de furnizare a cartelelor tahografice de catre ANTA.

CERTSIGN are capabilitatea de a actualiza sistemul actualei autoritati de certificare, tachoSAFE CA, comform noilor cerinţe care vor fi elaborate la nivel European deoarece componenta tachoSAFE CA, corespunzatoare MD-CA, este o componentă a produsului „tachoSAFE" dezvoltat de CERTSIGN, fapt demonstrat prin certificatul de înregistrare al acestui produs la ORDA, anexat prezentei oferte.

2.3.4.1 Arhitectura MD-CA

Din punct de vedere arhitectural, tachoSAFE CA este compusa din urmatoarele componente:



Asadar, exista:

1. O componenta care implementeaza serverul criptografic – **tachoSAFE-cryptoServer**

Scopul acestei componente este acela de a deservi necesitatile exclusiv criptografice ale autoritatii de certificare. Practic, acesta:

- gestioneaza cheile private ale autoritatii de certificare destinate operatiei de semnare a certificatelor
- gestioneaza cheia simetrica destinata personalizarii cardurilor de workshop (KmWS), primita de la ERCA
- implementeaza operatiile criptografice necesare - in speta, semnarea certificatelor destinate cartelelor tahografice precum criptarea/decriptarea cheii simetrice (KmWC)

Generarea, stocarea si utilizarea cheilor private de semnare a certificatelor (cheile secrete ale autoritatilor de certificare) precum si a cheilor simetrice (in speta, KmWS) este realizata prin intermediul unui dispozitiv criptografic hardware specializat de tip HSM nCipher, acreditat FIPS 140-2 level 3.

2. O componenta de interfatare si comunicare cu MD-CP – **tachoSAFE-responder**

Scopul acestei componente este acela de a se interfata cu centrul de personalizare (MD-CP) si de a raspunde la cererile de certificare primite din partea acestuia. Practic aceasta componenta preia de la MD-CP cererile de certificare in baza de date interna a autoritatii de certificare si intoarce certificatele corespunzatoare, semnate de catre autoritatea de certificare.

3. O componenta de administrare si operare a autoritatii de certificare

Scopul acestei componente – web based - este acela de a permite administrarea autoritatii de certificare precum si efectuarea unor operatii specifice.

4. O componenta de baza de date

Aceasta componenta este responsabila cu stocarea tuturor informatiilor necesare functionarii autoritatii de certificare. Practic, aceasta pastreaza evidenta cererilor de certificate sosite de la MD-CP, evidenta certificatelor emise, informatii interne de administrare a autoritatii de certificare

Toate componentele de mai sus dispun de module de jurnalizare, astfel incat toate operatiile efectuate la nivelul MD-CA sa poata fi verificate si auditate.

De asemnea exista prevazut mecanism de backup pentru datele critice din sistem. Periodic, la un interval de o luna se face backup la datele din baza de date interna a MD-CA. Fisierele de backup sunt transportate in mod securizat către locatia de disaster-recovery. Acestea sunt semnate digital asigurandu-se integritatea si autenticitatea acestor fisiere. Astfel, este asigurata 24 din 24 de ore disponibilitatea datelor din sistem.

În calitatea sa de producător şi implementator al sistemului, CERTSIGN poate asigura migrarea componentelor MD-CA pe servere noi, furnizate de către autoritatea contractantă, utilizand sisteme de operare de generaţie nouă, cum ar fi SuSE Linux Enterprise Server 11. Migrarea se va face pentru toate serverele sistemului MD-CA, şi anume:

- serverul de baze de date al MD-CA, şi
- serverul criptografic al MD-CA.

În procesul de migrare CERTSIGN va asigura:

- transferul complet al aplicatiilor software pe noua platformă hardware,
- transferul complet al datelor stocate în bazele de date ale MD-CA,
- transferul complet al fişierelor de audit.

Procesul de migrare nu va afecta în nici un fel continuitatea proceselor de inregistrare, emitere si gestiunea cartelelor tahografice, pe durata migrării asigurându-se funcţionalitatea sistemului existent. La finalul migrării, după testarea completă a sistemului migrat pe noua platformă HW şi acceptanţa acestuia, se va face comutarea proceselor de certificare cartele tahografice pe

noua platformă. Finalizarea migrării și comutarea pe noua platformă se va face într-un weekend pentru a nu afecta în nici un fel activitatea ANTA.

Fluxul principal de functionare si de intercomunicare intre aceste componente este urmatorul:

- In prima etapa, prin intermediul componentei de administrare si operare a autoritatii de certificare se genereaza autoritatile de certificare: autoritatile de certificare de emitere de certificate pentru cartele tahografice de test si autoritatea de certificare de emitere de certificate pentru cartele tahografice operationale. Aici se genereaza perechile de chei RSA de 1024 de biti de semnare a certificatelor specifice acestor autoritati si se instaleaza certificatele corespunzatoare cheilor publice semnate de ERCA. De asemnea, tot in aceasta faza se face configurarea autoritatii de certificare cu cheile publice ale ERCA precum si alte configuratii necesare.
- Prin intermediul componentei de interfatare cu MD-CP se primesc cereri de certificare. Fiecare cerere de certificat receptionata de la MD-CP este inregistata in baza de date a autoritatii de certificare.
- Fiecare cerere de certificare este trimisa de catre componenta de interfatare cu MD-CP catre serverul criptografic care semneaza cererea respectiva si emite certificatul corespunzator. Accesul la cheile de semnare se face numai la nivelul serverului criptografic.
- Componenta de interfatare cu MD-CP obtine de la serverul criptografic certificatul semnat, il inregistreaza in baza de date a autoritatii de certificare si apoi il furnizeaza catre MD-CP pentru a fi inserat pe echipament (cartela tahografica)

Aplicatia tachoSAFE CA permite implementarea modelului PKI ierarhic pe 3 nivele:

- o autoritate de certificare la nivel european (ERCA)
- o autoritate de certificare la nivel national (MD-CA)
- emiterea de catre autoritatea nationala de certificate pentru echipamente (cartele tahografice),

asa cum este cerut in specificatiile Comisiei Europene (EC) 1360/2002, cerintele CSM_006, CSM_007, CSM_008, CSM_009, CSM_010 din Anexa IB, Appendix 11.

2.3.4.2 Procese MD-CA

Ca si procese principale in cadrul functionarii MD-CA avem urmatoarele:

- generarea perechilor de chei de semnare ale autoritatilor de certificare
- preluarea cererilor de certificate de la MD-CP
- generarea certificatelor

2.3.4.2.1 Generarea cheilor si a cererilor de certificat pentru CA

Autoritatea de certificare tachoSAFE CA, poate gestiona mai multe CA-uri separate, cu chei de semnare diferite. Astfel, se pot genera perechi chei de semnare diferite prin intermediul carora se pot emite:

- certificate destinate cartelelor tahografice operationale (utilizand cheia de semnare special dedicata in acest scop)
- certificate destinate cartelelor tahografice de test (de asemenea, utilizand chei de semnare special dedicate pentru emiterea acestor tipuri de certificate)

In acest fel, prin intermediul autoritatii de certificare tachoSAFE CA prin care CERTSIGN implementeaza functia de MD-CA, se poate implementa si o infrastructura PKI de test bazata pe cel putin o pereche de chei de test la nivel de stat (Republica Moldova) si pe perechea de chei de test de la nivel european, conform cerintei CSM_011 din Reglementarea Comisiei Europene (EC) 1360/2002, Anexa IB, Appendix 11, care sa fie utilizata in cadrul executarii testelor de "type approval".

De asemenea, perechile de chei generate pentru semnarea certificatelor (de productie si de test) sunt chei RSA de 1024 de biti conforme cu cerintele specifice din Reglementarea Comisiei Europene (EC) 1360/2002 avand:

- modulul n pe 1024 biti
- exponentul public e pe 64 biti, avand valoarea mai mare sau egal cu 3 si
- exponentul privat d pe 1024 biti

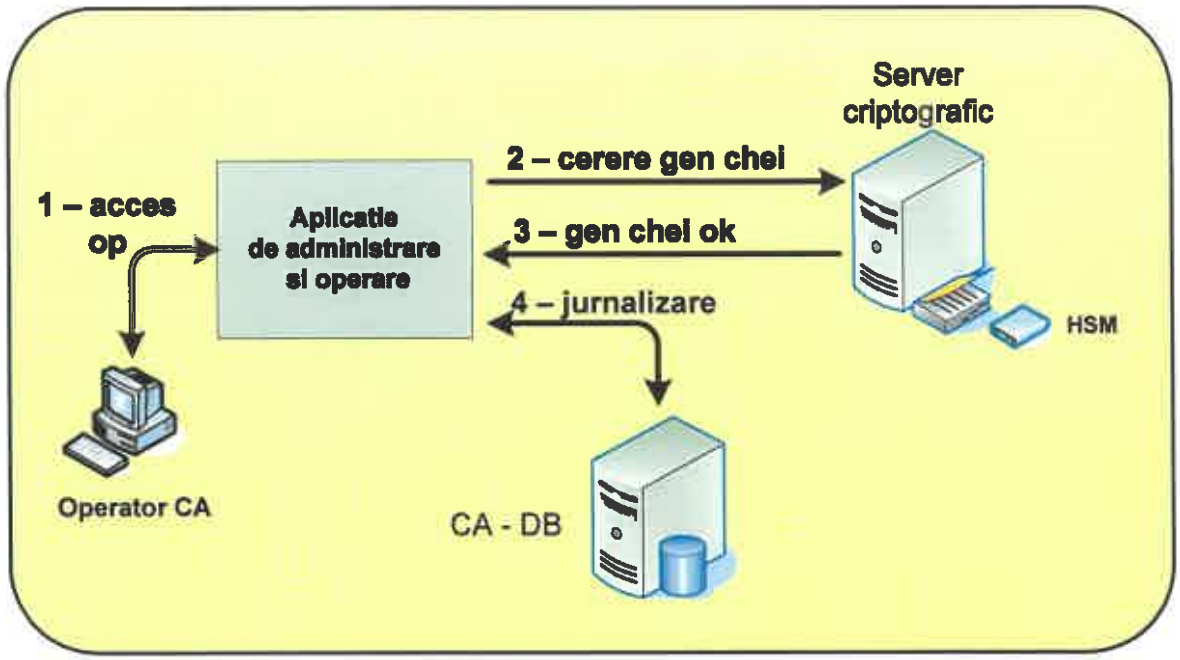
(cerintele CSM_003, CSM_014 din Reglementarea Comisiei Europene (EC) 1360/2002, Anexa IB, Appendix 11).

Generarea perechilor de chei ale autoritatii de certificare se face in faza de creare a CA-urilor folosindu-se aplicatia web-based de administrare si operare a tachoSAFE CA. Accesul la aplicatia de administrare si operare se obtine folosindu-se autentificarea bazata pe certificate X.509 si token criptografic. Aplicatia de administrare si operare ofera doar interfata de operare, necesara pentru aceasta operatie. Generarea efectiva a cheilor se face prin intermediul serverului criptografic (componenta tachSAFE-cryptoServer).

Generarea perechilor de chei de semnare a autoritatii de certificare se face pe un dispozitiv hardware criptografic temper-proof, acreditat FIPS 140-2 level 3, de tip HSM marca nCipher (Thales). Generarea perechilor de chei se face pe principiul K/N ("four eyes principle"). Astfel, autorizarea operatiei de generare de chei se face in prezenta a K (K>= 2) operatori cu roluri de administratori de chei fiind conforma cu specificatiile din Politica de Certificare si Codul de Practici si Proceduri propuse. Fiecare dintre acesti administratori de chei detine cate un smartcard special protejat pe baza de PIN pe care se afla chei criptografice speciale de acces la HSM. Autorizarea procesului de generare de chei pe HSM se face utilizand aceste smartcard-uri.

S.C. CERTSIGN S.A. certSIGN

Fluxul de operatii pentru procedura de generare chei este descris in schema urmatoare:



Asadar generarea cheilor se efectueaza prin participarea activa a cel putin 3 persoane, dintre care una cu rolul de administrator CA, dupa cum urmează:

- administratorul de CA acceseaza aplicatia de operare si administrare pentru operatia de generare de CA –uri. Autentificarea la aceasta aplicatie se face prin certificat digital X.509 stocat pe token criptografic
- se face autentificarea la HSM prin intermediul a K (K >=2) administratori de chei autorizandu-se accesul pentru generarea de chei RSA pe HSM
- se genereaza perechile de chei de semnare pentru CA –uri

Conform procedurii explicate mai sus, generarea perechii de chei de semnare MD.SK si MD.PK (chele de tip RSA pe 1024 biti) se face pe un dispozitiv temper-proof FIPS 140-2 level 3 iar procesul de generare necesita participarea activa a cel putin 3 persoane dintre care una cu rol de administrator de CA.

Dupa generarea perechilor de chei ale CA–urilor, partea publica a acestor chei (cheile publice ale CA -urilor) sunt extrase de pe HSM si sunt stocate in baza de date a autoritatii de certificare. Aceste chei publice sunt certificate prin intermediul cheilor private (secrete) ale ERCA, obtinandu-se certificatele corespunzatoare.

Dupa generarea perechilor de chei ale CA–urilor, cheile private (secrete) ale CA–urilor, nu parasesc niciodata dispozitivul HSM fiind imposibila extragerea lor in afara acestuia. Operatia de semnare a certificatelor se face exclusiv in interiorul HSM–ului si poate avea loc numai prin autorizarea cu smartcard-urile administratorilor de chei. Aceasta autorizare se poate face numai in prezenta activa a acestor administratori de chei (K administratori, cu K >=2) utilizand smartcardurile speciale de acces la HSM.

Cheile private (secrete) ale CA–urilor, generate si stocate pe dispozitivul hardware de tip HSM prin procedura de mai sus, reprezinta cheile de semnare a certificatelor digitale dedicate cartelelor tahografice fiind folosite exclusiv numai pentru acest scop.

Cheile publice ale CA –urilor, generate pe dispozitvul hardware de tip HSM prin procedura de mai sus, sunt cheile de verificare a certificatelor digitale dedicate cartelelor tahografice si emise de aceste CA –uri, fiind folosite exclusiv in acest sens.

Asadar, stocarea cheii secrete MD.SK de semnarea a certificatelor dedicate cartelelor tahografice se face pe un dispozitiv temper-proof FIPS 140-2 level 3, indeplinind cele mai riguroase cerinte de securitate. Accesul la cheia privata de semnare se face prin participarea activa a cel putin 2 persoane.

Cheia privata (MD.SK) este emisa pe o perioada limitata specificata in Politica de Certificare si Codul de Practici si Proceduri. Cheia publica (MD.PK) este emisa pe o perioada nelimitata. Aplicatia tachoSAFE CA permite schimbarea (reinoirea) cheilor de semnare a certificatelor (MD.SK), in mod regulat, la o anumita perioada asigurandu-se astfel cerintele din specificatiile Comisiei Europene (cerinta CSM_008 din Reglementarea Comisiei Europene (EC) 1360/2002, Anexa IB, Appendix 11). Dupa generarea unei noi perechi de chei, utilizand procedura descrisa in acest capitol, vechea cheie privata va fi distrusa, iar perechea sa publica va fi mentinuta in continuare in sistem putand fi folosita la verificarea certificatelor emise cu cheia privata pereche.

Cheile publice ale CA–urilor (de productie si de test) sunt utilizate pentru a obtine certificatele corespunzatoare semnate cu cheile private (secrete) corespunzatoare, ale autoritatii de certificare root de la nivel european (ERCA).

Astfel, prin intermediul aplicatiei de administrare si operare, cheia publica a MD-CA (MD.PK) poate fi exportata intr-o cerere de certificare - Key Certification Request (MD.KCR) - in formatul specificat in Anexa A din Politica de Certificare a ERCA, versiunea 2.1. Aceasta cerere de certificare va fi transmisa catre ERCA pentru a fi semnata cu cheia privata de la nivel european in cadrul unui certificat pentru Republica Moldova (MD.C). Aplicatia de administrare si operare permite importarea in sistem a certificatului MD.C emis de ERCA precum si a cheii publice EUR.PK a ERCA, verificand corectitudinea certificatului in raport cu cheia privata MD.SK.

S.C. CERTSIGN S.A. BUCUREŞTI - ROMÂNIA

Transportul cererii de certificare MD.KCR, respectiv a certificatului MD.C si a cheii publice ERCA, EUR.PK se va face conform specificatiilor din Anexa C a Politicii de Certificare a ERCA, versiunea 2.1.

Toate operatiile implicate in cadrul procesului de generare de chei si cereri de certificate sunt jurnalizate in loguri speciale care pot fi apoi auditate. Aceste mesaje de jurnalizare sunt protejate prin semnarea digitala cu o cheie privata, special dedicata in acest sens, aflata tot pe HSM. Prin acest mecanism se asigura astfel integritatea acestor mesaje de jurnalizare.

2.3.4.2.2 Preluarea cererilor de certificate de la MD-CP

Una dintre functiile importante ale entitatii MD-CA este aceea de interfatare cu centrul de personalizare a cartelelor tahografice, MD-CP. Astfel pentru a emite certificatele destinate cartelelor tahografice este necesar ca MD-CA sa primeasca cereri de certificate pentru acestea de la MD-CP. Pe baza cererilor primite de la MD-CP, MD-CA, prin intermediul aplicatiei tachoSAFE CA se vor emite si furniza catre MD-CP certificatele corespunzatoare.

Preluarea la MD-CA, a cererilor de certificate de la MD-CP, se va face prin intermediul aplicatiei de interfatare si comunicare cu MD-CP, una din componentele de baza ale tachoSAFE CA. Cererile de certificate ajung in sistemul de emitere certificate al tachSAFE CA unde sunt inregistrate in baza de date a acestela si sunt emise certificatele corespunzatoare.

Aplicatia de la MD-CA, de interfatare si comunicare cu MD-CP, comunica automat pentru preluarea cererilor de certificate cu o componenta pereche de la MD-CP folosind un canal securizat. Securizarea se face utilizand o conexiune SSL criptata si autentificata mutual prin certificate digitale X.509. Astfel toate informatiile vehiculate intre MD-CP si MD-CA si invers (inclusiv cererile de certificate) sunt criptate si semnate, asigurandu-se astfel confidentialitatea, autenticitatea si integritatea datelor.

Transmiterea cererilor de certificate la MD-CP catre MD-CA se face utilizand mesaje XML care contin datele necesare emiterii de certificate: cheia publica a echipamentului pentru care se va emite certificatul, identificarea tipului de echipament, tipul de certificat dorit (de test sau de productie), etc. Fiecare cerere de certificat contine un identificator unic pe baza caruia se identifica apoi raspunsul cu certificatul primit. Un mesaj XML poate contine una sau mai multe cereri de certificate. Pe baza unei cereri XML primita de de la MD-CP se genereaza astfel unul sau mai multe certificate de catre MD-CA.

Preluarea cererilor de certificate in tachoSAFE CA se poate face si manual prin intermediul aplicatiei de adminsitrare si operare a autoritatii de certificare. Aceasta

operatie poate fi facuta numai de administratorul de CA, pentru autentificarea acestuia la aplicatia de operare atachoSAFE CA, utilizandu-se certificat digital X.509 si token criptografic.

2.3.4.2.3 Generarea certificatelor

Scopul principal al aplicatiei tachoSAFE CA este acela de a emite certificate digitale pentru personalizarea cartelelor tachografice. Aplicatia tachoSAFE CA primeste cereri de certificate de la MD-CP, pentru echipamente (cartele tahografice) emitand certificate pentru cheile publice RSA ale acestora. Perechile de chei RSA pentru echipamente se genereaza la centrul de personalizare (MD-CP), iar la MD-CA sunt transmise numai cheile publice ale acestora.

Prin intermediul aplicatiei tachoSAFE CA, se pot emite:

- certificate de test, care vor fi utilizate pe cartele tahografice de test in cadrul executarii testelor de "type approval" cu ERCA
- certificate operationale, care vor fi utilizate pe cartele tahografice de productie

Aplicatia face diferenta intre cereri de certificate de test si cele de certificate de productie. Astfel, cererile de certificate vor identifica tipul certificatelor care vor fi emise la aceste cereri.

Certificatele sunt semnate cu cheile RSA special dedicate pentru acest scop. Astfel, certificatele de test vor fi emise folosind cheile private (secrete) de test, iar certificatele operationale vor fi emise folosind cheia privata (secreta) special dedicata pentru acest tip de certificate. Generarea, stocarea si gestiunea acestor chei este descrisa in aceasta oferta in capitolul special dedicat pentru "Generarea perechii de chei si a cererii de certificat pentru CA".

Semnarea certificatelor se face de catre componenta de server criptografic (tachoSAFE-cryptoServer). Acesta primeste o cerere de semnare a unui certificat si intoarce certificatul semnat. Serverul criptografic, componenta a solutiei tachoSAFE CA, utilizeaza pentru semnarea certificatelor dispozitivul hardware de tip HSM. Astfel, operatia de semnare se face exclusiv in interiorul HSM-ului, cheile de semnare nefiind expuse in exteriorul dispozitivului de semnare (HSM).

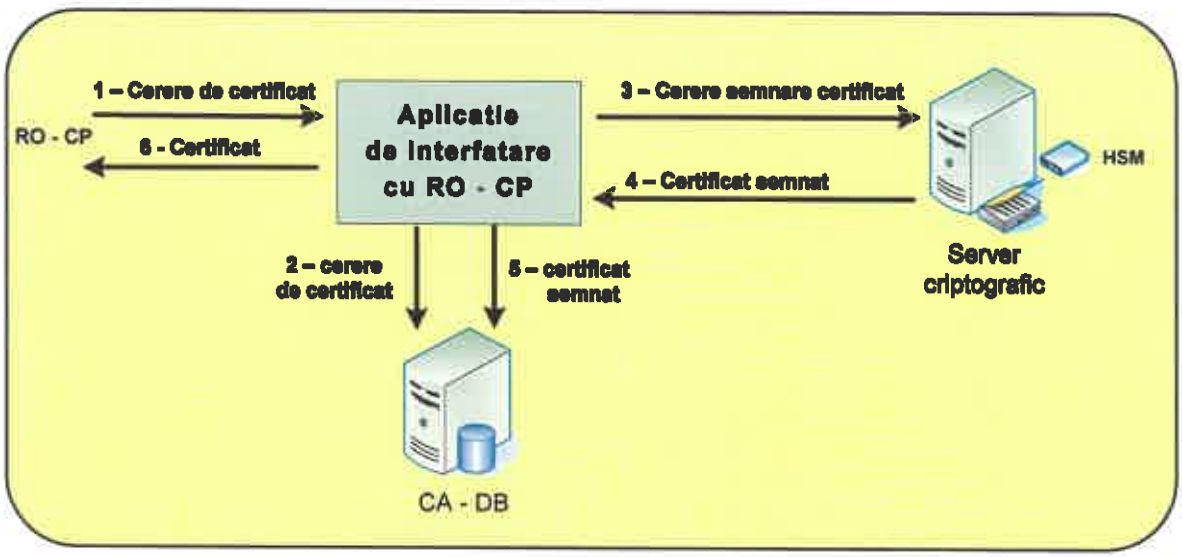
Structura certificatelor emise de MD-CA prin intermediul aplicatiei tachoSAFE CA este 100% conforma cu cerintele specificate de Reglementarea Comisiei Europene (EC) 1360/2002, Anexa IB, Appendix 11, cerintele CSM_016, CSM_017, CSM_018. Astfel, certificatele emise pentru cartelele tahografice contin identificarea tipului de echipament pentru care sunt emise (cartele tahografica de sofer, de companie, de control, sau de atelier). De asemenea, certificatele contin identificatorul autoritatii emitente (prin intermediul campului CAR – Certification Authority Reference), identificandu-se astfel inclusiv statul emitent (Republica Moldova) precum si tipul autoritatii emitente (operationala sau de test).

Verificarea certificatelor emise de aplicatia tachoSAFE CA se poate face utilizand cheia publica, pereche a cheii private (secrete) emitente, si continuta in certificatul MD.C, emis de autoritatea root europeana (ERCA). Procedura si mecanismele tehnice de verificare sunt cele descrise in Reglementarea Comisiei Europene (EC) 1360/2002, Anexa IB, Appendix 11, cerinta CSM_019.

Algoritmul de semnare a certificatelor (de test si de productie) este conform cu cerintele Reglementarii Comisiei Europene (CE) 1360/2002, Anexa IB, Appendix 11. Astfel:

- pentru semnarea certificatelor se foloseste schema de semnatura cu recuperare partiala a continutului certificatului specificata de standardul ISO/IEC 9796-2;
- de asemenea, mecanismul de semnare a certificatelor utilizeaza algoritmul de hash SHA-1;

Fluxul de emitere a certificatelor este descris in figura urmatoare:



Toate certificatele emise de catre tahcoSAFE CA pentru cartelele tahografice sunt stocate in baza de date interna a autoritatii de certificare. Pentru fiecare certificat emis, se pastreaza de asemenea cererea de certificat corespunzatoare, cu toate detaliile sale, primita de la MD-CP, pe baza careia s-a cerut emiterea acelui certificat. In felul acesta, autoritatea de certificare va pastra inregistrari cu toate cheile publice certificate precum si tipul de echipamente pentru care s-au facut acele certificari, asigurandu-se cerinta CSM_008, din Reglementarea Comisiei Europene (CE) 1360/2002, Anexa IB, Appendix 11.

2.3.4.3 Aplicatiile software ale MD-CA

Ca si aplicatii software, componente ale solutiei tachoSAFE CA, la MD-CA avem urmatoarele:

- aplicatia de server criptografic: responsabila cu gestiunea cheilor si a operatiilor criptografice;
- aplicatia de interfatare si comunicare cu MD-CP: responsabila cu interfatarea cu MD-CP, primirea cererilor de certificate de la acesta si furnizarea certificatelor;
- aplicatia de administrare si operare a tachoSAFE CA: responsabila cu operarea si administrarea tachoSAFE CA;

2.3.4.3.1 Serverul criptografic al MD-CA

Serverul criptografic asigura serviciile criptografice pentru celelalte componente ale MD-CA. Comunicatia cu serverul criptografic se desfasoara sincron prin intermediul mesajelor de tip XML, folosind o conexiune TCP/IP securizata SSL dublu autentificata.

Pentru ca o aplicatie sa poata folosi serviciile serverului criptografic, aplicatia in cauza trebuie sa se autentifice la server folosind un certificat digital valid. Certificatul prezentat de catre aplicatie este verificat in configuratia serverului pentru a stabili nivelul de acces al respectivei aplicatii.

Utilizand o conexiunea SSL dublu autentificata cu serverul criptografic se asigura astfel pentru toate informatiile schimbate cu acesta:

- confidentialitatea datelor transmise / primite de la serverul criptografic
- integritatea datelor transmise/primite de la serverul criptografic
- autenticitatea datelor transmise/primite de la serverul criptografic

Serverul criptografic este componenta care realizeaza functiile cele mai sensibile ca si nivel de securitate din cadrul MD-CA. In mare, principalele sale functionalitati sunt urmatoarele:

- generarea si stocarea, in conditii de maxima securitate a cheilor de semnare ale autoritatii de certificare
- semnarea certificatelor (de productie si de test)
- stocarea in conditii de maxima securitate a cheii simetrice KmWC care va fi inserata pe cardurile de workshop.

Operatiile criptografice sunt realizate la nivelul engine-urilor criptografice. Un engine criptografic reprezinta un store de chei impreuna cu operatiunile associate acestora. Practic pentru solutia tachoSAFE CA, un astfel de engine criptografic este gestionat prin intermediul dispozitivului hardware criptografic de tip HSM (nCipher), acreditat FIPS 140-2 level 3. Cheile de semnare ale CA –urilor vor fi stocate in aceste engine-uri. Fiecare CA (de productie sau de test) va fi gestionat

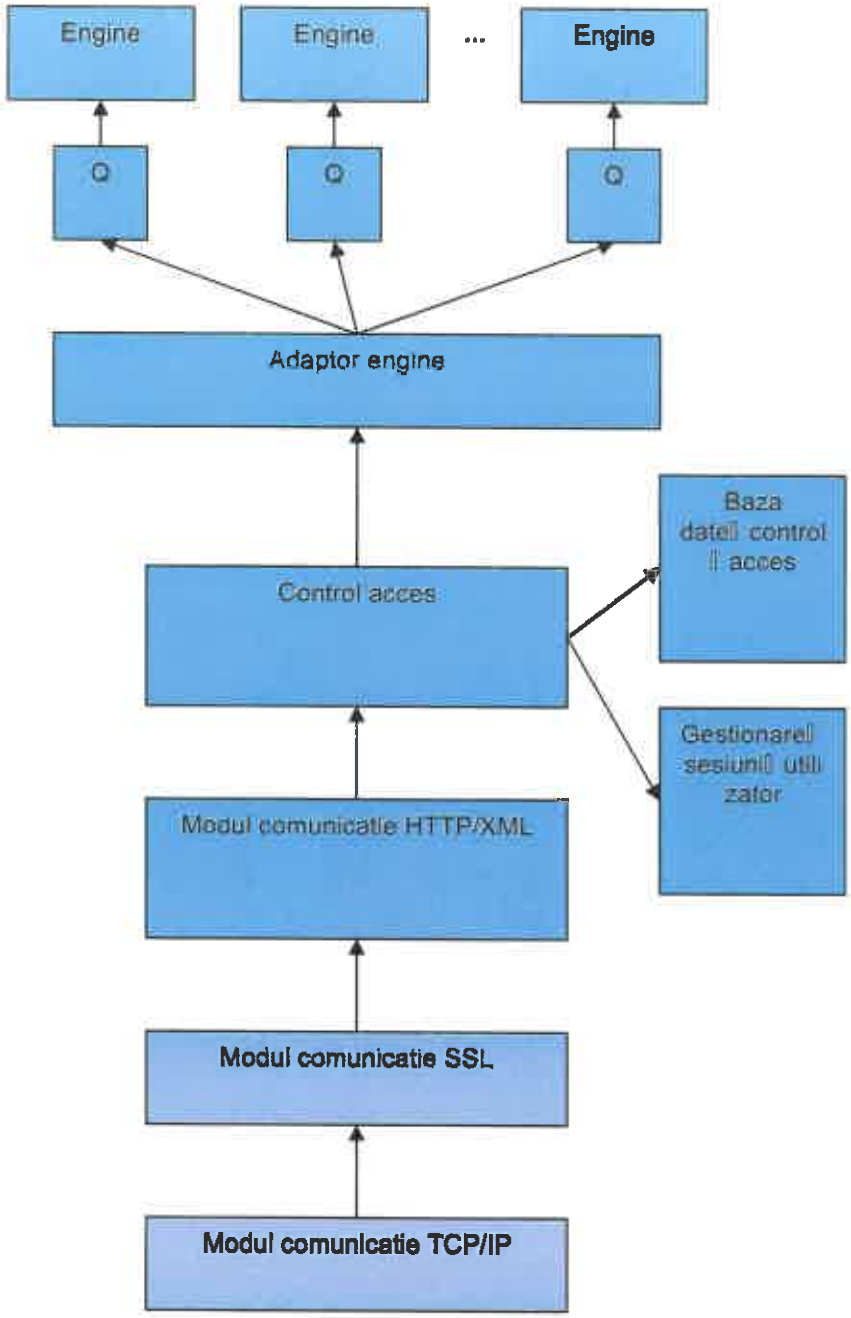
prin intermediul unui engine separat. Accesul la chei se poate face numai dupa autentificarea la aceste engine –uri de catre administratorii e chei corespunzatori.

Operatiile oferite de catre un engine criptografic sunt urmatoarele:

- login/logout (suportul pentru autorizarea de catre administratorii de chei a accesului la chei, generarea cheilor)
- generare pereche de chei (suportul pentru generarea cheilor de semnare ale CA–urilor si a cheilor asimetrice de transport)
- listare chei disponibile in engine, cautare si regasire chei
- semnare certificate (suportul pentru semnarea certificatelor)
- decriptare date (suportul pentru decriptarea datelor sensibile cum ar fi cheia simetrica destinata cardurilor de workshop – KmWC, primita de la ERCA)
- import de chei (suportul pentru stocarea cheii simetrice destinata cardurilor de workshop, KmWC).

Serverul criptografic asigura infrastructura necesara aplicatiilor pentru a putea utiliza engine-urile criptografice.

Arhitectura functionala a serverului criptografic este descrisa de figura urmatoare:



Astfel:

- Modulul comunicatie TCP/IP gestioneaza conexiunile de retea, stabilirea si inchiderea acestora, precum si situatiile de eroare. Prin intermediul sau se efectueaza comunicatia cu aplicatiile, la cel mai scazut nivel.
- Modulul comunicatie SSL realizeaza criptarea si autentificarea canalului de comunicatie, precum si verificarile legate de validitatea certificatelor digitale.

- Modulul comunicatie HTTP/XML realizeaza schimbul de pachete XML folosind protocolul HTTP, verifica validitatea acestora din punct de vedere al protocolului intern de comunicatie si asigura impachetarea/despachetarea sau codificarea/decodificarea structurilor de date unde acest lucru este necesar.
- Modulul control acces verifica daca cererile efectuate sunt facute de catre o aplicatie care are drepturi suficiente de acces. Tot aici se verifica la initierea unei noi conexiuni daca certificatul digital este prezent in listele de acces.
- Adaptorul de engine pregateste mesajele pentru a efectua operatiunile criptografice, Tot el are ca sarcina incarcarea dynamica a engine-urilor si instantierea acestora conform cu informatiile de configurare.
- Engine-ul efectueaza operatiunile criptografice propriu-zise si intoarce rezultatele acestor operatiuni in mod sincron.

Fluxul de date la nivelul serverului criptografic este urmatorul:

- Initiere conexiune:
  - Aplicatia se conecteaza la portul pe care asculta serverul criptografic
  - Se initiaza handshake-ul SSL
  - Aplicatia prezinta certificatul sau digital, serverul la randul sau prezinta propriul certificat.
  - Certificatele digitale sunt verificate pentru a se asigura ca sunt valide din punct de vedere PKI.
  - Daca este necesar, aplicatia lanseaza o cerere de log-in la engine-ul criptografic dorit (aceasta cerere se lanseaza doar in cazul nu exista o sesiune anterioara a aplicatiei de operare, in cazul in care exista o asemenea sesiune ea este refolosita)
  - In cazul in care a fost efectuata o cerere de log-in, i se remite aplicatiei identificatorul de sesiune care Il va folosi in continuare.
- Operatii criptografice:
  - Aplicatia lanseaza o cerere de operatiune criptografica pentru un anumit engine.
  - Cererea este receptionata, si se verifica validitatea sa din punct de vedere al protocolului de comunicatie XML
  - Serverul criptografic verifica pe baza datelor de conectare si pe baza identificatorului de sesiune furnizat daca aplicatia are drept de utilizare pentru engine-ul criptografic selectat.
  - In cazul in care drepturile sunt suficiente, engine-ul realizeaza operatiunile criptografice
  - Serverul impacheteaza raspunsul intr-un mesaj XML si-l remite aplicatiei.

Toate actiunile desfasurate la nivelul server-ului criptografic sunt jurnalizate, toate logurile fiind semnate digital de catre serverul criptografic pentru asigurarea integritatii si autenticitatii acestora.

2.3.4.3.2 Aplicatia de interfatare si comunicare cu MD-CP

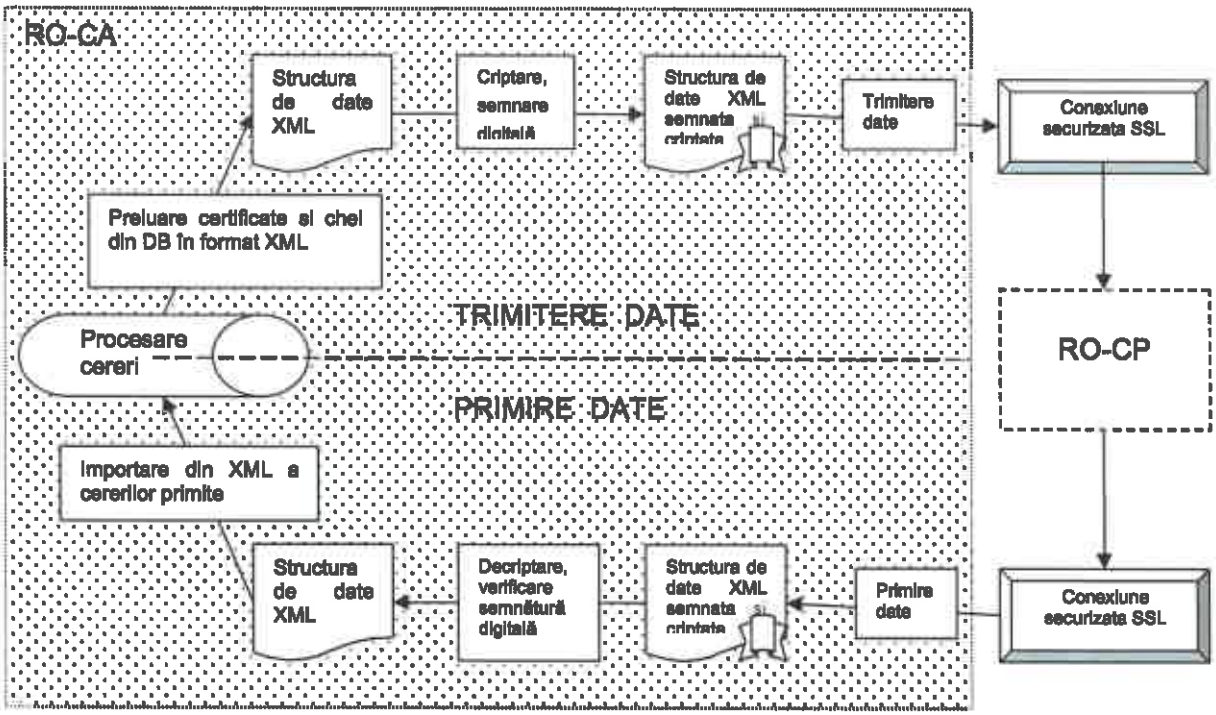
Avand in vedere ca cele doua autoritati MD-CA si MD-CP se gasesc in locatii fizice diferite si pentru a realiza un canal de comunicatie cu un grad ridicat de securitate care sa asigure transmiterea datelor in ambele sensuri: de la CA catre CP si de la CP catre CA se foloseste un canal de comunicatie securizat SSL cu autentificare mutuala bazata pe certificate digitale. Cele doua aplicatii vor avea cite un certificat digital X.509 prin intermediul carora face securizarea schimbului de informatii.

Astfel, la MD-CA va opera aplicatia de interfatare si comunicatie intre MD-CA si MD-CP care este responsabila de comunicarea automata cu o componenta speciala, similara de la MD-CP. Se asigura astfel, un serviciu de comunicatii securizate automate intre MD-CP si MD-CA, utilizand un dispozitiv de separare zone.

Securizarea schimbului de date dintre MD-CA si MD-CP este realizat de catre cele doua aplicatii de comunicare si interfatare de la MD-CA si MD-CP astfel:

- Semneaza datele de transmis cu cheia privata proprie
- Cripteaza datele de transmis cu cheia publica a celeilalte aplicatii
- Comunica prin intermediul unui dispozitiv hardware de separare zone.

In figura urmatoare este prezentat fluxul de date corespunzator aplicatiei de interfatare cu MD-CP:



Fluxul operatiilor aplicației de intefațare și comunicare cu MD-CP este urmatorul:

- Receptioneaza cererile, in forma de structuri de date XML, semnate si criptate care vin de la MD-CP. Aceste structurile de date contin cereri de certificate pentru cartele tahografice;
- Extrage si reasambleaza datele receptionate de la RO_CP;
- Decripteaza datele primite de la MD-CP;
- Verifica integritatea datelor primite de la MD-CP prin verificarea semnăturii acestora;
- Verifica structura si consistenta datelor continute in structurile XML receptionate;
- Daca toate verificarile au fost realizate cu success datele (cererile) receptionate, sunt inserate in baza de date a MD-CA si sunt furnizate modulelor de procesare ale MD-CA.
- Obtine certificatele emise pentru cartelele tahografice si le exporta în structuri de date XML. Aceste structuri de date XML vor contine pe langa certificate si id-urile cererilor pentru care s-au emis certificatele respective;
- Semneaza structurile XML folosind cheia privata proprie;
- Cripteaza structurile XML semnate cu cheia publica a aplicatiei corespondente de la MD-CP;

- Impacheteaza structurile de date XML semnate si criptate intr-un format acceptat de canalul de comunicatie realizat prin intermediul dispozitivului hardware de separare zone;
- Transmite datele astfel impachetate către MD-CP utilizând dispozitivul hardware de separare de zone;

Pentru toate transferurile de date intre MD-CA si MD-CP se genereaza jurnalizari in fisierele speciale de audit folosind modulul de logare si notificare. Sunt logate momentul de timp al evenimentului, id-uri de cereri pentru care s-a realizat transferul, rezultatul transferului (success sau fail), eventualele probleme legate de operatiile criptografice (criptare, semnare, verificare semnatura), erorile de comunicaţie, de integritate a datelor.

2.3.4.3.3 Aplicatia de administrare si operare a MD-CA

Aplicatia de administrare si operare a MD-CA este componenta prin care se pot executa functii de administrare si operare a tachoSAFE CA. Este o aplicatie web-based care permite excutarea urmatoarelor operatii:

- Generarea si administrarea CA–urilor
- Vizualizarea cererilor primite si procesate de catre tachoSAFE CA
- Vizualizarea certificatelor emise de catre tachoSAFE CA
- Gestionarea informatiilor transmise/primite de la ERCA
- Crearea si gestionarea operatorilor si a drepturilor acestora in aplicatie

Practic, aceasta este consola de lucru a tachoSAFE CA. Conectarea la aplicatie se face utilizand un browser de internet. Aplicatia permite numai conectarea prin SSL utilizand certificate digitale X.509. Autentificarea operatorilor se face pe baza de certificat digital si cheie privata RSA stocata pe token criptografic. La furnizarea de catre operator a certificatului digital pentru autentificare se face si identificarea rolului acestuia in aplicatie si implicit si a drepturilor de operare pe care le are.

Interfata grafica (consola de lucru) a aplicatiei de administrare si operare a tachoSAFE CA este in limba Romana.

Prin intermediul aplicatiei de administrare si operare se pot creea si gestiona CA –urile (de productie si de test). Operatiile care pot fi efectuate pe aceasta linie sunt urmatoarele:

- generarea cheilor CA –urilor, conform cu specificatiile din capitolul dedicat pentru "Generarea perechii de chei si a cererii de certificat pentru CA" din aceasta oferta.
- declararea CA –urilor active;
- distrugerea cheilor private care nu mai sunt active; inactivarea CA –urilor

Pentru aceste operatii, aplicatia de administrare se interfateaza cu componenta de server criptografic. Practic ea este un client pentru serverul criptografic efectuand diverse cereri catre acesta.

Prin intermediul aplicatiei de administrare si operare se pot gestiona informatiile care trebuiesc trimise catre ERCA pentru certificare precum si informatiile receptionate de la ERCA. Astfel, consola de lucru permite executarea urmatoarelor operatiuni:

- Dupa generarea cheilor de CA, din consola de administrare si operare se poate exporta cheia publica a MD-CA –ului intr-un MD.KCR, in formatul specificat de Anexa A a Politicii de Certificare a ERCA versiunea 2.1 pentru a se transmite catre ERCA pentru certificare.
- La primirea certificatului MD.C asociat cheii publice a MD-CA –ului de la ERCA, acesta poate fi importat in sistem; La importul in sistem, aplicatia verifica corespondenta cu cheia privata a MD.SK stocata pe dispozitivul HSM.
- De asemenea, aplicatia permite importul cheii publice a ERCA - EUR.PK in sistem si stocarea acesteia in conditii de maxima siguranta. Astfel, la momentul importului, aplicatia va pastra un rezumat (hash SHA-1) al acestei chei semnat cu cheia privata a MD-CA pentru a se putea valida apoi autenticitatea si integritatea sa.
- Aplicatia permite prin consola sa de lucru si utilizand componenta de server criptografic, generarea pe dispozitivul HSM, a unei perechi de chei RSA de transport a cheii simetrice KmWC destinata cardurilor de workshop, care urmeaza a fi achizitionata de la ERCA. Permite de asemnea, emiterea unei cereri KDR (Km) in formatul definit de Anexa D a Politicii de Certificare a ERCA, versiunea 2.1, pentru a fi transmisa catre ERCA in vederea obtinerii cheii KmWC.
- Aplicatia permite, prin consola sa de lucru si utilizand serverul criptografic, importul cheii simetrice KmWC extrangand aceasta cheie din KDM (Key Distribution Message) primit de la ERCA. Va stoca cheia simetrica KmWC pe dispozitivul FIPS 140-2 level 3 de tip HSM in conditii de maxima securitate. Accesul la aceasta cheie se face numai prin autentificare K/N la dispozitivul HSM. Cheia KmWC va fi distribuita catre MD-CP pentru a fi inserata pe cartelele tahografice de workshop.

Prin intermediul aplicatiei de administrare si operare se pot vizualiza in orice moment starea cererilor primite si a certificatelor emise precum si detalii despre acestea. Exista posibilitati de cautare/filtrare a acestora pentru a permite o operare cat mai facila si mai rapida.

Prin intermediul aplicatiei de adminstrare si operare se poate face gestiunea operatorilor. Astfel,

- se pot crea operatori

- se pot asocia roluri in aplicatie pentru acesti operatori conform Politicii de Certificare propuse

Toate operatiile efectuate la nivelul aplicatiei de administrare si operare sunt jurnalizate. Inregistrarile (logurile) jurnalizate de aceasta, inclusiv accesele operatorilor la aplicatie, sunt semnate digital utilizand o cheie speciala de semnare pentru a se putea verifica in orice moment integritatea si autenticitatea acestor mesaje de jurnalizare.

2.3.4.3.4 Baza de date a MD-CA

Baza de date este una dintre componentele tachoSAFE CA. Practic aceasta componenta este responsabila cu stocarea tuturor informatiilor necesare functionarii autoritatii de certificare, pastrand evidenta cererilor de certificate sosite de la MD-CP, evidenta certificatelor emise, informatii interne de administrare a autoritatii de certificare, etc.

Aplicatia permite utilizarea mai multor tipuri de sisteme de baze de date. In cazul sistemului deja implementat se foloseste un sistem de baze de date Oracle Database 10g instalat pe o platforma software de tip Suse Linux Enterprise Server.

2.3.4.3.5 Modulul de logare de la MD-CA

Modulul de logare si notificare este o componenta comuna utilizata de catre toate aplicatiile MD-CA si ofera urmatoarele functionalitati:

- permite logarea de mesaj de audit
- permite logarea de mesaje de eroare
- permite logarea de mesaje de debug
- permite trimitere mesaje e-mail de notificare administratorilor in cazul evenimentelor critice

Mesajele continute in aceste fisiere sunt in limba Romana.

Mesajele cu logurile de audit, erori si debug sunt stocate in fisiere de pe disc. Pentru asigurarea confidentialitatii, aceste fisiere pot fi criptate utilizand cheile publice ale certificatelor auditorilor si accesul la ele este permis numai acestuia. Pentru asigurarea integritatii, aceste fisiere pot fi semnate utilizand cheia private a aplicatiei respective.

Fisierele de audit inregistreaza toate operatiile efectuate si rezultatele lor. Acestea contin: numele (ID-ul) operatorului, tipul de operatie efectuata si codul de succes sau eroare corespunzator si data la care a efectuat operatia. Prin configurare, modulul poate loga orice alte informatii, la cererea beneficiarului.

Fisierele de eroare inregistreaza numai mesajele de eroare aparute in urma operatiilor efectuate. Acestea contin: numele (ID-ul) operatorului, codul de eroare si mesajul text care descrie motivul si locul unde a aparut eroarea si data la care a

efectuat operatia. . Prin configurare, modulul poate loga orice alte informatii specifice erorii, la cererea beneficiarului.

Componenta de logare utilizeaza un mecanism de rotatie a log-urilor care permite ca la un interval de timp predefinit fisierele cu logurile curente sa fie arhivate, semnate, criptate si mutate manual sau automat pe un mediu de stocare extern (CD, DVD, NAS, FTP, etc.)

Functionalitatea de trimitere mesaje de notificare permite aplicatiilor care utilizeaza modulul de logare sa trimita un e-mail sau SMS atunci cand s-a detectat un anumit eveniment in sistem. Acest mecanism permite alertarea administratorilor de securitate despre incidentele de securitate si a administratorilor de sistem despre eventualele erori sau cazuri exceptionale aparute in functionarea aplicatiei pentru a permite interventia rapida a acestora.

Componenta de logare si notificare este configurabila, parametrii de functionare fiind cititi dintr-un fisier de pe disc in format XML. Acestia specifica:

- locatia fisierelor de audit (logare) de pe disc
- intervalul de rotatie a fisierelor de audit (logare)
- certificatele auditorilor cu care sunt criptate fisierele audit (logare)
- scenariile care duc la inserarea de inregistrari in fisierele speciale de audit
- continutul inregistrarilor de audit pentru fiecare situatie in parte
- filtrele de notificari

2.3.4.4 Securitatea sistemului MD-CA

CERTSIGN va asigura gazduirea, intreţinerea, administrarea şi operarea sistemului autoritatii de certificare nationale, MD-CA, in aceleasi conditii de maximă securitate ca in prezent. Sistemul MD-CA va fi gazdui în premisele CERTSIGN din sediul aflat în Bulevardul Tudor Vladimirescu, nr. 29 A, AFI Tech Park 1, Sector 5, Bucureşti, România, CP 050881. Conditiile de securitate sunt comforme politicii de securitate *„„National Authority Policy of Republic of Moldova for the Digital Tachograph""*, aprobata de ERCA si reglementarii Comisiei Europene nr. 1360/2002, fapt confirmat prin rapoartele de audit ale sistemului tahografului digital national, incluzand sistemul centrului de personalizare MD-CP, desfasurate in anii 2009 şi 2012 de catre Ministerul Transporturilor, in calitate de MD-MSA. Sumarele de audit corespunzătoare au fost acceptate şi publicate pe site-ul ERCA: http://dtc.jrc.ec.europa.eu/dtc_audit_report_status.php.

De asemenea, asigurarea conditiilor de securitate corespunzatoare pentru sistemul autoritatii de certificare nationale, MD-CA, este certificată si prin rapoartele de audit ISO 27001 pentru sistemului de management al securitatii informatiilor obtinute de catre CERTSIN.

Securizarea sistemului MD-CA se face pe mai multe nivele. Astfel exista elemente de securitate la nivel aplicatie, la nivel retea si la nivel fizic.

2.3.4.4.1 Securitate aplicatii

La nivelul aplicatiilor securitatea este asigurata de urmatoarele elemente:

- Accesul operatorilor la aplicatia de administrare si operare se face pe baza de certificate digitale X.509 si token –uri criptografice. Dupa autentificarea pe baza de certificat, fiecare operator are asociat un rol in cadrul aplicatiei care limiteaza accesul si operarea aplicatiei de catre acesta.
- Generarea, stocarea si utilizarea cheilor private (secrete) de semnare ale CA –urilor se face numai prin intermediul dispozitivului de tip HSM, acreditat FIPS 140-2 level 3. Aceste chei nu parasesc niciodata dispozitivul HSM.
- Generarea cheilor de semnare ale CA –urilor se face numai dupa autentificarea a cel putin 3 operatori dintre care cel putin un administrator de CA. Generarea de chei se face numai dupa autentificarea administratorilor de chei la HSM, prin utilizarea smartcardurilor speciale de acces la HSM.
- Accesul la cheile de semnare ale CA –urilor se face numai dupa autentificarea de tip K/N (K >=2) a administratorilor de chei, cu control dual, prin utilizarea smartcardurilor speciale de acces la HSM.
- Cheile de semnare sunt generate si utilizate pentru perioada limitata de timp. Dupa incetarea perioadei de viata a acestora, cheile private se distrug in mod securizat de pe HSM.
- Cheia simetrica pentru cartelele de workshop (KmWC) este stocata in mod securizat pe dispozitivul HSM. Accesul la aceasta cheie pentru a fi exportata catre MD-CP se face numai dupa autentificarea administratorilor de chei (K/N), cu control dual (K>=2).
- Transportul si importul cheii publice a ERCA (EUR.PK), a certificatului digital a MD-CA (MD.C) si a cheii simetrice pentru cartelele de workshop se face cu respectarea tuturor cerintelor de securitate impuse de Reglementarea Comisiei Europene (CE) 1360/2002 si a Politicii de Certificare a ERCA, versiunea 2.1.
- Stocarea cheii publice a ERCA (EUR.PK) se face in conditii de securitate maxima care sa asigure autenticitatea si integritatea acestia.
- Toate operatiile criptografice sunt separate de restul sistemului. Ele sunt gestionate de componenta de server criptografic si sunt executate pe dispozitivul de tip HSM acreditat FIPS 140-2 level 3.
- Accesul la serverul criptografic se face numai prin SSL cu autentificare mutuala (reciproca) cu certificate digitale X.509.
- Securitatea comunicaţiei între MD-CA şi MD-CP este asigurată de Aplicaţia de interfaţare şi comunicare cu MD-CP, astfel:
    - *La nivelul de comunicatie* securitatea este asigurata folosind un canal de comunicatie securizat SSL cu autentificare mutual, bazata pe utilizarea de chei criptografice si certificate digitale.

- *La nivel software* securitatea este asigurată prin mijloace criptografice. Aplicatia dispune de propriul certificat digital si cheia privata corespunzatoare cat si de certificatul digital al aplicatiei corespondente de la MD-CP. Folosind aceste certificate aplicaţia de interfaţare va semna datele de transmis dupa care le va cripta pentru aplicatia corespondenta. La receptie aplicatia decripteaza datele si verifica semnatura aplicata de aplicatia corespondenta. Astfel sunt asigurate conditiile de confidentialitate, autenticitate si integritate a datelor vehiculate intre MD-CA si MD-CP. Astfel, orice alterare a informaţiei pe traseul dintre cele două zone va fi detectată imediat şi va fi urmată de notificări specifice către administratorii de system folosind modulul de logare si notificare

- Toate mesajele de jurnalizare (loguri) destinate auditarii sunt semnate digital pentru asigurarea integritatii si autenticitatii acestora.
- Accesul personalului in locatia de lucru a sistemului MD-CA se face controlat si este restrictionat numai pentru personalul autorizat.

2.3.4.4.2 Securitate retea

Securitatea la nivel de retea pentru MD-CA este asigurata prin masurile implementate la nivelul centrului de date ce va gazdui infrastructura hardware. Este utilizata o protectie multilayer ce asigura protectia pe mai multe nivele:

Primul nivel de protectie este asigurat de echipamentele de rutare utilizate pentru interconectare la retele publice de date Intener. Aceste echipamente asigura suplimentar fata de functionalitatile de rutare si functionalitati precum filtrare traficului prin intermediul listelor de contol al accesului, protectie DoS si spoofing.

Urmatorul nivel este asigurat prin protectie firewall stateful realizata prin echipamente dedicate ce asigura functionalitati specifice precum protectie atacuri de retea, protectie DoS si DDoS, reasamblare TCP pentru protectia pachetelor fragmentate, protectie la atacuri tip forta bruta, protectie SYN cookie, protectie IP spoofing bazata pe zone, protectie la pachete malformate

Toate echipamentele de comunicatii si serverele din data center sunt monitorizate permanent asigurandu-se interventia rapida in caz de atacuri informatice sau probleme de functionare.

Sistemul de monitorizare interogheaza sistemele MD-CA in mod activ pentru a asigura o functionare in conditii optime atat a sistemelor de operare cat si a aplicatiilor specifice care ruleaza pe acestea. Sunt monitorizati o serie de parametrii ai sistemului de operare cum ar fi: memoria RAM, incarcarea pe sistem, numarul de procese din sistem, utilizarea disk-ului dar si aplicatiile specifice platformei CA.Atacurile informatice sau problemele de functionare constituie incidente care trebuie tratate corespunzator. Fiecare incident este inregistrat intr-un registru de incidente electronic, inregistrandu-se pentru fiecare incident urmatoarele tipuri de informatii: numarul incidentului, data incidentului, descrierea

incidentului, cauza, solutia, masuri corective, data solutionarii si in functie de severitatea acestuia, entitatile instiintate (de exemplu MD-MSA, ERCA).

2.3.4.4.3 Securitate fizica

Activităţile MD-CA se desfăşoară într-un mediu de producţie special amenajat pentru a oferi cele mai bune condiţii de operare, atât din punct de vedere al sarcinilor ce trebuiesc îndeplinite zilnic cât şi din punct de vedere al securităţii.

Spaţiul de producţie se află în sediul certSIGN aflat în Bulevardul Tudor Vladimirescu, nr. 29 A, AFI Tech Park 1, Sector 5, Bucureşti, România, CP 050881. Spaţiul este mai mare de 100 de metri pătraţi, este compartimentat în mai multe camere. Într-una dintre camerela situate la subsolul cladirii este instalată o incintă ecranată cu atenuare de minim 55db în gama 1MHz-1GHz conforma standardului IEEE STD 299. Această incintă ecranată gazduieşte sistemul în condiţii de maxomă securitate sitemul autorităţii de certificare MD-CA. Detalii privind măsurătorile se găsesc anexate. Spaţiul este corespunzator din punct de vedere al iluminatului, aerisirii şi climatizării.

Politicile de acces în incintele utilizate pentru activităţile MD-CA sunt gestionate separat şi sunt diferite de politicile de acces în celelalte spaţii.

Spaţiul se află într-o clădire este amplasată într-un perimetru închis cu gard şi dotat cu echipamente de control acces pentru autovehicule, având ca dispozitiv de blocare bariere auto. Accesul autovehiculelor se face prin control dual, cartele de proximitate si agenti de paza. Accesul pietonal este de asemenea controlat la intrarea în perimetru de catre agentii de paza. Toate caile de acces catre locatia ocupata de certSIGN sunt controlate dual, cu echipamente de control acces si cu agenti de paza.

Spaţiul alocat certSIGN este prevazut cu agenţi de pază proprii şi este organizat pe trei nivele de securitate:

- la primul nivel are acces tot personalul certSIGN, pe bază de cartele de proximitate, purtand fotografia angajatului si datele de identificare ale firmei (aria delimitată este de tip „zonă administrativă")
- al doilea nivel este destinat „zonelor tehnice"
- al treilea nivel este format de „zonele de securitate-clasă 2"; accesul in aceste zone este permis pe baza acelorasi cartele de proximitate.

Incintele astfel definite, unde se instalează echipamentele de procesare date sau se păstrează documente, sunt protejate la intruziune prin instalarea de dispozitive de detecţie adecvate, care fac parte dintr-un subsistem de detecţie la efracţie. Accesul in fiecare zona de securitate este permis numai persoanelor autorizate de administratorul de securitate, prin programarea corespunzatoare a sistemului de acces fizic.

În vederea asigurării unui control complet al circulaţiei personalului propriu şi al vizitatorilor, punctele de control acces în zonele de securitate sunt supravegheate cu ajutorul unui subsistem de TVCI, care permite vizualizarea în

timp real a imaginilor culese, înregistrarea acestora, căutarea şi redarea imaginilor de la anumite momente de timp.

Conform reglementărilor în vigoare, toate încăperile şi holurile de circulaţie fac obiectul detecţiei la incendiu, detectie asigurata printr-un sistem de detecţie şi semnalizare. Accesul grupelor de intervenţie la incendiu va fi permis şi supervizat de personalul firmei de pază, cu anunţarea administratorului de securitate a certSIGN.

Sistemul de securitate pentru cladirile centrului de personalizare cuprinde: un sistem de control al accesului, un sistem CCTV (pentru supraveghere video), proceduri de a monitoriza si raporta incidentele CCTV, sisteme aritiefractie si antiincendiu

Aplicatia de management a securităţii sistemului fizic contine o baza de date in care se înregistreaza toate evenimentele din sistem (intrari/iesiri, alarme). Aplicatia contine un modul de rapoarte, utilizabil de catre administratorul de securitate (sau de catre o persoana autorizata de acesta), dupa cum urmeaza:

- rapoarte de prezenta (listeaza perioadele de timp petrecute in interiorul obiectivului pentru fiecare persoana in parte, cu posibilitatea de filtrare pe departamente/persoane si pe o anumita perioada de timp (zile/saptamani/luni);
- rapoarte de evenimente de acces, de tipul "cine, când, unde", cu posibilitatea de selectie pe anumite filtre şi într-o anumita perioada de timp ;
- rapoarte cu tentativele de acces nepermise, referitoare la situatiile cand anumite persoane incearca sa acceseze un anumit filtru la care nu au dreptul sau cand se folosesc alte cartele decat cele introduse in sistem ; acestea se asociază cu imaginile înregistrate de subsistemul de TVCI .

În scopul asigurării pazei şi securităţii bunurilor existente şi a informaţiilor există un post de pază permanent, 24/24 ore, asigurat cu agent de pază, amplasat la intrarea obiectivului, în interiorul acestuia, cu misiunea de a permite accesul autorizat în incintă a salariaţilor si a vizitatorilor. În cazul unui incident, după declansarea alarmei sosesc echipajele de interventie.

Accesul în obiectiv este controlat printr-un sistem electronic prevăzut cu uşi cu broaşte electromagnetice ce pot fi acţionate de către cititoarele de cartele de proximitate. Cartelele de proximitate sunt personalizate prin inscripţionarea unei serii unice personalizarea acestora fiind cotrolată de administratorul de securitate.

2.3.4.4.4 Securitate cibernetica

Evaluarea Vulnerabilitatilor

CERTSIGN va realiza Evaluarea Vulnerabilitatilor sistemului MD-CA, proces in cadrul caruia se va evalua nivelul de risc cu privire la fiecare vulnerabilitate identificata si se vor face recomandari de remediere.

Serviciile de evaluarea vulnerabilităților ofertate în prezentul document vor fi livrate de către experți în acest domeniu. Acest serviciu presupune realizarea mai multor tipuri de acțiuni în mod recurent, respectiv: identificarea sistemelor informatice ce trebuie scanate, prioritizarea acestora, scanarea, revizuirea rezultatelor obținute, evalurea vulnerabilităților identificate și acordarea unui indice de risc, formularea de recomandări de remediere, retestare.

În livrarea serviciului se vor utiliza instrumente automate de scanare a sistemelor MD-CA. Aplicatiile si metodele de realizare a evaluarii sunt de ultima generatie si sunt cotate ca tehnologii de varf. Modul in care se va derula evaluarea nu va impacta in niciun fel performantele sistemelor informatice evaluate si va permite descoperirea de vulnerabilitati la nivel de: sistem de operare, retea LAN, aplicatii, aplicatii web si baze de date, etc.

Ultima etapă din fiecare iterație a serviciului de evaluării de vulnerabilități va fi formularea de recomandări care să permită realizarea corecțiilor necesare pentru remedierea breșelor de securitate.

Teste de Penetrare

CERTSIGN va livra servicii de tipul Penetration Testing pentru sistemul MD-CA, care permit testarea nivelului de securitate al infrastructurii tinta prin identificarea și validarea vulnerabilităților la nivel de rețea, sistem de operare, aplicații, aplicatii web si servicii.

Testele de penetrare se vor derula cu ajutorul unor specialiști certificați, care vor utiliza aplicații comerciale dedicate de ultimă generație.

De asemenea, CERTSIGN desfășoară testele de penetrare în baza unor proceduri ce au fost concepute prin respectarea standardelor și recomandărilor în domeniu (SANS, NIST, ENISA, etc.).

În cadrul metodologiei de lucru cu privire la serviciile de penetration test au fost cuprinse următoarele etape:

- realizarea unui penetration test plan cu privire la: tipul de pentest care se va realiza (black box – din exteriorul rețelei, white box – din interiorul rețelei), sistemele care vor fi cuprinse în iterația respectivă de pentest, prioritizarea acestora, intervalul de realizare al testelor și durata acestora, strategia de comunicare în cadrul echipei de lucru, etc. De asemena, planul de penetration test va mai include o analiză de proiect la nivelul echipei CERTSIGN în care se va stabili: membrii echipei de pentest, scenariile de testare, tool-urile utilizate.

- stabilirea modului în care se va face gestionarea datelor/informațiilor sensibile ce vor fi descoperite cu privire la infrastructura MD-CA, respectiv: colectarea datelor și stocarea lor într-o formă sigură.

Fiecare pentest in parte se va incheia cu intocmirea unui raport in cadrul caruia vor fi cuprinse toate vulnerabilitatile identificate si recomandari pentru remedierea acestora.

S.C. CERTSIGN S.A.

Asigurarea reactiei la atacuri informatice

CERTSIGN va livra pentru sistemul MD-CA, servicii de reactie la atacuri informatice prin intermediul unor specialisti dedicati acestei activitati care vor realiza:

- Confirmarea atacului informatic
- Analiza probelor colectate
- Stabilirea cauzelor
- Evaluarea pagubelor
- Identificarea tuturor victimelor in reteau compromisa
- Sanitizarea retelei
- Formularea unui raport de incident

Activitatile de raspuns la incident au drept scop eradicarea unei infectii din cadrul retelei intr-un timp optim astfel incat sa fie diminuate pagubele.

Serviciile ofertate vor fi livrate conform unor proceduri de lucru interne care au fost concepute prin respectarea recomandărilor (SANS) și standardelor în domeniu (NIST Special Publication 800-137) astfel încât să se poată furniza un timp de reacție redus pentru a iniția răspunsul la potențialele incidente de securitate cibernetică.

Monitorizare a sistemelor

CERTSIGN va asigura monitorizarea sistemelor MD-CA, folosind experți specializați (analiști de securitate) în acest domeniul. Monitorizarea va realiza identificarea în mod proactiv și eficient a potențialelor amenințări informatice prin monitorizarea proactivă și continuă a activității care impacteaza sistemele informatice protejate ale MD-CA.

2.3.4.5 Infrastructura de comunicatii a MD-CA

In cladirea unde este localizat centrul de date ce va gazdui platforma MD-CA este realizata o cablare structurata de date si voce ce respecta standardele: ISO-IEC 11801, EN50173, EN50167/68/69, EIA/TIA568A, EIA/TIA 568A-5, TSB67.

Toate echipamentele sunt produse in conformitate cu standardul calitatii ISO9001.

Sistemul de cablare structurata este de categorie 5 complet modulară, având la bază conceptele actuale de cablare structurată, cu conexiuni individuale pentru fiecare post de lucru (telefon sau calculator) la tablouri de conexiuni și repartiție (patch panel-uri), și apoi către echipamente centrale (switch-uri, respectiv centrala telefonică). Reteaua este de tip switching Ethernet, cu rate de transfer de 10/100/1000 Mbps.

Cladirea centrului de date detine toate dotarile necesare unui centru informatic modern (climatizare, alimentare electrica, generator de curent, sistem de control acces, paza si protectie, supraveghere video).

Tot aici este localizat si Centrului de Monitorizare (NOC – Network Operation Center) prin intermediului caruia se asigura servicii de monitorizare si management in timp real al echipamenetelor active de retea precum si a serverelor.

2.4 Mentenanţă şi Suport Tehnic

CERTSIGN este producatorul solutiei de emitere a cartelelor tahografice, componentele tachoSAFE CIA, tachoSAFE CA si tachoSAFE TACHOnet fiind produse dezvoltate şi inregistrate la ORDA de către CERTSIGN.

CERTSIGN in calitate de producator al solutiei, va asigura inclusiv prin serviciul propriu help-desk, integral în limba Română, 24 de ore din 24, 7 zile pe saptamana, 365 zile pe an, pentru toate componentele sistemului, şi anume MD-CIA, respectiv tachoSAFE CIA, tachoSAFE TACHOnet, inclusiv birourile de inregistrare MD-CIA, şi MD-CA, respectiv tachoSAFE CA, suport tehnic şi interventie on-site in timpul programului de lucru, fara nici o limitare in numarul de interventii.

Suportul tehnic şi interventiile on-site la birourile de înregistrare ANTA se vor realiza remote, în termen de maximum 2 ore de la semnalarea problemei. În cazurile cu totul excepţionale în care intervenţia remote nu este posibila, un specialist CERTSIGN se va deplasa la biroul de înregistrare ANTA in termen de maximum 24 de ore ore de la semnalarea problemei, pentru a oferi suportul tehnic si eventuala intervenţie.

CERTSIGN are mai mult de 3 specialisti, cetăţeni Români, vorbitori nativi de limba Romana, cu experienta de cel putin 3 ani in asigurarea suportului tehnic pentru sistemele MD-CIA, inclusiv birourile de inregistrare ale MD-CIA, TACHOnet şi MD-CA. CERTSIGN va aloca pe durata contractului, cel putin 3 dintre aceşti specialisti, pentru asigurarea suportului tehnic pentru sistemele respective.

CERTSIGN va asigura pe perioada contractului mentenanta pentru componentele sistemului national de emitere a cartelelor tahografice, si anume:

- infrastructura software şi hardware a MD-CA, incluzand si infrastructura de disaster recovery;
- Infrastructura software şi hardware a MD-CIA, incluzand sistemul TACHOnet.

Suport tehnic şi mentenanţa oferita pe toata durata contractului este asigurata prin implicarea acelulaşi personal înalt calificat care a realizat dezvoltarea şi implementarea sistemelor respective.

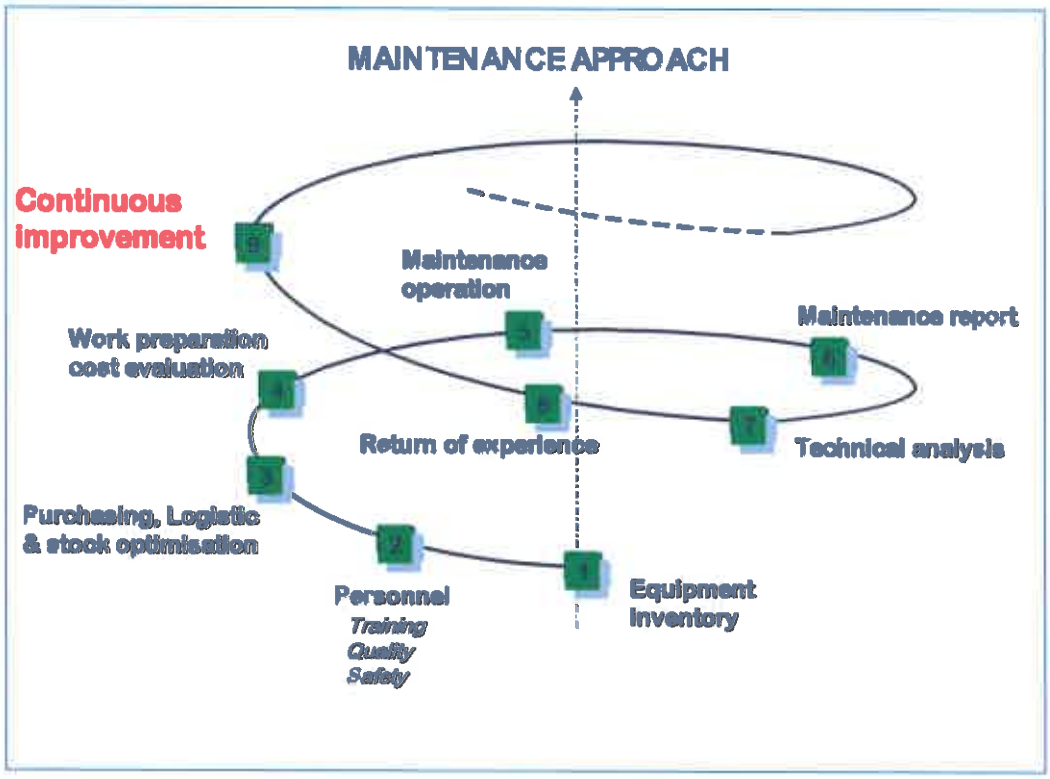
Strategia de mentenanta va fi axata pe doua mari directii:

- Mentenanta proactiva care include:
  - Un program de mentenanta preventiva

- Un program de mentenanta predictiva menit sa identifice eventuale probleme inainte ca acestea sa apara

- Mentenanta corectiva

Implementarea directiilor strategice de mai sus va fi bazata pe modelul consacrat al buclei inchise, model care are ca scop imbunatatirea continua prin intermediul experientei acumulate.



Mentenanta preventiva

Mentenanta preventiva va fi realizata asupra tuturor componentelor sistemului la intervale regulate, in functie de necesitatile fiecarei componente, care sa asigure ca sistemul functioneaza in parametrii de performanta stabiliti. Furnizorul va oferi programul de intretinere preventiva pentru fiecare componenta a sistemului.

Mentenanta preventiva are ca scop reducerea defectelor la nivelul minim posibil.

Mentenanta predictiva

Majoritatea echipamentelor ofera semne care indica o posibila defectiune viitoare. Aplicarea unei solutii de mentenanta predictiva ajuta la depistarea acestor semne si corectarea problemelor inainte ca acestea sa apara.

Mentenanta corectiva

Mentenanta corectiva asigura un raspuns rapid si organizat in momentul aparitiei unei probleme prin implementarea unui proces clar si strict de escaladare a problemelor identificate.

2.4.1 Mentenanta si suport tehnic Software

CERTSIGN va asigura suport pe toată perioada contractului atât pentru softul de bază (sisteme de operare, sisteme de gestiune a bazelor de date, etc.) cât şi pentru softul de aplicaţie al tuturor componentelor sistemului tahograf digital naţional: MD-CIA, MD-CA şi MD-CP.

Întreţinerea software este asigurată de un set de activităţi, simultan tehnice şi manageriale, care să garanteze că software-ul continuă să asigure obiectivele instituţionale şi de afaceri.

Întreţinerea software are un scop mult mai larg decât se înţelege uneori prin utilizarea termenului de corecţie a erorilor.

Aceasta înseamnă că trebuie realizate cât mai multe în faza de dezvoltare, pentru a asigura păstrarea costurilor de întreţinere cât mai scăzute cu putinţă.

A fost introdusă o metodă de mentenanţă software care permite utilizatorului să aplice schimbări în sistem. Scopul este de a asigura că schimbările minore în specificaţiile sistemului să se reflecte în schimbări minore ale aplicaţiilor, şi să nu necesite o revalidare a întregului sistem.

Oricum, o revizie a specificaţiilor înseamnă un proces complex, care presupune şi aspecte de planificare, analiză, costuri etc, dincolo de aspectele software. Adaptarea documentaţiei, re-instruirea personalului, informarea publicului, etc, sunt aspecte importante de luat în considerare înaintea migraţiei.

Pentru a păstra impactul cât mai scăzut, utilizăm o proiectare orientată pe obiecte, metode de specificare formale, programare structurată şi metode adaptate pentru testare.

Calculatoarele folosite ca staţii de lucru şi serverele sunt bazate pe o arhitectură moderna, care permite o simplificare a procedurilor de upgrade software şi de aplicare de corecţii (patches).

2.4.2 Întreţinere hardware

Pentru asigurarea serviciilor de întreţinere a echipamentelor, CERTSIGN va desfasura activităţi de întreţinere şi mentenanţă pe perioada derulării contractului. Principalele activitati de mentenanta hardware vor cuprinde:

- Activităţile si operaţiile de întreţinere necesare pentru masinile de personalizare (imprimantele de carduri si sistemul aferent)
- Activităţile si operaţiile de întreţinere necesare pentru echipamentele IT (servere, echipamente de comunicaţii, echipamente de stocare)

S.C. CERTSIGN S.A.

CERTSIGN va asigura service, mentenanţa şi suport tehnic pe durata contractului pentru toate echipamentele sistemelor MD-CIA, MD-CP şi MD-CA puse la dispoziţia ANTA.

2.4.3 Gestionarea serviciului şi help desk

CERTSIGN va forma o echipa de mentenanta cu sediul in Bucuresti. Echipa de mentenanta va fi formata din specialisti care acopera toate componentele sistemului:

- specialisti in inginerie de sistem
- specialisti in comunicatii
- specialistii in electronica
- specialisti in securitate fizica
- specialisti in securitate IT
- specialisti software

De asemenea furnizorul va numi o persoana care va coordona activitatile de mentenanta si va avea urmatoarele atributii:

- coordonarea persoanelor responsabile de mentenata
- supervizarea activitatilor
- aplicarea procedurilor
- urmarirea respectarii timpilor de interventie si rezolvare a problemelor

Furnizorul pune la dispozitia beneficiarului un serviciu de tip Call Center cu urmatoarele caracteristici:

- Disponibilitate 24 de ore pe zi, 7 zile pe saptamana
- canale de comunicare: telefon, fax, e-mail
- Echipa Call Center va receptiona problemele semnalate de Beneficiar si le va trimite catre echipa de mentenanta
- Fiecare problema semnalata va avea un numar unic de inregistrare, numar cunoscut atat de Beneficiar cat si de Furnizor

Procedura de lucru

Procedura de lucru constă în succesiunea următoarelor activităţi:

1. preluarea şi înregistrarea solicitării beneficiarului

Pentru preluarea tuturor solicitărilor de intervenţie a echipei Furnizorului asupra sistemului aplicativ pe perioada de mentenanţă, beneficiarul va folosi serviciul **de help desk.**

Serviciul este disponibil în limba Română, 24h pe zi, 7 zile pe săptămână, 365 zile pe an.

Solicitările vor fi preluate de un operator specializat şi transmise imediat persoanelor responsabile din cadrul echipei d eintervenţie. Fiecare apel înregistrat

va primi un ID unic după care beneficiarul va putea să verifice stadiul de rezolvare a solicitării sale.

Informaţiile pe care le va prelua operatorul de la beneficiar sunt:

- Denumirea şi adresa obiectivului
- Numele şi funcţia persoanei care anunţă incidentul
- Numărul de telefon la care poate fi contactată persoana care a anunţat incidentul
- Descrierea incidentului

2. Identificarea şi remedierea incidentului de către echipa de mentenanţă desemnată

Solicitările preluate de operator sunt transmise specialiştilor desemnaţi pentru prestarea activităţilor de mentenanţă care vor lua legătura cu persoana ce a semnalat incidentul pentru a obţine detalii despre incident.

Dacă se va considera că incidentul se încadrează în alt domeniu decât cel specificat iniţial de solicitant, specialistul va lua legătura cu responsabilul desemnat pentru acel domeniu.

Pe baza informaţiilor primite de la solicitant (inclusiv gradul de urgenţă), specialistul va decide acordarea suportului telefonic sau deplasarea la sediul beneficiarului pentru identificare mai exactă a incidentului.

Solicitantul va completa o fişă de intervenţie, precizând detalii despre incident, de către cine şi când a fost semnalat, alte informaţii şi o va transmite echipei de mentenanţă.

3. Închiderea problemei semnalate

După preluarea sesizării şi a detaliilor despre incident (telefonic sau prin prezenţa la sediul beneficiarului) de către echipa de intervenţie, se va încerca rezolvarea problemei în cel mai scurt timp.

Se va solicita semnătura beneficiarului pentru închiderea fişei de intervenţie. În unele cazuri se poate ca incidentul semnalat de beneficiar să fie o problemă falsă sau o greşeală de utilizare, administrare sau configurare a sistemului, greşeală efectuată de beneficiar. Acest lucru se va consemna în fişa de intervenţie.

Folosind serviciul help desk CERTSIGN va asigura suport tehnic in limba Romana pe toată perioada contractului pentru:

- Aplicatia web de inregistrare a aplicantilor si gestiune a cartelelor tahografice
- Aplicatia de interfatare & validare / notificare cu serviciul TACHOnet
- Aplicatia de interfatare si comunicare cu MD-CP

Furnizorul va asigura suport pe toată perioada contractului la sediul DataCenter-ului MD-CIA sau a birourile MD-CIA, in functie do situatie, pentru toate problemele care nu au putut fi rezolvate prin serviciul callcenter, pentru:

S.C. CERTSIGN S.A. BUCUREŞTI - ROMÂNIA

- Apicatia web de inregistrare a aplicantilor si gestiune a carteletor tahografice
- Aplicatia de interfatare & validare / notificare cu serviciul TACHOnet
- Aplicatia de interfatare si comunicare cu MD-CP

2.5 Training

CERTSIGN oferă după fiecare actualizare a platformei hardware si software a MD-CIA servicii de şcolarizare (cursuri) în limba Română pentru specialiştilor IT&C si utilizatorii din cadrul ANTA pentru a putea utiliza în condiţii optime soluţia implementată.

Programul de instruire se va desfăşura fie online, folosind o platforma pusă la dispoziţie de CERTSIGN (ex. Microsoft Teams), fie la sediul ANTA din Republica Moldova mun. Chişinău str. Aleea Gării, 6, în condiţiile în care evoluţia actualei pandemii o va permite. Participarea la curs include suportul de curs în limba Română.

Cursurile vor fi organizate pentru operatorii MD-CIA, în regimul "train the trainers"

Pentru persoanele responsabile cu instruirea operatorilor MD-CIA o grupa se constituie cu minimum 2 participanti şi maxim 5. In functie de modificarile facute platformei MD-CIA cursul poate dura intre 1 si 3 zile.

Obiective

- Dobândirea de cunoştinţe pentru operarea aplicaţiei web de înregistrare, emitere si gestiune a cartelelor tahografice;
- Transmiterea către MD-CP a cererilor obţinerea cartelelor tahografice;
- Primirea cartelelor şi a codurilor PIN şi distribuirea acestora către aplicanţi;
- Transmiterea cunoştinţelor dobândite către operatorii MD-CIA.

Pentru persoanele responsabile cu întreţinerea şi administrarea MD-CIA o grupa se constituie cu minimum 2 participanti şi maxim 5. In functie de modificarile facute platformei MD-CIA cursul poate dura intre 1 si 3 zile, se desfasoara in intervalul 9.00-17.00 si include o pauza de pranz de o ora si doua pauze de cafea.

Obiective

- Administrarea aplicaţiei web de înregistrare a aplicanţilor şi gestiunea cartelelor tahografice
- Administrarea bazelor de date ale sistemului
- Administrarea aplicaţiei de interfaţare şi comunicare cu MD-CP
- Administrarea aplicaţiei de interfaţare cu TACHOnet
- Administrarea aplicaţiei de validare automată a datelor aplicanţilor

3 Răspuns punct cu punct

Cerinţa impusă în documentaţia de atribuire		Comformitate cu cerinţa	Mod de îndeplinire
Suplimentar, ofertantul trebuie să întrunească următoarele cerinţe obligatorii:			
1	Ofertantul trebuie să dovedească faptul că a implementat sisteme complete de emitere şi gestiune a cartelelor tahografice si ca emite cartei tahografice pentru cel puţin 3 state dintre care cel puţin un stat membru UE.	**DA**	CERTSIGN a implementat sisteme complete de emitre şi gestiune a cartelelor tahografice in Romania, Moldova, Ucraina, Cipru, Bulgaria, Serbia, Uzbekistan şi Tajikistan. CERTSIGN emite cartele tahografice pentru Romania, Cipru (state membre UE) şi Moldova, Ucraina, Uzbekistan şi Tajikistan. A se vedea *Capitolul 1.1 CERTSIGN S.A.* al prezentei oferte şi recomandările ataşate ofertei.
2	Ofertantul trebuie să pună la dispoziţia Autorităţii Contractante pe întreaga durată a contractului infrastructura hardware şi software necesară funcţionării sistemului tahograf digital la nivel naţional, pentru emiterea şi gestiunea de carduri tahografice	**DA**	CERTSIGN va pune la dispoziţia Autorităţii Contractante pe întreaga durată a contractului infrastructura hardware şi software necesară funcţionării sistemului tahograf digital la nivel naţional, pentru emiterea şi gestiunea de carduri tahografice. Sistemul care va fi pus la dispoziţia ANTA este sistemul deja implementat şi utilizat şi în present de către ANTA pentru emiterea şi gestiunea de cartele tahografice. A se vedea *capitolul 2.1 Conţinutul Ofertei* al prezentei oferte.
3	Ofertantul trebuie să asigure operarea întregii infrastructuri hardware şi software a sistemului pentru emiterea şi gestiunea de carduri tahografice, cu excepţia infrastructurii	**DA**	CERTSIGN va asigura operarea întregii infrastructuri hardware şi software a sistemului pentru emiterea şi gestiunea de

	aferente birourilor de înregistrare a solicitărilor de carduri tahografice, care va fi operate de către personalul Autorității administrative "Agenția Națională Transport Auto", în continuare ANTA.		carduri tahografice, cu excepția infrastructurii aferente birourilor de înregistrare a solicitărilor de carduri tahografice, care va fi operată de către personalul ANTA. A se vedea *capitolul 2.1 Conținutul Ofertei* al prezentei oferte.
4	Ofertantul trebuie sa asigure întreținerea și actualizarea tuturor componentelor infrastructurii sistemului pentru emiterea și gestiunea de carduri tahografice pentru a respecta în totalitate cerințele specificate în prezentul caiet de sarcini cît și noile cerințe elaborate la nivelul Uniunii Europene și AETR în acest domeniu.	**DA**	CERTSIGN va asigura întreținerea și actualizarea tuturor componentelor infrastructurii sistemului pentru emiterea și gestiunea de carduri tahografice pentru a respecta în totalitate cerințele specificate în prezentul caiet de sarcini cît și noile cerințe elaborate la nivelul Uniunii Europene și AETR în acest domeniu. A se vedea *capitolele 2.1 Conținutul Ofertei* și *2.4 Mentenanță și Suport Tehnic* ale prezentei oferte.
5	Ofertantul trebuie să asigure trainingul și suportul tehnic în limba Română pentru operarea aplicației ANTA la nivelul birourilor de înregistrare.	**DA**	CERTSIGN, în calitate de producător al soluției oferite, va asigura trainingul și suportul tehnic în limba Română pentru operarea aplicației ANTA la nivelul birourilor de înregistrare. A se vedea *capitolele 2.1 Conținutul Ofertei* și *2.5 Training* ale prezentei oferte.
6	Având în vedere faptul că întreruperea furnizării de carduri tahograf către solicitanți (conducătorii auto, companii, ateliere și organele de control) ar duce la perturbarea activităților de transport rutier în Republica Moldova și ar produce daune importante companiilor de transport și conducători auto care efectuează transport internațional, se impune ca ofertantul să asigure continuitatea procesului de emitere de carduri personalizate pentru tahograful digital în	**DA**	Prin soluția propusă în prezenta ofertă CERTSIGN S.A. asigură realizarea integrală a obiectivelor autorității contractante, și anume continuitatea procesului de emitere de carduri personalizate pentru tahograful digital în Republica Moldova pentru conducătorii auto, companii, ateliere și organele de control, astfel încât să nu se perturbe activitățile de

	Republica Moldova.		transport rutier în Republica Moldova şi să nu se producă daune companiilor de transport şi conducătorilor auto care efectuează transport internaţional. CERTSIGN va asigura continuitatea functionarii sistemului de emitere si gestiunea a cartelelor tahografice, cât şi emiterea fără intreruperi pe toată durata contractului, începând cu prima zi de la intrarea în vigoare a acestuia, a cartelelor Tahografice personalizate. A se vedea *capitolul 2.1 Conţinutul Ofertei* al prezentei oferte.
7	În acest scop, ofertantul trebuie să: - emită primele carduri personalizate, în conformitate cu toate reglementările AETR şi ale Uniunii Europene în domeniu, cât şi cu cerinţele din prezentul caiet de sarcini, în termen de maximum 10 zile de la data intrării în vigoare a contractului;	**DA**	Prin punerea la dispoziţia ANTA în vederea utilizării pe durata contractului a sistemului folosit şi in prezent cât şi furnizarea aceloraşi tipuri de cartele tahograf, deja certificate, CERTSIGN va emite primele carduri personalizate, în conformitate cu toate reglementările AETR şi ale Uniunii Europene în domeniu, cât şi cu cerinţele din prezentul caiet de sarcini, în termen de **maxim 1 zi** de la data intrării în vigoare a contractului. A se vedea *capitolul 2.1 Conţinutul Ofertei* al prezentei oferte.
8	În acest scop, ofertantul trebuie să: - asigure gestiunea tuturor cardurilor tahograf emise în Republica Moldova începînd cu luna Decembrie 2010 şi pană în prezent, cât şi a cardurilor care urmează să fie emise pe durata contractului	**DA**	Prin punerea la dispoziţia ANTA în vederea utilizării pe durata contractului a sistemului folosit şi in prezent, CERTSIGN va asigura gestiunea tuturor cardurilor tahograf emise în Republica Moldova începînd cu luna Decembrie 2010 şi pană în prezent, cât şi a cardurilor care urmează să fie emise pe durata contractului. Cardurile emise începand cu luna

			Decembrie 2010 se regasesc deja in baza de date a sistemului, fiind vorba de acelaşi sistem, cu aceeaşi bază de date. A se vedea *capitolul 2.1 Conţinutul Ofertei* al prezentei oferte.
9	În acest scop, ofertantul trebuie să: - asigure continuitatea schimbului de informaţii cu autorităţile naţionale din celelalte state participante în sistemul tahografului digital, fără întreruperi, prin intermediul sistemului TACHOnet, începând cu data intrării în vigoare a contractului	**DA**	Prin punerea la dispoziţia ANTA în vederea utilizării pe durata contractului a sistemului folosit şi în prezent, CERTSIGN va asigura continuitatea schimbului de informatii cu autoritatile nationale din celelalte state participante in sistemul tahografului digital, fără întreruperi, prin intermediul serviciului TACHOnet, începând cu data intrării în vigoare a contractului. A se vedea *capitolul 2.1 Conţinutul Ofertei* al prezentei oferte.
10	În acest scop, ofertantul trebuie să: - asigure emiterea neîntreruptă de cartele tahografice personalizate pe toată durata contractului, conform comenzilor transmise de către ANTA	**DA**	Prin punerea la dispoziţia ANTA în vederea utilizării pe durata contractului a sistemului folosit şi în prezent cât şi furnizarea aceloraşi tipuri de cartele tahograf, deja certificate, CERTSIGN asigură emiterea neîntreruptă de cartele tahografice personalizate pe toată durata contractului, conform comenzilor transmise de către ANTA, sistemul fiind deja cunoscut şi rodat de catre ANTA prin utilizarea zilnică a acestuia în ultimii 10 ani. A se vedea *capitolul 2.1 Conţinutul Ofertei* al prezentei oferte.
11	cardurile tahografice furnizate pe toată durata contractului trebuie să fie certificate la nivel European, să albă un design similar actualelor cartele tahografice emise în Republica	**DA**	CERTSIGN va furniza pe toată durata contractului carduri tahografice certificate la nivel European. Acestea vor avea un design

	Moldova conform *specificației tehnice - Design & Layout Personalizare Cartele Tahografice*, să fie fabricate din același material, și anume policarbonat, să fie personalizate prin aceeași tehnologie, și anume gravare laser, cu respectarea layout-ului de personalizare al actualelor carduri de tahograf digital.		similar actualelor cartele tahografice emise în Republica Moldova, sunt conforme specificațiilor tehnice aprobate pentru Republica Moldova, vor fie fabricate din același material, și anume policarbonat, și vor fi personalizate prin aceeași tehnologie, și anume gravare laser, cu respectarea layout-ului de personalizare al actualelor carduri de tahograf digital. A se vedea *capitolele 2.1 Conținutul Ofertei, 2.2 Cartele tahografice și Anexa 1: Descrierea Tehnică a Cartelelor Tahografice oferite pentru Sistemul Tahograf Digital al Republicii Moldova* ale prezentei oferte.
12	Pentru a asigura emiterea neîntreruptă a cartelelor tahografice în Republica Moldova, ofertantul trebuie să dovedească faptul că poate furniza carduri tahografice personalizate, certificate la nivel European, cu respectarea tuturor cerințelor. În acest scop, ofertantul va prezenta type approval-ul pentru cardurile tahografice oferite și cîte o mostră de cartelă tahografică personalizată funcțională pentru fiecare tip de cartelă, si anume: *o mostră de cartelă de conducător auto, o mostră de cartelă de companie, o mostră de cartelă de control și o mostră de cartelă de agent economic autorizat împreună cu scrisoarea de PIN aferentă*;	**DA**	Pentru a demonstra faptul ca CERTSIGN poate asigura emiterea neîntreruptă în Republica Moldova a cartelelor tahografice personalizate, certificate la nivel European, cu respectarea tuturor cerințelor, prezentăm atașate acestei oferte: ▪ Certificatului de Securitate: *BSI-DSZ-CC-0272-2004 for TCOS tachograph card Version 1.0 Release 2* ▪ Fogra test report 24509 for type of cards PCS-C-ID1-01A/MDA_eTG/TP97172 ▪ Certificatului de Functionalitate: *Functional Certificate for TCOS Tachograph-AETR for Moldova* ▪ Certificatului de Interoperabilitate: *Interoperability Certificate Nº. JRC_DTC/AC-040/058/MA01/2010* ▪ Type Approval-ul cardurilor tahografice pentru Republica Moldova:

			*Bauartgenehmigung Nr. / Approval No.: e1*209*01* ▪ mostre de cartele tahografice personalizate funcţionale pentru fiecare tip de cartelă, si anume: o mostră de cartelă de conducător auto o mostră de cartelă de companie o mostră de cartelă de control o mostră de cartelă de agent economic autorizat împreună cu scrisoarea de PIN aferentă A se vedea certificatele, inclusiv Type Approval-ul şi scanurile după mostrele de cartele tahografice personalizate funcţionale şi implicuite ataşate prezentei ofertei. La cererea autorităţii contractante CERTSIGN S.A. va transmite fizic mostrele de cartele tahografice personalizate funcţionale împreună cu scrisoarea de PIN aferentă cartelei de agent economic autorizat.
13	Ofertantul trebuie să ofere o soluţie de disaster recovery pentru toate componentele sistemului pentru ANTA, care să poată prelua activitatea oricărei componente a site-ului principal de producţie în mai puţin de 24 de ore de la producerea evenimentului. Soluţia de disaster recovery trebuie să fie operaţională pe întreaga perioadă de derulare a contractului.	**DA**	CERTSIGN S.A. poseda o solutie de disaster recovery utilizată şi în prezent pentru toate componentele sistemulu de emitere cartele tahografice, şi anume: MD-CIA, MD-CA si MD-CP. Soluţia de disaster recovery oferită poate prelua activitatea oricarei componente a site-ului principal de productie in mai putin de 24 de ore de la producerea catastrofei. Componentele solutiei de disaster recovery sunt localizate în Constanta, la o distanta de peste 200 km fata de locatia principala de producţie din Bucuresti. CERTSIGN oferă aceeaşi soluţie de disaster

			recovery, pusă și în prezent la dispoziția ANTA, pentru toate componentele sistemului, care poate prelua activitatea oricărei componente a site-ului principal de producție în mai puțin de 24 de ore de la producerea evenimentului. Soluția de disaster recovery va fi operațională pe întreaga perioadă de derulare a contractului. A se vedea *capitolul 2.1 Conținutul Ofertei* al prezentei oferte.
14	Ofertantul va implementa și opera toate componentele sistemului, ANTA, cu respectarea strictă a tuturor cerințelor de Securitate specificate în politica de securitate *National Authority Policy of Republic of Moldova for the Digital Tachograph System*. Toate sistemele ANTA trebuie protejate de o infrastructură de securitate care să se asigure respectarea tuturor cerințelor stipulate în politica de securitate *„National Authority Policy of Republic of Moldova for the Digital Tachograph"*, aprobata de ERCA, în politica de securitate a ERCA, în Acordul AETR, appendix IB, și să asigure securitatea cibernetică a acestor sisteme ținând cont de noile amenințări cibernetice;	**DA**	CERTSIGN va implementa și opera toate componentele sistemului pus la dispoziția ANTA, respectiv MD-CIA, MD-CA și MD-CP, cu respectarea strictă a tuturor cerințelor de securitate specificate în politica de securitate *National Authority Policy of Republic of Moldova for the Digital Tachograph System*. Toate sistemele puse la dispoziția ANTA pe durata contractului vor fi protejate de o infrastructură completă de securitate care asigură respectarea tuturor cerințelor stipulate în: ▪ politica de securitate *„National Authority Policy of Republic of Moldova for the Digital Tachograph"*, aprobata de ERCA ▪ politica de securitate a ERCA, *Digital Tachograph System European Root Policy Version 2.1* ▪ Acordul *AETR, appendix IB*. Această infrastructură de securitate asigură și securitatea cibernetică a acestor sisteme ținând cont de noile amenințări cibernetice.

			A se vedea *capitolele 2.1 Conținutul Ofertei, 2.4.2.4 Securitatea sistemului MD-CIA, 2.4.3.7 Securitatea sistemului MD-CP, 2.4.4.4 Securitatea sistemului MD-CA* ale prezentei oferte, și *Certificatul ISO 27001* atașat ofertei.
15	Ofertantul, în calitate de furnizor de servicii de personalizare de cartele tahografice, trebuie să prezinte codul de practici și proceduri corespunzător pentru ANTA.	**DA**	CERTSIGN, în calitate de furnizor de servicii de personalizare de cartele tahografice, a implementat, operează și va opera și în continuare sistemul MD-CP conform codului de practici și proceduri: *„Sistemul de Tahograf Digitale pentru Republica Moldova, Codul de Practici si Proceduri pentru operarea MD-CP"*. Documentul *„Sistemul de Tahograf Digitale pentru Republica Moldova, Codul de Practici si Proceduri pentru operarea MD-CP"* este anexat prezentei oferte.
16	Ofertantul, în calitate de furnizor de servicii de certificare pentru cartelele tahografice, trebuie să prezinte codul de practice și proceduri corespunzător pentru ANTA.	**DA**	CERTSIGN, în calitate de furnizor de servicii de certificare pentru cartelele tahografice, a implementat, operează și va opera și în continuare sistemul MD-CA conform codului de practici și proceduri: *„Sistemul de Tahograf Digital pentru Republica Moldova, Codul de Practici și Proceduri pentru implementarea Politicii de Certificare a MD-CA si operarea MD-CA"*. Documentul *„Sistemul de Tahograf Digital pentru Republica Moldova, Codul de Practici și Proceduri pentru implementarea Politicii de Certificare a MD-CA si operarea MD-CA"* este anexat prezentei oferte.
Cerințe pentru sistemul de înregistrare, gestiune și emitere de carduri tahograf			
17	Ofertantul trebuie să asigure pe durata contractului upgrade-	**DA**	CERTSIGN S.A., în calitate de producătoare a

	ul aplicațiilor software ale ANTA comform noilor cerințe care vor fi elaborate la nivel European, AETR și național, cît și de către Autoritatea Contractantă, fără întreruperea activității de înregistrare și furnizare a cartelelor tahografice de către ANTA și fără costuri suplimentare. În acest scop, ofertantul trebule să dovedească capabilitatea de a asigura upgrade-ul aplicațiilor software ale ANTA		sistemului tachoSAFE, este în masură să asigure și va asigura pe durata contractului upgrade-ul aplicațiilor software ale sistemului pus la dispoziția ANTA comform noilor cerințe care vor fi elaborate la nivel European, AETR și național, cît și a cerințelor Autorității Contractante, fără întreruperea activității de înregistrare și furnizare a cartelelor tahografice de către ANTA și fără costuri suplimentare. Pentru a demonstra calitatea de producător al sistemului pus la dispoziția ANTA și capabilitatea de a asigura upgrade-ul aplicațiilor software ale sistemului, atașăm prezentei oferte *Certificatul de înregistrare în Registrul Național al Programelor pentru Calculator* emis de către Oficiul Român pentru Drepturile de Autor, ORDA, corespunzător aplicațiilor *tachoSAFE*. A se vedea *capitolele 2.1 Conținutul Ofertei* și *2.3.2 MD-CIA* ale prezentei oferte, și *Certificatul ORDA* atașat ofertei.
18	Ofertantul trebule să asigure pe durata contractului mentenanța și suportul tehnic al sistemului pentru înregistrarea de cereri carduri tahograf digital, emitere carduri și gestiune a cardurilor emise de către ANTA. În acest scop, ofertantul trebule să dovedească capabilitatea de a asigura mentenanța și suportul tehnic al sistemului ANTA	**DA**	CERTSIGN S.A., în calitate de producator al sistemului tachoSAFE pus la dispoziția ANTA, inclusiv a aplicatiilor tachoSAFE MD-CIA, tachoSAFe TACHOnet și tachoSAFE ProxyTACHOnet, este în măsură să asigure și va asigura pe durata contractului mentenanța și suportul tehnic în limba Română al sistemului pentru înregistrarea de cereri carduri tahograf digital, emitere carduri și gestiune a cardurilor emise de către ANTA. Pentru a demonstra calitatea de producător al sistemului pus la dispoziția ANTA și

			capabilitatea de a asigura mentenanța și suportul tehnic de la producător pentru sistem, atașăm prezentei oferte *Certificatul de înregistrare în Registrul Național al Programelor pentru Calculator* emis de către Oficiul Român pentru Drepturile de Autor, ORDA, corespunzător aplicațiilor *tachoSAFE*. A se vedea *capitolele 2.1 Conținutul Ofertei* și *2.4 Mentenanță și Suport Tehnic* ale prezentei oferte, și *Certificatul ORDA* atașat ofertei.
19	Ofertantul trebuie să asigure pe durata contractului infrastructura tehnică necesară conectării sistemului gestionat de ANTA la sistemul European TACHOnet prin punctul de acces al unui stat membru UE la rețeaua privată a Uniunii Europene, sTESTA	**DA**	CERTSIGN S.A. va asigura pe durata contractului infrastructura tehnică necesară conectării sistemului gestionat de ANTA la sistemul European TACHOnet prin punctul de acces al unui stat membru UE, respectiv România, la rețeaua privată a Uniunii Europene, sTESTA. Conectarea este deja realizată și ANTA are deja acces la sistemul European TACHOnet prin punctul de acces la rețeaua sTESTA al României folosind sistemul pus la dispoziție de CERTSIGN. CERTSIGN va pune la dispoziția ANTA, pe durata contractului, aceeași infrastructura tehnică pentru conectarea la TACHOnet. A se vedea *capitolele 2.1 Conținutul Ofertei* și *2.3.2.3.2 Aplicația de interfațare cu sistemul TACHOnet* ale prezentei oferte.
20	Ofertantul trebuie să asigure pe durata contractului upgrade-ul aplicațiilor software pentru verificarea și validarea cererilor aplicanților la nivel european, prin interfațarea cu sistemul TACHOnet, conform noilor specificații și cerințe care vor fi elaborate la nivel European. În acest scop, ofertantul trebuie	**DA**	CERTSIGN S.A., în calitate de producatoar al sistemului tachoSAFE TACHOnet, va asigura pe durata contractului upgrade-ul aplicațiilor software pentru verificarea și validarea cererilor aplicanților la nivel european, prin

	să dovedească capabilitatea de a asigura upgrade-ul aplicațiilor software ale sistemului TACHOnet național		Interfațarea cu sistemul TACHOnet, conform noilor specificații și cerințe care vor fi elaborate la nivel European. Pentru a demonstra calitatea de producător al sistemului pus la dispoziția ANTA și capabilitatea de a asigura upgrade-ul aplicațiilor software ale sistemului TACHOnet național, atașăm prezentei oferte *Certificatul de înregistrare în Registrul Național al Programelor pentru Calculator* emis de către Oficiul Român pentru Drepturile de Autor, ORDA, corespunzător aplicațiilor *tachoSAFE*, care include și componentele software *tachoSAFE TACHOnet*. A se vedea *capitolul 2.1 Conținutul Ofertei* al prezentei oferte și *Certificatul ORDA* atașat ofertei.
21	Ofertantul trebuie să asigure pe durata contractului mentenanța și suportul tehnic al aplicațiilor software pentru verificarea și validarea cererilor aplicanților la nivel european, prin interfațarea cu sistemul TACHOnet. În acest scop, ofertantul trebuie să dovedească capabilitatea de a asigura mentenanța și suportul tehnic al sistemului TACHOnet național	**DA**	CERTSIGN S.A., în calitate de producatoar al sistemului tachoSAFE TACHOnet, va asigura pe durata contractului mentenanța și suportul tehnic, în limba Română, al aplicațiilor software pentru verificarea și validarea cererilor aplicanților la nivel european, prin interfațarea cu sistemul TACHOnet. Pentru a demonstra calitatea de producător al sistemului pus la dispoziția ANTA și capabilitatea de a asigura mentenanța și suportul tehnic de la producător al acestor aplicații software, atașăm prezentei oferte *Certificatul de înregistrare în Registrul Național al Programelor pentru Calculator* emis de către Oficiul Român pentru Drepturile de Autor, ORDA, corespunzător aplicațiilor *tachoSAFE*, care include și componentele software

			tachoSAFE TACHOnet. A se vedea *capitolele 2.1 Conținutul Ofertei* și *2.4 Mentenanță și Suport Tehnic* ale prezentei oferte, și *Certificatul ORDA* atașat ofertei.
Cerințe pentru sistemul Autorității de Certificare			
22	Având în vedere faptul că în perioada de derulare a Contractului la nivelul Uniunii Europene, posibil va fi introdusă noua generație de tahografe digitale și noua generație de carduri pentru tahograful digital care vor include noi mecanisme criptografice și o structură modificată a sistemului de fișiere, Ofertantul va trebuie să: - realizeze tranziția la noua generație de carduri tahografice, fără a depăși termenele impuse de Acordul AETR și Reglementările Europene în acest sens. Ofertantul va trebui să obțină și să prezinte Autorității Contractante Type Approval-ul corespunzător noilor carduri în acest termen.	**DA**	În cazul în care în perioada de derulare a Contractului va fi luată decizia introducerii la nivelul statelor AETR a noii generații de tahografe digitale și a noii generații de carduri pentru tahograful digital, care vor include noi mecanisme criptografice și o structură modificată a sistemului de fișiere, CERTSIGN va upgrada sistemul pentru emiterea de carduri tahograf pentru republica Moldova și va realiza tranziția la noua generație de carduri tahografice, fără a depăși termenele impuse de Acordul AETR și Reglementările Europene în acest sens. Pentru a realiza tranziția la noua generație de carduri tahografice, CERTSIGN va: ▪ dezvolta cardurile tahografice de generația a doua pentru Republica Moldova și va obține și prezinta Autorității Contractante Type Approval-ul pentru aceste carduri în termenele impuse de Acordul AETR și Reglementările Europene. A se vedea *capitolul 2.1 Conținutul Ofertei* al prezentei oferte.
23	- actualizeze sistemul actualei autorități de certificare "ANTA", care să implementeze noile	**DA**	În cazul în care în perioada de derulare a Contractului va fi luată decizia introducerii la

	mecanisme criptografice stabilite pentru sistemul tahograf digital, și să asigure compatibilitatea cu actualele tahografe digitale și carduri tahograf pe perioada de tranziție în care ambele mecanisme criptografice vor fi folosite;		nivelul statelor AETR a noii generații de tahografe digitale și a noii generații de carduri pentru tahograful digital, care vor include noi mecanisme criptografice și o structură modificată a sistemului de fișiere, CERTSIGN va upgrada sistemul pentru emiterea de carduri tahograf pentru republica Moldova și va realiza tranziția la noua generație de carduri tahografice, fără a depăși termenele impuse de Acordul AETR și Reglementările Europene în acest sens. Pentru a realiza tranziția la noua generație de carduri tahografice, CERTSIGN va: ▪ actualiza sistemul actualei autorități de certificare pusă la dispoziția ANTA, MD-CA, pentru a implementa noile mecanisme criptografice stabilite pentru sistemul tahograf digital de generația a doua, și a asigura compatibilitatea cu actualele tahografe digitale și carduri tahograf pe perioada de tranziție în care ambele mecanisme criptografice vor fi folosite. A se vedea *capitolul 2.1 Conținutul Ofertei* al prezentei oferte.
24	- actualizeze sistemul centrului de personalizare pentru personalizarea noilor carduri tahografice	**DA**	În cazul în care în perioada de derulare a Contractului va fi luată decizia introducerii la nivelul statelor AETR a noii generații de tahografe digitale și a noii generații de carduri pentru tahograful digital, care vor include noi mecanisme criptografice și o structură modificată a sistemului de fișiere, CERTSIGN va upgrada sistemul pentru emiterea de carduri tahograf pentru republica Moldova și

			va realiza tranziţia la noua generaţie de carduri tahografice, fără a depăşi termenele impuse de Acordul AETR şi Reglementările Europene în acest sens. Pentru a realiza tranziţia la noua generaţie de carduri tahografice, CERTSIGN va: ▪ actualiza sistemul centrului de personalizare, MD-CP, pentru personalizarea cardurilor tahografice de generatia a doua. A se vedea *capitolul 2.1 Conţinutul Ofertei* al prezentei oferte.
25	Ofertantul trebule să dovedească capabilitatea de a asigura actualizarea aplicaţiilor software ale autorităţii de certificare "ANTA", conform noilor cerinţe elaborate la nivel European şi AETR în acest domeniu. Implementarea noilor cerinţe în sistemul ANTA se va realiza cu respectarea strictă a termenelor impuse de AETR şi reglementările Europene în acest sens, fără întreruperea activităţii de furnizare a cardurilor tahografice şi fără costuri suplimentare pentru Autoritatea Contractantă.	**DA**	CERTSIGN S.A., in calitate de producatoare a actualului sistem *tachoSAFE CA* utilizat pentru implementarea autoritatii de certificare MD-CA este în masură să asigure şi va asigura actualizarea, pe durata contractului, a aplicatiilor software ale autoritatii de certificare MD-CA conform noilor cerinte care vor fi elaborate la nivel European şi AETR în această perioadă. Implementarea noilor cerinţe în sistemul ANTA se va realiza cu respectarea strictă a termenelor impuse de AETR şi reglementările Europene în acest sens, fără întreruperea activităţii de furnizare a cardurilor tahografice şi fără costuri suplimentare pentru Autoritatea Contractantă. Pentru a demonstra calitatea de producător al sistemului tachoSAFE CA pus la dispoziţia ANTA şi capabilitatea de a asigura actualizarea aplicaţiilor software ale autorităţii de certificare ANTA, ataşăm prezentei oferte *Certificatul de înregistrare în Registrul National*

			al Programelor pentru Calculator emis de către Oficiul Român pentru Drepturile de Autor, ORDA, corespunzător aplicaţiilor *tachoSAFE CA*. A se vedea *capitolul 2.1 Conţinutul Ofertei* al prezentei oferte şi *Certificatul ORDA* ataşat ofertei.
26	Ofertantul va trebui sa actualizeze politica de securitate *National Authority Policy of Republic of Moldova for the Digital Tachograph System* conform noilor cerinţe impuse de tranziţia la generaţia a doua a tahografului digital şi conform noii Politici de Securitate a ERCA care va fi emisă pentru generaţia a doua a sistemului tahograf digital.	**DA**	CERTSIGN va actualiza politica de securitate *National Authority Policy of Republic of Moldova for the Digital Tachograph System* conform noilor cerinţe impuse de tranziţia la generaţia a doua a tahografului digital şi conform noii Politici de Securitate a ERCA care va fi emisă pentru generaţia a doua a sistemului tahograf digital. A se vedea *capitolul 2.1 Conţinutul Oferte* al prezentei oferte.
27	Infrastructura de securitate a ofertantului, care va proteja componentele sistemului ANTA trebuie să asigure respectarea tuturor cerinţelor stipulate în politica de securitate *„ National Authority Policy of Republic of Moldova for the Digital Tachograph System"*, aprobată de ERCA, în politica de securitate a ERCA şi în Acordul AETR, appendix IB.	**DA**	Toate sistemele puse la dispoziţia ANTA de către CERTSIGN pe durata contractului vor fi protejate de o infrastructură completă de securitate care asigură respectarea tuturor cerinţelor stipulate în: ▪ politica de securitate *„National Authority Policy of Republic of Moldova for the Digital Tachograph"*, aprobata de ERCA ▪ politica de securitate a ERCA, *Digital Tachograph System European Root Policy Version 2.1* ▪ *Acordul AETR, appendix IB.* A se vedea *capitolul 2.1 Conţinutul Ofertei* al

			prezentei oferte.
28	Această infrastructură de securitate trebuie să includă o incintă securizată ce va fi utilizată pentru emiterea certificatelor digitale, semnare, criptare și manipulare chei criptografice, pentru protecția acestora. Această incintă trebuie să îndeplinească următoarele cerințe minimale: - Să fie incinta ecranata cu atenuare de minim 55dB in gama 1MHz-1GHz și să prezinte un document cu măsurători conform standardului IEEE STD 299	**DA**	Infrastructura de securitate a CERTSIGN care protejează componentele sistemului autorității de certificare ANTA, MD-CA, include o incintă securizată în interiorul căreia sunt instalate toate serverele și componentele hardware ale sistemului și care este utilizată pentru emiterea certificatelor digitale, semnare, criptare și manipulare chei criptografice, în vederea protecției acestora. Această incintă securizată îndeplinește următoarele cerințe: ▪ este incinta ecranata, cu o atenuare de minim 55dB in gama 1MHz-1GHz. Atașat prezentei oferte este prezentat raportul de încercări emis de către Laboratorul de Încercări de Joasă și Inaltă Tensiune, conform standardului IEEE STD 299: 2007; A se vedea capitolul *2.1 Conținutul Ofertei* al prezentei oferte și documentul *Raport de Încercări Nr. 46715/28.02.2019* emis de către *Laboratorul de Încercări de Joasă și Înaltă Tensiune*, conform standardului IEEE STD 299: 2006 atașat ofertei.
29	- Să dispună de supraveghere video;	**DA**	Incinta securizată care protejează componentele sistemului autorității de certificare ANTA, MD-CA,: ▪ dispune de sistem de supraveghere video CCTV; A se vedea capitolul *2.1 Conținutul Ofertei* al prezentei oferte.
30	- Să dispună de sistem de detecție și avertizare în caz	**DA**	Incinta securizată care protejează

	de incendiu;		componentele sistemului autorității de certificare ANTA, MD-CA: ▪ dispune de sistem de detecție și avertizare în caz de incendiu; A se vedea capitolul *2.1 Conținutul Ofertei* al prezentei oferte.
31	- Să dispună de sistem de climatizare;	**DA**	Incinta securizată care protejează componentele sistemului autorității de certificare ANTA, MD-CA,: ▪ dispune de sistem de climatizare, în vederea asigurării condițiilor optime de funcționare a echipamentelor; A se vedea capitolul *2.1 Conținutul Ofertei* al prezentei oferte.
32	- Să dispună de sistem de control acces.	**DA**	Incinta securizată care protejează componentele sistemului autorității de certificare ANTA, MD-CA,: ▪ dispune de sistem de control acces. A se vedea capitolul *2.1 Conținutul Ofertei* al prezentei oferte.

4 Anexe

1. Anexa 1: Descrierea Tehnică a Cartelelor Tahografice oferite pentru Sistemul Tahograf Digital al Republicii Moldova
2. Anexa 2: Codul de practici și proceduri pentru MD-CP
3. Anexa 3: Codul de practici și proceduri pentru MD-CA
4. Anexa 4: Certificate și atestari
5. Anexa 5: Mostre carduri

Data completării: 30.12.2020

Operator economic,

CERTSIGN S.A.

Semnat:_____ L.Ș.

Nume: Armand-Dragos ROPOT

În calitate de: Reprezentant imputernicit

ANEXA 1

Descrierea Tehnică a Cartelelor Tahografice oferite pentru Sistemul Tahograf Digital al Republicii Moldova

Table of Content

S.C. CERTSIGN S.A. BUCUREȘTI - ROMÂNIA

1 Cardurile Tahografului Digital pentru Republica Moldova

1.1 Prezentare Generală

Scopul acestui document este de a prezenta cardurile tahografului digital pe care CERTSIGN propune să le furnizeze în cardul proiectului tahografului digital al Republicii Moldova, în conformitate cu prevederile acordului AETR.

1.2 Descrierea Tehnică a Cardurilor Blank

Formatul	8.55 x 5.4 cm (Conform standardului ISO 7810)
Tipuri	4 tipuri: Carduri de șofer, companie, control și atelier
Layout	Layout-ul cardurilor agreat împreună cu ANTA
Offset Printing	Front: max. 9 Fcolors (max. 40% acoperirea de culoare și max. 2 runde de tipărire)
Screen Printing	1 OVI® pe spatele cardului
Laminarea	Glossy laminated, fără caracteristici tactile și MLI
Cip	Implantarea cipului SLE66CX322P TCOS v1.0 R2 (TCOS)
Materialul	Policarbonat, alb și transparent, fără umpluturi optice, tehnologie multistrat, grosime 0.83 mm (conform standardului ISO 7810/7816)
Nivelul de calitate	Swiss Prime

1.3 Descrierea materialului Cardurilor

100% Policarbonat, alb şi transparent, fară umpluturi optice

Policarbonatul este superior multor altor material sintetice şi oferă cea mai mare rezistenţă la stresul mecanic, chimic şi termic. Policarbonatul este inert la influenţele mediului înconjurător. Atît datele ştiinţifice cît şi cele experimentale indică o durată de viaţă între 7 şi 10 ani. Durata de viaţă reală poate varia de la card la card în funcţi de factorii de mediu în care este folosit, cum ar fi temperatura, transpiraţia, umiditatea, stresul mechanic şi expunerea la radiaţiile luminoase, în special la radiaţiile ultra violet.

Cardurile furnizate de CERTSIGN sunt fabricate prin laminarea mai multor folii din material policarbonat identice în condiţii special de temperatură şi presiune fără ajutorul nici unui adeziv sau material termoplastice. Această technică asigură imposibilitatea dezasamblării cardurilor şi astfel previne accesul şi contrafacerea vreunui element constitutiv al cardurilor.

CERTSIGN S.A 2/8

1.4 Descrierea Elementelor de Securitate

Element	Descriere
Micro-printing	**Obligatoriu:** O linie continua de text (microprint line) sub titlul cardului scrisă cu albastru si pe marginea de jos în culori speciale (culori IRIS). **Element suplimentar de securitate:** Micro tiparirea este integrată în primului guilloche, iar linia continuă este separator fata de al doilea guilloche. Înaltimea micro tiparului este mai mica de 0,3 mm în toate cazurile Conține textul "Republica Moldova"
Text print  	**Obligatoriu:** Textul este tipărit pe fața și spatele cartelei cu albastru și steagul Republicii Moldova conform secțiunii 2.1 și a modelelor din apendixul 1B, secțiunea IV.1 a acordului AETR **Element suplimentar de securitate:** Plasat pe fața și spatele cardului între nucleul cardului și stratul transparent al cardului. Aceasta înseamnă că, toate literele sunt pe un strat la 100ym deasupra stratului gravat laser cu informațiile de personalizare. ➔ Reprezintă o cerință specială pentru tahograful German, care protejează datele personale. Propunem utilizarea acestui element ca un foarte util element de securitate și pentru tahograful Republicii Moldova.
Rainbow/IRIS print 	Trecerea continuă de la o culoare la alta fără rasterizarea datelor de culoare. Recomandarea noastră pentru tranzițiile de culoare Rainbow/Iris sunt: I.) cardul de șofer: alb/gri – cu tranziția de culoare IRIS spre albastru spre marginile din stînga și dreapta ale cardului II.) cardul de control: albastru - cu tranziția de culoare IRIS spre verde spre marginile din stînga și dreapta III.) cardul de atelier: roșu – cu tranziția de culoare IRIS spre verde spre marginile din stînga și dreapta Iv.) cardul de companie: - cu tranziția de culoare IRIS în galben spre marginile din stînga și dreapta

Element	Descriere

Guilloches 	**Combinarea a 2 proceduri de tipărire:** 1.) Printing plate: negative guilloches with space for endless text, consisting of the card title in the other union languages (including the new EU-member states' languages), areas of negative guilloches brightened by dash screen, on the lower edge integration of a micro-writing line into the guilloche motif, IRIS dying with transition of colours from the left to the right card edge according to section 2.1 relation of IRIS zones 25/50/25 of card width. 2.) Printing plate: positive guilloches, adjusted to the motif of the first printing plate, with integrated outlining of the endless text spared in first printing plate, in the space micro-writing with endless text, uniformly dyed I.) Driver card: white/grey – with IRIS colour transitions in blue towards left & right edge II.) Control card: blue – with IRIS colour transitions into second colour towards left & right edge III.) Workshop card: red - with IRIS colour transitions into second colour towards left & right edge Iv.) Company card: - with IRIS colour transitions into second colour towards left & right edge Placement on front and rear side between core of the card and the following transparent card layer overlapping in the scope of the photograph.
OVI print 	**Element suplimentar de securitate:** Cerneală variabilă optic (OVI) îşi schimbă culoarea cînd cardul este privit din unghiuri diferite. This OVI is only available for registered state printers such as banknote printers, and ID and/or Passport printers. Print of an OVI (optical variable ink) e.g. an arrow on the reverse side of the card in a way that its colour changes from gold to red, dependent on the incidental light. Copy-proof printing element as an optically variable characteristic, among others, in form of light-diffracting structures (on account of the required qualification for use underneath the uppermost, i.e. surface layer of the card).

Element	Description
Tiparire cu cerneală vizibilă	**Obligatoriu:**

S.C. CERTSIGN S.A. certSIGN ŞTI - ROMÂNIA

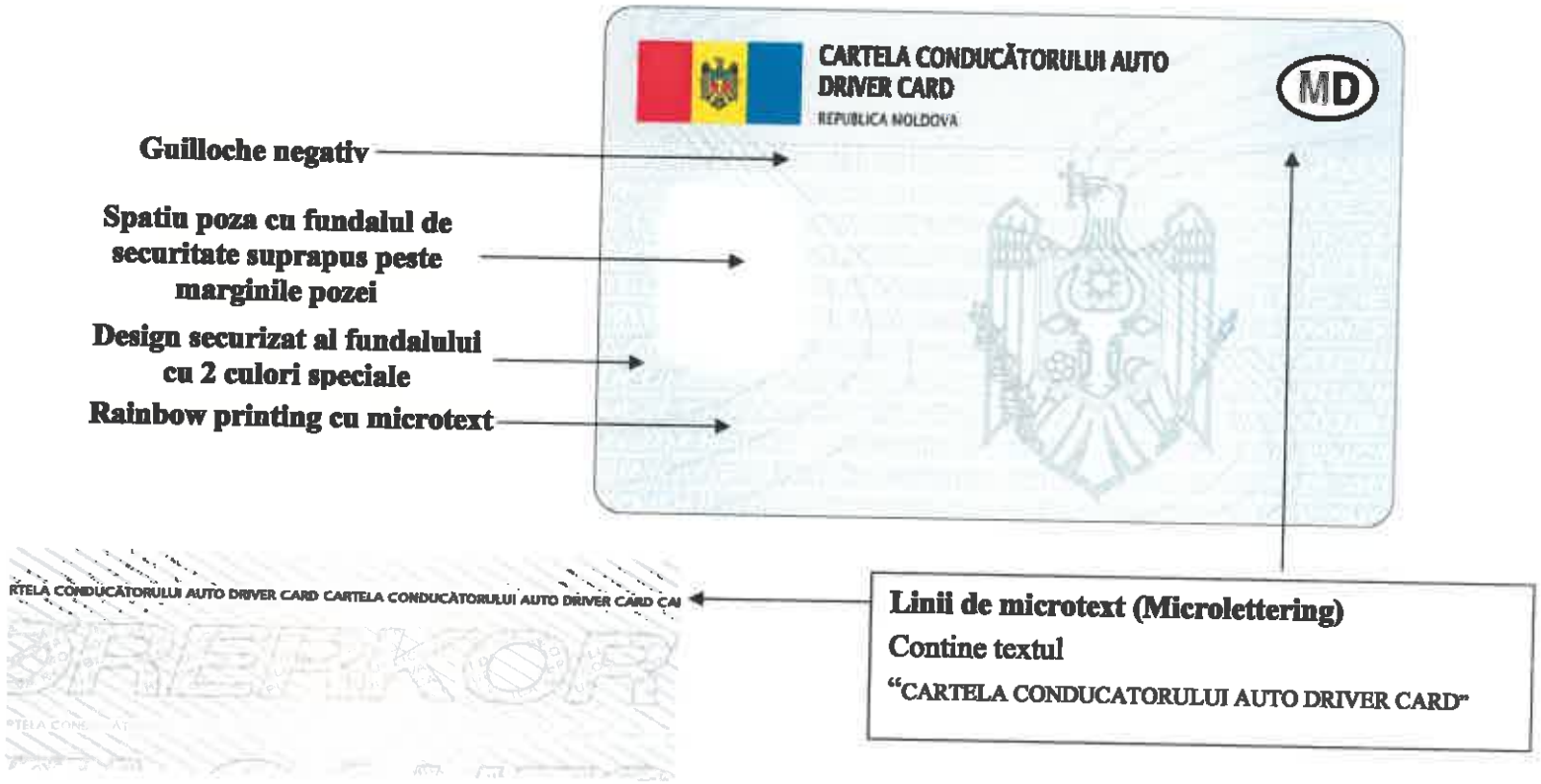
În lumină UV 	Pe fața cardului: brightly colored printed features that are invisible in normal light become visible when illuminated by ultraviolet light. The invisible fluorescent printing comprises a multi-colored feature with to the security industry reserved UV-colors Authenticity test only possible with UV lamp. ➔ *În designul Republicii Moldova va fi schimbat simbolul.* **Additional UV-security features** (proposition): Printing on the front side, three fluorescence colours: a.) EU-stars will change from yellow to UV-red; b.) EU-blue will change to yellow (inverse-effect)
Contact-responsive chip 	Un microcip va fi integrat pe spatele cardului.

1.5 Designul cartelelor tahografice

În continuare sunt prezentate designul graphic și de securitate al cartelelor tahografice propuse a fi furnizate de către CERTSIGN.

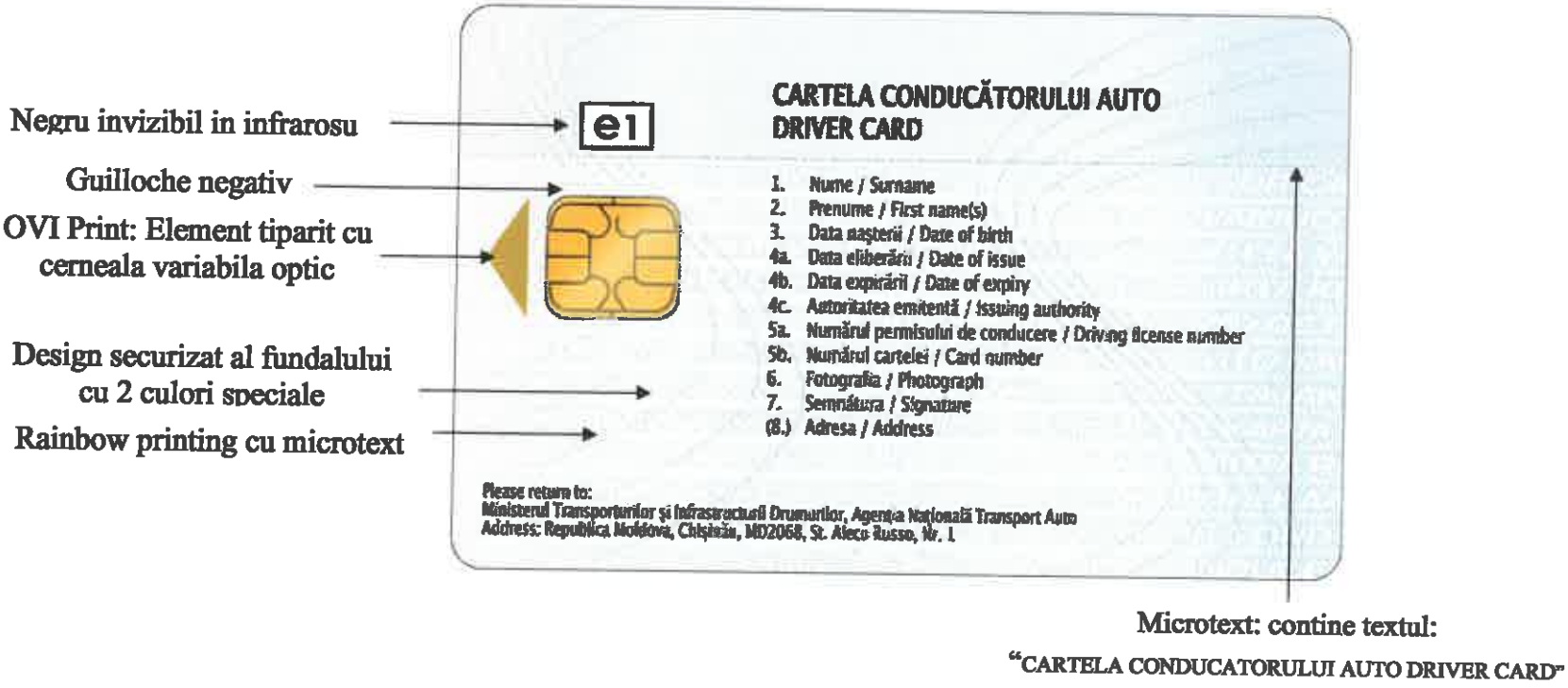
1.5.1 Designul cartelei conducătorului auto

FAȚA CARDULUI – Elemente vizibile în lumină normală



FATA CARDULUI – Elemente vizibile în lumină ultravioletă

VERSO – Elemente vizibile în lumină normală



Microtext: contine textul:

"CARTELA CONDUCATORULUI AUTO DRIVER CARD"

1.5.2 Designul cartelei operatorului de transport

FATA CARDULUI – Elemente vizibile în lumină normală

FATA CARDULUI – Elemente vizibile în lumină ultravioletă

VERSO – Elemente vizibile în lumină normală

Negru invizibil in infrarosu

Guilloche negativ

OVI Print: Element tiparit cu cerneala variabila optic

Design securizat al fundalului cu 2 culori speciale

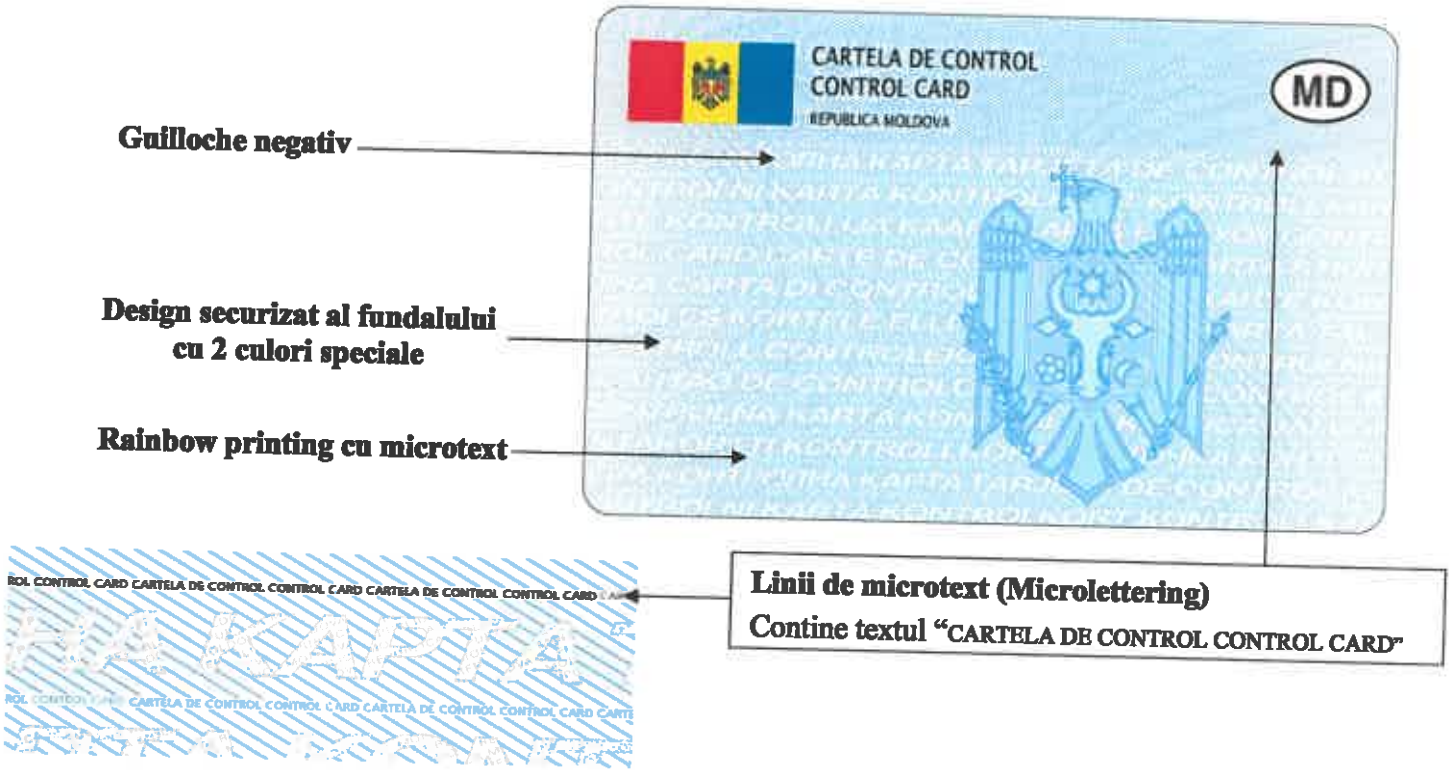
Rainbow printing cu microtext

Microtext: contine textul:

"CARTELA OPERATORULUI DE TRANSPORT COMPANY CARD"

1.5.3 Designul cartelei de control

FATA CARDULUI – Elemente vizibile în lumină normală



FATA CARDULUI – Elemente vizibile în lumină ultravioletă

VERSO – Elemente vizibile în lumină normală

Negru invizibil in infrarosu

Guilloche negativ

OVI Print: Element tiparit cu cerneala variabila optic

Design securizat al fundalului cu 2 culori speciale

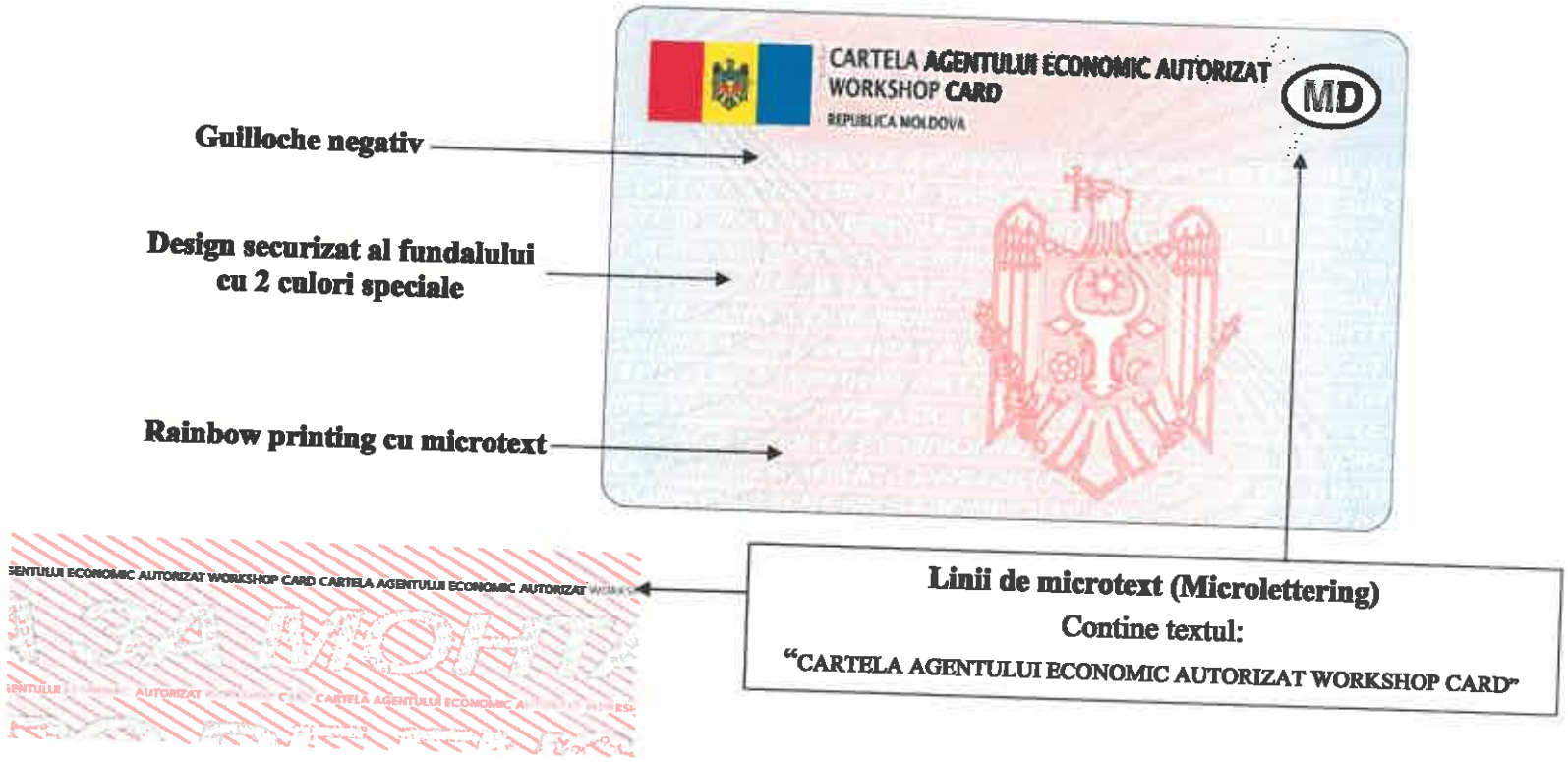
Rainbow printing cu microtext

Microtext: contine textul:

"CARTELA DE CONTROL CONTROL CARD"

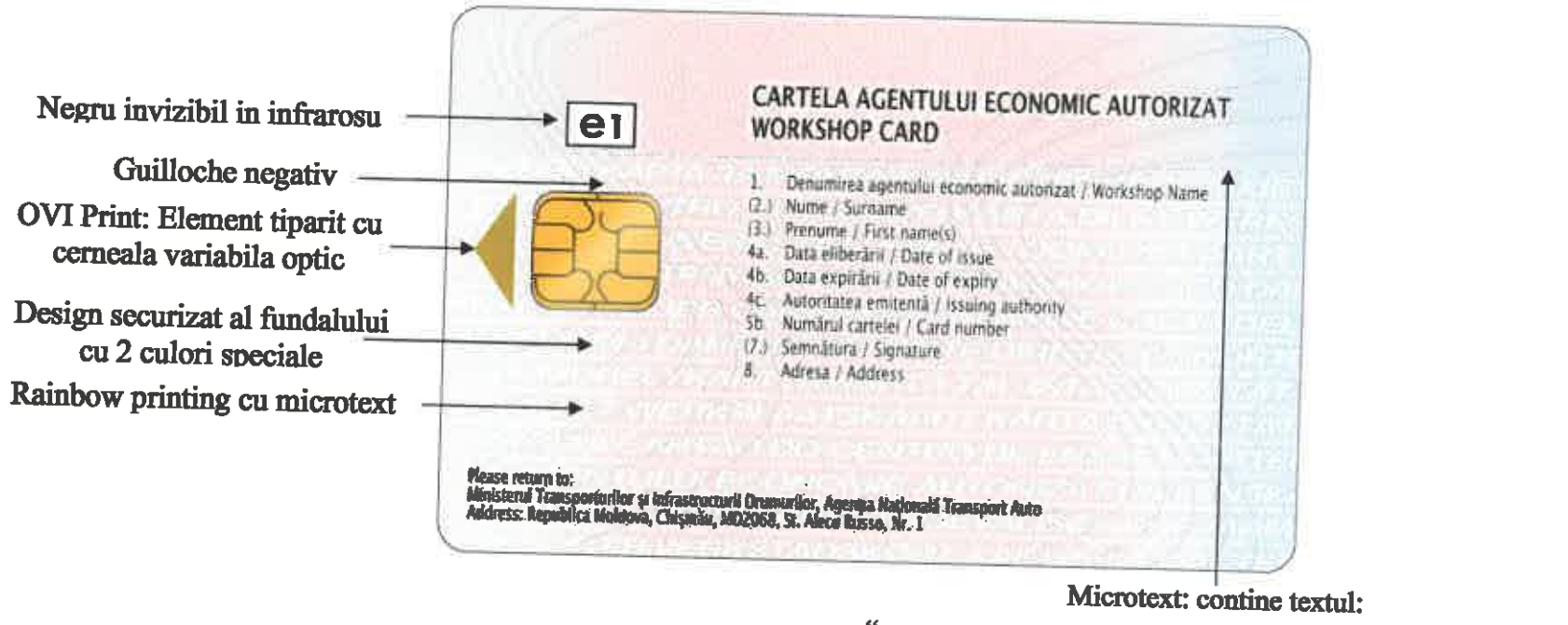
1.5.4 Designul cartelei agentului economic autorizat

FATA CARDULUI – Elemente vizibile în lumină normală



FATA CARDULUI – Elemente vizibile în lumină ultravioletă

VERSO – Elemente vizibile în lumină normală



Microtext: contine textul:

"CARTELA AGENTULUI ECONOMIC AUTORIZAT WORKSHOP CARD"

1.6 Layout-ul de personalizare al cartelelor tahografice

Pentru a asigura un nivel de securitate corespunzator, poza, semnatura si celelalte date variabile corespunzatoare fiecarui posesor de cartela de conducator auto vor fi personalizate prin gravare laser.

Cimpurile ingrosate (bold) de mai jos vor fi personalizate folosind caractere tactile.

1.6.1 Layout personalizare cartelă conducător auto

1.6.2 Layout personalizare cartelă operator de transport

1.6.3 Layout personalizare cartelă control

1.6.4 Layout personalizare cartelă agent economic autorizat

1.7 Standarde şi Reglementări

La baza proiectării cardurilor tahografice pentru Republica Moldova stau următoarele standard şi regulementări:

- ISO 7810, ISO/IEC 7501-1, ISO/IEC 7501-3; ISO-IEC 10373, ISO 7816; ISO-1831
- Specificaţiile din Appendix 1B al acordului AETR pentru cardurile de tahograf digital
- Specificaţiile din Annexx 1B al Commision Regulation No. 1360/2002 pentru cardurile de tahograf digital

Certificarile cartelelor tahografice oferite cat si type approval-ul sunt anexate prezentei oferte.

S.C. CERTSIGN S.A

1.8 Conformitatea cu Standardele

Cardurile Tahografice propuse îndeplinesc următoarele standarde[1], cît și standardele suplimentare ale poliției Federale din Germania pentru Cardurile de Tahograf:

Standarde de calitate		
Descriere	Standard	Test-Standard
ID Card technology	ISO/IEC 7810	ISO/IEC 10373
ID Card dimensions	ISO/IEC 7810	ISO/IEC 10373
Delamination	ISO/IEC 7810	ISO/IEC 10373
Resistance to plasticiser	Internal test method	Internal test method
Blank Card dimensional stability and warpage with temperature	ISO/IEC 7810	ISO/IEC 10373
Light fastness	ISO/IEC 7810; DIN 54004	DIN 54004
Static force warping	DIN 32753/1	DIN 32753/1
Unilateral dynamic bending stress	ISO/IEC 7810 & DIN 32753/1	ISO/IEC 10373 & DIN 32753/1
Torsion strength	ISO/IEC 7810	ISO/IEC 10373
Resistance to scratches	Internal test method	Internal test method
Resistance to chemicals (incl. saltdust)	ISO/IEC 7810	ISO/IEC 10373
Resistance to perspiration and saliva	Internal test method	Internal test method
Cantilever method	DIN 32753/1	DIN 32753/1
Resistance to oils and fats	Internal test method	Internal test method
The Card is not detrimental to health in any way in normal use.	ISO/IEC 7810	ISO/IEC 10373
Supported chip Card standards	ISO 7816 parts 3,4,8,9	Certified

[1] Aceasta este testat și certificat de către Independent Forschungsanstalt der Graphischen Industrie – FOGRA - in Munich, și Kraftfahrt Bundesamt in Flensburg/Germania.

Sistemul de Tahograf Digital pentru Republica Moldova

Codul de Practici si Proceduri pentru operarea MD-CP

certSIGN

CUPRINS

1 INTRODUCERE

Agentia Nationala Transport Auto este responsabila pentru funcţia de Autoritate Naţionala de Certificare a infrastructurii de management a cheilor criptografice din cadrul sistemului de tahografe digitale introdus prin Reglementarea Consiliului UE nr. 3821/85, revizuita prin Reglementarea Comisiei CE nr. 1360/2002 si Reglementarea Comisiei CE nr. 432/2004.

Aceasta infrastructura de chei publice consta din sisteme, produse si servicii care asigura:

- Certificate pentru chei publice pentru componente de tahograf (carduri, unitati de vehicul si senzor de mişcare);
- Chei de criptare pentru datele senzorilor de mişcare.

Scopul acestui document este acela de a descrie practicile implementate de MD-CP in lucrul cu cardurile de tahograf si cheile de criptare.

Documentul a fost creat pentru a asigura conformitatea cu cerinţele enunţate in Politica de Certificare a MD-CA si se bazează pe cadrul creat prin IETF RFC 3647.

1.1 Descriere generala

Scopul principal al acestui document este acela de a fi folosit de către MD-MSA si de către cei care doresc sa evalueze gradul de încredere care poate fi acordat serviciilor oferite de MD-CP sau sa determine măsura in care acestea respecta cerinţele sistemului pentru tahografe digitale.

Sistemul de management al cheilor criptografice (vezi figura următoare) este necesar pentru a implementa mecanismele de securitate definite in:

- Reglementarea Comisiei CE nr. 1360/2002, Anexa I(B), Appendix 11 Common Security Mechanisms.
- ISO / IEC 16844-3 Road vehicles, Tachograph systems, Part 3: Motion sensor interface.

MD-CA si MD-CP sunt operate sub responsabilitatea si autoritatea autorităţilor naţionale sau a furnizorilor de servicii externi autorizaţi.

MD-CA are rolul de a certifica cheile RSA care sunt introduse in cardurile pentru tahografe de către MD-CP.

Mai multe tipuri de carduri sunt emise următoarelor entităţi: şoferilor, atelierelor, organelor de control si firmelor de transport.

MD-CP primeşte cererile de cartele tahografice de la MD-CIA in format electronic securizat, generează perechile de chei RSA pentru cartele, generează cererile de certificat corespunzătoare, le transmite MD-CA, primeşte certificatele de la MD-CA, personalizează cartelele, ambalează cartelele si PIN-ul (pentru cartelele de atelier) si le trimite la MD-CIA pentru distribuţie.

MD-CA îşi schimba cheile la intervale regulate.

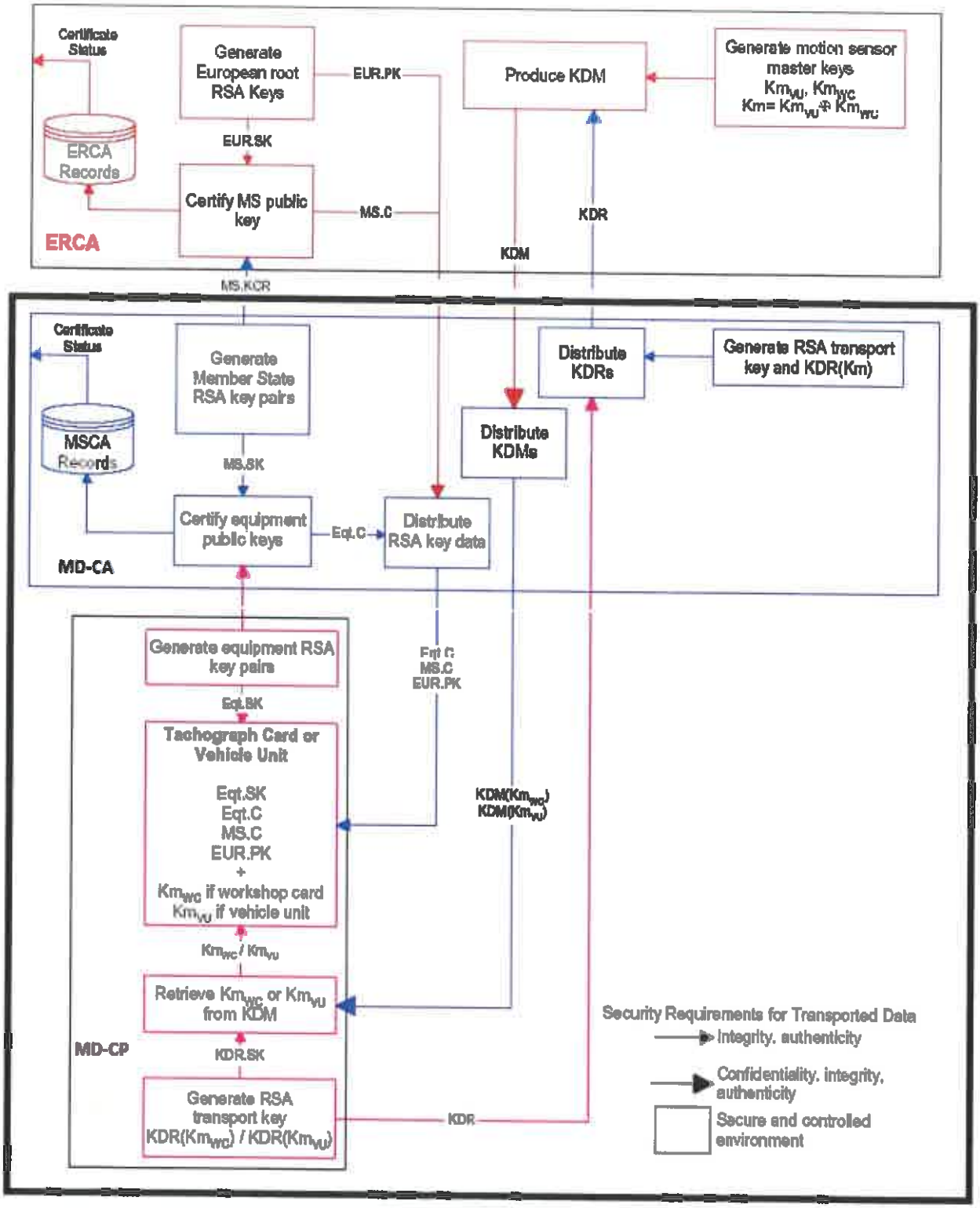
Formatul certificatelor digitale folosite este proprietar si incompatibil cu formatul X.509, al certificatelor digitale a căror utilizare este presupusa, dar nu ceruta obligatoriu de către IETF RFC 3647.

MD-CA generează, separa si distribuie o singura cheie criptografica simetrica, necesara pentru securizarea datelor de mişcare ale vehiculelor , in conformitate cu mecanismele definite de standardul ISO / IEC 16844-3.

Cheia master Km este separata in doua parţi , Km_{VU} si Km_{WC}. Km_{wc} sunt inserate in cardurile de atelier de către personalizatorii de carduri.

Pentru a asigura confidenţialitatea cheii Km_{wc} in timpul transportului de la ERCA la MD-CA, ERCA o criptează folosind o cheie publica de criptare RSA, pentru a produce un mesaj de distribuţie a cheii (KDM). Acelaşi lucru este valabil si pentru transportul aceleiaşi cheii Km_{wc} de la MD-CA la MD-CP. Cheile RSA folosite la crearea mesajelor KDM sunt create de MD-CA sau MD-CP si trimise către ERCA sau respectiv MD-CA printr-o cerere de distribuţie (KDR).

Necesitatea ca MD-CA sau MD-CP sa primească cheia Km_{wc} este definita intr-un acord semnat de ERCA si MD-MSA.


Certificate Status
Generate European root RSA Keys
EUR.PK
Produce KDM
Generate motion sensor master keys
Km_VU, Km_WC
Km= Km_VU ⊕ Km_WC
ERCA Records
EUR.SK
Certify MS public key
MS.C
KDR
ERCA
KDM
MS.KCR
Certificate Status
Generate Member State RSA key pairs
Distribute KDRs
Generate RSA transport key and KDR(Km)
MSCA Records
Distribute KDMs
MS.SK
Certify equipment public keys
Eqt.C
Distribute RSA key data
MD-CA
Generate equipment RSA key pairs
Eqt.C
MS.C
EUR.PK
Eqt.SK
Tachograph Card or Vehicle Unit
Eqt.SK
Eqt.C
MS.C
EUR.PK
+
Km_WC if workshop card
Km_VU if vehicle unit
KDM(Km_WC)
KDM(Km_VU)
Km_WC / Km_VU
Retrieve Km_WC or Km_VU from KDM
MD-CP
KDR.SK
Generate RSA transport key KDR(Km_WC) / KDR(Km_VU)
KDR
Security Requirements for Transported Data
Integrity, authenticity
Confidentiality, integrity, authenticity
Secure and controlled environment

1.2 Numele si Identificarea Documentului

Acest document poarta denumirea de "Codul de Practici si Proceduri pentru Operarea MD-CP pentru Sistemul Tahografelor Digitale" si va fi referit in continuare simplu ca MD-CP CPP.

1.3 Participanți

Acest CPP este creat doar pentru a îndeplini cerințele sistemului pentru tahografe digitale.

1.3.1 Autoritatea de Certificare

MD-CA si MD-CP sunt operate sub autoritatea si responsabilitatea autorităților moldovene responsabile, sau a furnizorilor de servicii autorizați. MD-CA este certificat de ERCA.

1.3.2 Autoritatea de Înregistrare

Autoritatea Națională de Înregistrare implementează sisteme, produse si servicii necesare pentru emiterea de carduri de tahograf. RA-ul național este responsabil pentru a menține legătura intre identificatorii subiecților certificatelor (cardurile) si persoanele fizice sau juridice care le folosesc. In Moldova, funcția RA pentru emiterea de certificate digitale pentru carduri de tahograf si cheii Km_{wc} este asigurata de MD-CIA.

1.3.3 Abonați

Abonații serviciilor de certificare oferite de MD-CA sunt cardurile de tahograf.

1.3.5 Destinatarii Cheilor pentru Senzorii de Mișcare

Destinatarii cheilor Km_{wc} sunt organizațiile care personalizează cardurile de atelier. Acestea sunt identificate in acordul semnat intre ERCA si MD-CA.

1.4 Utilizarea certificatului

Certificatele de cheie publica pentru tahografe trebuie inserate in componentele tahografelor digitale, așa cum se cere in procesul de autentificare mutuala descris in cerința CSM_020 Reglementarea 1360/2002, Annex I(B) Appendix 11 Common Security Mechanism.

Certificatele pentru tahografele digitale pot fi folosite in aplicații in legătura sistemul tahografelor digitale (de exemplu: Echipamente de calibrare utilizate in ateliere, echipamente pentru descărcarea de date folosite de organele de control, sisteme de management al flotelor auto si/sau mărfurilor folosite de firmele de transport etc.).

Certificatele pentru tahografe digitale nu pot fi folosite pentru nici un alt scop.

1.5 Utilizarea Mesajului pentru Distribuirea Cheii (KDM)

Mesajele KDM trebuie folosite doar in scopul transmiterii securizate a cheii Km_{wc} intre ERCA si MD-CA si intre MD-CA si MD-CP.

1.6 Administrarea CPP

1. Acest CPP este creat, menținut si revizuit de către S.C. CERTSIGN S.A., care îndeplinește funcția de furnizor de servicii de personalizare pentru MD-CP, având ManufacturerCode 21_{16} alocat de către "Digital Tachograph Laboratory" al Comisiei Europene, conform cerinței din Commission Regulation 1360/2002,

Annex I(B) Appendix 1, paragraph 2.67. De asemenea, S.C. CERTSIGN S.A. este declarat ca "service agency for MD-CA" conform politicii de securitate "Moldovian CA Policy", aprobata de către ERCA:

Organizaţia Moldoveana pentu Personalizarea Cardurilor de Tahograf

S.C. CERTSIGN S.A.

Sediu Social: Sos. Olteniţei nr. 107 A, clădirea C1, parter

Sector 4, CP 041303, Bucureşti, Romania

Sediu: Bulevardul Tudor Vladimirescu, nr. 29 A, AFI Tech Park 1,

Sector 5, Bucureşti, România, CP 050881

Tel. (+4031)1011870

Fax: (+4021)3119905

2. Orice întrebare referitoare la prezentul CPP trebuie trimise către: S.C. CERTSIGN S.A.
3. Orice întrebare referitoare la operarea MD-CP trebuie trimise către S.C. CERTSIGN S.A.
4. Autoritatea Naţionala, MD-MSA, trebuie sa stabilească daca acest CPP este conform cu Politica de Certificare a MSA.
5. Stabilirea conformităţii se bazează pe o evaluare de securitate realizata fie chiar de către MD-MSA, fie de un terţ autorizat.

1.7 Definiţii si Acronime

Criptare Asimetrica: procesul de criptare in care o cheie este folosita pentru a cripta mesajul si o cheie diferita este utilizata pentru decriptarea mesajului.

Detectarea Intruziunii: detectarea unei intruziuni fizice de către un agent de paza, sau a uneia informatice de către un sistem care cuprinde un senzor, un mediu de transmisie si un panou de alarma unde se trimite alarma.

Escrow-ul cheii: trimiterea unei copii a cheii către o entitate autorizata sa folosească aceasta copie pentru alt scop decât acela de a-l returna entităţii care a generat cheia.

Criptare simetrica: procesul de criptare in care aceeaşi chei este folosita si la criptarea mesajului si la decriptarea lui.

CAR	Certification Authority Reference
CHA	Certificate Holder Authorisation
CHR	Certificate Holder Reference
CP	Component Personaliser
CPI	Certificate Profile Identifier
CPS	Certification Practices Statement
CRL	Certificate Revocation List
CSP	Certification Service Provider
DES	Data Encryption Standard (symmetric encryption scheme)
EA	European Authority
ENI	ESSOR Nuclear Island
EOV	End Of Validity
ERCA	European Root Certification Authority
ETSI	European Telecommunications Standards Institute
KCR	Key Certification Request
KDR	Key Distribution Request
KDM	Key Distribution Message
Km	Motion sensor master key
Km_{wc}	Motion sensor master key inserted in workshop card
NCA	National Certification Authority
MD-MSA	Moldavia Authority
MD-CA	Moldavia Certification Authority
MD-CIA	Moldavia Card Issuance Authority
OA	Operating Agent

OE	Operational Entity (used to refer to both a NCA and a CP)
OM	Operations Manager
PK	RSA public key
PKI	Public Key Infrastructure
PR	Permanent Representation of Member State
RSA	Rivest, Shamir, Adleman (asymmetric encryption scheme)
SAS	Single access system
SK	RSA secret key
TDES	Triple DES

2 CONTROALE TEHNICE DE SECURITATE

Acest capitol descrie procedurile de generare şi management a perechii de chei criptografice a Autorităţii de Certificare şi Abonatului, inclusiv cerinţele tehnice asociate.

2.1 Generarea si Instalarea Perechii de Chei pentu Carduri

2.1.1 Generarea perechii de chei

Procedurile de management a cheii se referă la păstrarea şi folosirea în siguranţă de către proprietar a cheilor sale.

Semnătura electronică este creată prin folosirea algoritmului RSA în combinaţie cu rezumatul criptografic SHA-1.

Generarea perechii de chei pentru carduri este realizata in serverul criptografic utilzând un HSM Cryptographic P3 data preparation module. Modulul HSM al serverului criptografic este conform cu cerinţele FIPS 140-2 Nivel 3. Cheia privata este menţinuta în permanenţă criptata atât pe dispozitivul HSM, in baza de date CP si in tranzit către maşina de personalizat carduri.

Acţiunile întreprinse în momentul generării perechii de chei sunt înregistrate si datate. Înregistrările sunt păstrate din motive de audit sau pentru verificările obişnuite ale sistemului.

2.1.2 Distribuirea cheii private către entităţi

Transferul cheii private din modulul HSM in card se face in mod securizat cu ajutorul aplicaţiei de personalizare. Nici o entitate nu poate interveni pentru a compromite cheia sau pentru a o copia.

2.1.3 Trimiterea cheii publice către emiţătorul certificatului (MD-CA)

Conform politicii MD-CA.

2.1.4 Distribuirea cheilor publice ale cardurilor către entităţile partenere

Cheia publica a cardului este distribuita de MD-CP pe card sub forma de certificat emis de MD-CA, semnat cu cheia privata a MD-CA. Cheia publica a MD-CA este distribuita către MD-CP sub forma de certificat emis de ERCA. Cheia publica ERCA este distribuita către MD-CP ca atare. Distribuirea certificatului MD-CA si a cheii publice a ERCA către MD-CP se face împreuna cu certificatul cardului ca urmare a unei cererii KCR primite de MD-CA de la MD-CP.

2.1.5 Mărimile cheilor

Cheile RSA trebuie sa aibă un modul de 1024 biţi si un exponent public de 64 biţi.

2.1.6 Parametrii de generare ai cheilor publice

Entitatea ca generează o cheie este responsabila de verificarea calităţii parametrilor cheii generate. Aceasta trebuie să verifice:

- posibilitatea de a efectua operaţii de criptare şi decriptare, inclusiv creare de semnături electronice şi verificare a acestora,
- procesul de generare a cheii trebuie să se bazeze pe generatoare puternice de numere aleatoare – surse fizice de zgomot alb, dacă este posibil,
- imunitatea la atacuri cunoscute (în cazul algoritmilor RSA şi DSA).

2.1.7 Verificarea calităţii parametrilor

Se folosesc module HSM certificate, configurate pentru a genera chei RSA cu modulul de 1024-biti.

2.1.8 Generarea Hardware/software a cheii

Cheile pentru carduri sunt generate in module HSM certificate.

2.1.9 Utilizarea perechii de chei

Cheia privata RSA a cardului este utilizata doar pentru semnarea certificatelor cheilor cererii de certificat către MD-CA.

2.2 Protecţia Cheii Private

2.2.1 Standarde si controale pentru modulele criptografice

MD-CP utilizează pentru generarea si stocarea cheilor private RSA ale cardurilor doar module HSM certificate. Operaţia modulului HSM este verificata periodic prin teste interne, iar upgrade-ul de firmware pentru HSM este realizat anual de administratorul HSM, daca este cazul.

2.2.2 Controlul k din n al cheii private

Generarea cheii private este realizata de un HSM P3 data preparation pentru autorizarea căruia este necesara prezenta a trei persoane autorizate.

2.2.3 Backup-ul cheii private

Nu se aplica.

2.2.4 Arhivarea cheii private

Nu se aplica.

2.2.5 Transferul cheii private din sau intr-un modul HSM

Cheia privata RSA pentru carduri este generata in HSM si apoi transferata pe card in mod securizat.

2.2.6 Păstrarea cheii private intr-un modul HSM

Cheile private ale cardurilor nu sunt păstrate in modulul HSM unde au fost generate.

2.2.7 Metoda de activare a cheii private

Activarea modului HSM pentru generarea cheilor private pentru cardurile tahograf se face folosind o schema 3/3.

2.2.10 Certificarea modulului HSM

MD-CP foloseşte module criptografice certificate cel puţin FIPS 140-2 Level 3.

2.3 Alte Aspecte ale Managementului Perechii de Chei

2.3.1 Arhivarea Cheii Publice

Perechile de chei a cardurilor tahograf sunt păstrate criptat in baza de date CP pentru o perioada de 30 de zile.

2.3.2 Perioadele de validitate pentru cheile publice si private emise de MD-CP

Perioada de validitate a cheii private a cardului este de maximum: 5 ani (şoferi si companie), 2 controlor si 1 an (atelier).

Perioada de validitate a cheii publice a cardului este de maximum: 5 ani (şoferi si companie), 2 controlor si 1 an (atelier).

2.4 Datele de Activare

Singurul tip de card care foloseşte date de activare (PIN) este cardul de atelier.

2.5 Controale de Securitate a Calculatoarelor

Sarcinile operatorilor si administratorilor care lucrează în cadrul MD-CP sunt realizate prin intermediul unor dispozitive hardware şi aplicaţii software de încredere.

2.5.1 Cerinţele tehnice specifice securităţii calculatoarelor

Cerinţele tehnice prezentate în acest capitol se referă la controalele de securitate specifice calculatoarelor şi aplicaţiilor, folosite în cadrul MD-CP. Măsurile de securitate care protejează sistemele de calcul sunt aplicate la nivelul sistemului de operare, al aplicaţiilor precum şi din punct de vedere fizic.

Calculatoarele aparţinând MD-CP dispun de următoarele mijloace de securitate:

- autentificarea obligatorie la nivelul sistemului de operare şi al aplicaţiilor,
- control discreţionar al accesului,
- posibilitatea de a fi auditate din punct de vedere al securităţii,
- calculatorul este accesibil doar personalului autorizat, cu roluri de încredere în MD-CP,
- separarea sarcinilor, conform rolului în cadrul sistemului,

- identificarea şi autentificarea rolurilor şi a personalului care îndeplineşte aceste roluri,
- prevenirea refolosirii unui obiect de către un alt proces după eliberarea acestuia de către procesul autorizat,
- protecţia criptografică a schimburilor de informaţii şi protecţia bazelor de date,
- arhivarea istoricului operaţiunilor executate pe un calculator şi a datelor necesare auditării,
- o cale sigură ce permite identificarea şi autentificarea rolurilor şi a personalului care îndeplineşte aceste roluri,
- metode de restaurare a cheilor (numai în cazul modulelor hardware de securitate), a aplicaţiilor şi a sistemului de operare,
- mijloace de monitorizare şi alertare în cazul accesului neautorizat la resursele de calcul.

2.5.2 Evaluarea securităţii calculatoarelor

Sistemele de calcul ale MD-CP respectă cerinţele descrise în standardul CEN CWA 14167 (Cerinţele de Securitate pentru Sistemele de Încredere care asigură Managementul certificatelor).

2.5.3 Controale tehnice specifice ciclului de viaţa

Controale specifice dezvoltării sistemului

Fiecare aplicaţie, înainte de a fi folosita în producţie de către MD-CP, este instalata astfel încât să se permită controlul versiunii curente şi să se prevină instalarea neautorizată de programe sau falsificarea celor existente.

Reguli similare se aplică în cazul înlocuirii componentelor hardware, cum ar fi:

- dispozitivele fizice sunt furnizate în aşa fel încât să poată fi urmărita şi evaluată ruta fiecăruia, până la locul său de instalare,
- livrarea unui dispozitiv fizic pentru înlocuire se realizează într-un mod similar celui de livrare al dispozitivului original; înlocuirea se realizează de către personal calificat şi de încredere.

Controale pentru managementul securităţii

Scopul controalelor pentru managementului securităţii este acela de a superviza funcţionalitatea sistemelor MD-CP, garantând astfel că acestea operează corect şi în concordanţă cu configurarea acceptată şi implementată.

Configuraţia curentă a sistemelor MD-CP, precum şi orice modificare şi actualizare a acestora, este înregistrată şi controlată.

Controalele aplicate sistemelor MD-CP permit verificarea continuă a integrităţii aplicaţiilor, versiunii şi autentificarea şi verificarea originii dispozitivelor hardware.

2.5.4 Controale de securitatea a rețelei

Serverele și stațiile de lucru de încredere aparținând MD-CP sunt conectate prin intermediul unei rețele locale (LAN), divizate în mai multe subretele, cu acces controlat. Accesul dinspre alte rețele către orice segment, este protejat prin intermediul unui firewall inteligent.

Controalele de securitate sunt dezvoltate pe baza firewall-ului și a filtrelor de trafic aplicate la nivelul ruterelor.

Mijloacele de asigurare a securității rețelei acceptă doar mesajele transmise prin protocoale securizate. Evenimentele (log-urile) sunt înregistrate în jurnalele de sistem și permit supravegherea folosirii corecte a serviciilor furnizate de MD-CP.

2.5.5 Controale specifice modulelor criptografice

Controalele modulelor criptografice includ cerințele impuse pentru dezvoltarea, producția și livrarea modulelor. MD-CP nu definește cerințe specifice în acest domeniu. Totuși, MD-CP acceptă și utilizează numai module criptografice care corespund cerințelor Politicii de Certificare a MSA.

2.5.6 Înregistrarea evenimentelor și procedurile de auditare

Pentru a gestiona eficient sistemele MD-CP și pentru a putea audita acțiunile utilizatorilor și personalului MD-CP, toate evenimentele care apar în sistem sunt înregistrate. Informațiile înregistrate alcătuiesc jurnalele (log-urile) de evenimente și trebuie păstrate în așa fel încât să permită, daca este cazul, să se acceseze informațiile corespunzătoare și necesare rezolvării disputelor, sau să detecteze tentativele de compromitere a securității MD-CP. Evenimentele înregistrate fac obiectul procedurilor de arhivare. Arhivele sunt păstrate în afara incintei MD-CP.

Când este posibil, log-urile sunt create automat. Dacă înregistrările nu pot fi create automat, se vor folosi jurnalele de evenimente pe hârtie. Fiecare înregistrarea în log, electronic sau de mână, este păstrata și dezvăluita atunci când se desfășoară un audit.

Tipuri de evenimente înregistrate

Fiecare activitate critică din punctul de vedere al securității MD-CP este înregistrată în log-urile de evenimente și arhivată. Arhivele sunt depozitate pe medii de stocare ce nu pot fi suprascrise pentru a preveni modificarea sau falsificarea lor.

Log-urile de evenimente MD-CP conțin înregistrări ale tuturor activităților generate de componentele software din cadrul sistemului. Aceste înregistrări sunt împărțite în trei categorii separate:

- **Înregistrări de sistem** – conțin informații despre cererile clienților software și răspunsurile server-ului (sau invers) la nivelul protocolului de rețea (de exemplu: https); datele concrete care se înregistrează sunt: adresa IP a stației sau a server-ului, operațiunile executate (de exemplu:

căutare, editare, scriere etc.) şi rezultatele lor (de exemplu introducerea cu succes a unei înregistrări în baza de date),

- **erori** – conţine informaţii despre erori la nivelul protocoalelor de reţea şi la nivelul modulelor aplicaţiilor;
- **audit** – conţin informaţii specifice serviciilor de certificare, de exemplu: cererea de înregistrarea şi de certificare, cererea de schimbare a cheii, acceptarea certificatului, emiterea de certificat etc.

Jurnalele de evenimente de mai sus sunt comune fiecărei componente instalate pe un server sau staţie de lucru şi au o capacitate prestabilită. Atunci când se depăşeşte această capacitate, este creată automat o nouă versiune de jurnal. Jurnalul anterior este arhivat şi şters de pe disc.

Fiecare înregistrare, automată sau manuală, conţine următoarele informaţii:

- tipul evenimentului,
- identificatorul evenimentului,
- data şi ora apariţiei evenimentului,
- identificatorul persoanei responsabile de eveniment.

Conţinutul înregistrărilor se refera la:

- alertele firewall-urilor şi IDS-urilor,
- operaţiile asociate înregistrării, certificării etc.,
- modificări ale structurii hard sau soft,
- modificări ale reţelei şi conexiunilor,
- înregistrările fizice în zonele securizate şi violările de securitate,
- schimbările de parole, drepturi asupra codurilor PIN, rolurile personalului,
- accesul reuşit şi nereuşit la baza de date MD-CP şi la aplicaţiile serverului,
- generarea de chei pentru carduri, etc.,
- fiecare cerere primită şi decizia emisă în format electronic,
- istoria creării copiilor de backup şi a arhivelor cu înregistrări.

Accesul al jurnalele de evenimente (log-uri) este permis în exclusivitate administratorului de securitate şi auditorilor.

Frecvenţa analizei jurnalelor de evenimente

Înregistrările din jurnalul de evenimente trebuie revăzute în detaliu cel puţin o dată pe lună. Orice eveniment având o importanţă semnificativă trebuie explicat şi descris într-un jurnal. Procesul de verificare a jurnalului include verificarea unor eventuale falsificări, sau modificări şi verificarea fiecărei alerte sau anomalii consemnată în log-uri. Orice acţiune executată ca rezultat al funcţionări defectuoase detectate trebuie înregistrată în jurnal.

Perioada de retenţie a jurnalelor de evenimente

Înregistrările evenimentelor sunt stocate în fişiere pe discul sistem până când acestea ajung la capacitatea maximă permisă. După depăşirea spaţiului alocat, jurnalele sunt păstrate în arhive.

Jurnalele arhivate sunt păstrate cel puţin 10 ani.

Protecţia jurnalelor de evenimente

Săptămânal, fiecare înregistrare din jurnale face obiectul arhivării pe suport de stocare dedicat. După depăşirea numărului acceptat de înregistrări pentru un jurnal, conţinutul acestuia este arhivat. Arhivele pot semnate si criptate. O cheie folosită pentru criptarea arhivelor este plasată sub controlul administratorului de securitate.

Un jurnal de evenimente poate fi revăzut numai de administratorului de securitate, sau de către un auditor.

Accesul la jurnalul de evenimente este configurat în aşa fel încât:

- numai entităţile de mai sus au dreptul să citească înregistrările jurnalului,
- numai administratorul de securitate poate arhiva sau şterge fişiere (după arhivarea acestora) care conţin evenimentele înregistrate,
- este posibilă detectarea oricărei violări de integritate; acest lucru asigură faptul că înregistrările nu conţin goluri sau falsuri,
- nici o entitate nu are dreptul să modifice conţinutul unui jurnal.

În plus, procedurile de protecţie a jurnalului sunt implementate în aşa fel încât, chiar şi după arhivarea jurnalului, este imposibil să ştergi înregistrări, sau să ştergi jurnalul înaintea expirării perioadei de retenţie a jurnalului.

Procedurile de backup pentru jurnalele de evenimente

Procedurile de securitate MD-CP solicita ca jurnalul de evenimente să facă obiectul backup-ului lunar. Aceste backup-uri sunt stocate în locaţii auxiliare ale MD-CP.

Notificarea entităţilor responsabile de tratarea evenimentelor

Modulul de analiză a jurnalului de evenimente implementat în sistem examinează evenimentele curente şi sesizează automat activităţile suspecte sau pe cele care au ca scop compromiterea securităţii. În cazul activităţilor care au influenţă asupra securităţii sistemului, sunt notificaţi automat administratorul de securitate. În celelalte cazuri, notificarea este direcţionată numai către administratorul de sistem. Transmiterea informaţiilor către persoanele autorizate despre situaţiile critice – din punctul de vedere al securităţii sistemului – se face prin alte mijloace de comunicare, protejate corespunzător, de exemplu: telefon mobil, poştă electronică. Entităţile notificate iau măsurile corespunzătoare pentru a proteja sistemul faţă de ameninţarea detectată.

Procedura de backup si restaurare

Copiile de siguranţă permit restaurarea completă (dacă este necesar, de exemplu, după distrugerea sistemului) a datelor esenţiale pentru activitatea MD-CP. Pentru a realiza acest lucru, sunt copiate următoarele aplicaţii şi fişiere:

- discurile de instalare a aplicaţiilor sistem (de exemplu sistemul de operare),
- discurile de instalare a aplicaţiilor pentru MD-CP,
- istoricul cheilor,
- datele privind personalul MD-CP,
- jurnalele de evenimente.

Metoda de creare a copiilor de backup are o influenţă deosebită asupra timpului şi costului restaurării aplicaţiilor după defectarea, sau distrugerea sistemului. MD-CP foloseşte atât backup-uri full (săptămânale), cat şi backup-uri incrementale (zilnice), toate copiile sunt clonate şi clonele sunt păstrate în altă locaţie, în aceleaşi condiţii de securitate ca şi cele din locaţia primară.

Procedura de restaurare va fi verificata cel puţin o data la 6 luni, pentru a se verifica utilitatea backup-ului, în caz de dezastru. Concluziile testelor vor fi înregistrate.

2.5.7 Arhivarea înregistrărilor

Este necesar ca toate datele şi fişierele referitoare la informaţiile despre securitatea sistemului să fie arhivate.

Pe baza arhivelor se creează copiile de siguranţă care sunt ţinute în afara locaţiei MD-CP.

Tipurile de date arhivate

Următoarele date sunt incluse în procesul de arhivare:

- informaţiile rezultate în urma examinării şi evaluării (ca urmare a unui audit) măsurilor de protecţie logica şi fizica ale MD-CP,
- fişiere de audit,
- fişiere de configurare.

Frecvența arhivării datelor

Datele se arhivează cel puțin o data pe săptămână.

Perioada de păstrare a arhivelor

Arhivele de păstrează cel puțin 10 ani.

3 Controale de securitate fizică, organizațională și de personal

Acest capitol descrie cerințele generale privind securitatea fizică și organizațională, precum și activitatea personalului MD-CP în activitatea de management al cheilor, personalizarea logica si optica a cardurilor, audit și crearea de copii de siguranță.

3.1 Controale de securitate fizică

3.1.1 Controale de securitate fizică în cadrul MD-CP

Sistemele de calcul, terminalele operatorilor și resursele informaționale ale MD-CP sunt dispuse într-o zonă dedicată, protejată fizic împotriva accesului neautorizat, distrugerilor sau perturbării activității. Aceste locații sunt monitorizate. Fiecare intrare și ieșire este înregistrată în jurnalul de evenimente (log-urile sistemului); stabilitatea sursei de electricitate precum și temperatura sunt de asemenea monitorizate și controlate.

Amplasarea locației

MD-CP este localizată în București, la următoarea adresă:

Bulevardul Tudor Vladimirescu, nr. 29 A, AFI Tech Park 1,

Sector 5, București, România, CP 050881

Accesul fizic

Accesul fizic în cadrul MD-CP este controlat și monitorizat de un sistem de alarmă integrat. MD-CP dispune de sisteme de prevenire a incendiilor, sisteme de detectare a intruşilor și sisteme de alimentare cu energie electrică în caz de urgență.

Sediul MD-CP este accesibil numai persoanelor autorizate de către conducerea MD-CP. Vizitatorii locațiilor aparținând MD-CP trebuie să fie însoțiți permanent de persoane autorizate.

Zonele ocupate de MD-CP se împart în:

- zona serverelor,
- zona operatorilor CP
- zona de dezvoltare și testare.

Zona serverelor este echipată cu un sistem de securitate monitorizat continuu, alcătuit din senzori de mișcare, efracție și incendiu. Accesul în această zonă este permis numai personalului autorizat, de exemplu, administratorul de securitate, administratorul HSM și administratorul de sistem. Monitorizarea drepturilor de acces se face folosind carduri și cititoare, montate lângă punctul de acces. Fiecare intrare și ieșire din zonă este înregistrată automat în jurnalul de evenimente.

Controlul accesului în *zona operatorilor* se face prin intermediul cardurilor şi a cititoarelor de carduri. Deoarece toate informaţiile senzitive sunt protejate prin folosirea unor seifuri, iar accesul la terminalele operatorilor şi administratorilor necesită în prealabil autorizarea acestora, securitatea fizică în această zonă este considerată ca fiind adecvată. Cheile de acces pot fi ridicate numai de personalul autorizat. În această zonă au acces numai angajaţii MD-CP şi persoanele autorizate; ultimilor nu le este permisă prezenţa în zonă neînsoţiţi.

Zona de dezvoltare şi testare este protejată într-o manieră similară cu zona operatorilor. În această zonă este permisă şi prezenţa persoanelor neînsoţite. Programatorii şi dezvoltatorii nu au acces la informaţii senzitive. Dacă este necesar un astfel de acces, atunci el se poate face numai în prezenţa administratorul de securitate. Proiectele în curs de implementare şi software-ul aferent este testat în mediul de dezvoltare al MD-CP.

Sursa de alimentare cu electricitate şi aerul condiţionat

Zona operatorilor şi administratorilor, precum şi zona de dezvoltare şi testare sunt prevăzute cu aer condiţionat. Din momentul întreruperii alimentării cu energie, sursele de electricitate de urgenţă (UPS) permit continuarea neperturbată a activităţii până la intervenţia automată a grupului electrogen al clădirii.

Expunerea la apă

Riscul de inundaţie în zona serverelor este foarte mic, deoarece distanţa faţă de conductele de apă este mare. Locaţia MD-CP dispune de sistem de prevenire a inundaţiilor, fiind utilizaţi senzori amplasati la nivelul podelelor în conformitate cu standardele şi reglementările în domeniu.

Prevenirea incendiilor

Locaţia MD-CP dispune de sistem de prevenire şi protecţie împotriva incendiilor în conformitate cu standardele şi reglementările în domeniu.

Depozitarea mediilor de stocare a informaţiilor

În funcţie de sensibilitatea informaţiilor, mediile electronice care conţin arhivele şi copiile de siguranţă ale datelor curente sunt stocate în seifuri metalice, localizate într-o camera cu grad ridicat de securitate. Accesul la camera şi seifuri este permis numai persoanelor autorizate.

Aruncarea deşeurilor

Hârtiile şi mediile electronice care conţin informaţii importante din punct de vedere al securităţii MD-CP sunt distruse după expirarea perioadei de păstrare. Modulele de securitate hardware sunt resetate şi şterse conform recomandărilor producătorului. Aceste dispozitive sunt, de asemenea, resetate şi şterse atunci când sunt trimise în service sau reparate.

Depozitarea backup-urilor în afara locaţiei

Copiile parolelor, codurile PIN şi cardurile criptografice pentru autorizarea accesului sunt stocate în containere speciale, situate în afara locaţiei MD-CP.

Stocarea în afara locaţiei se aplică şi în cazul arhivelor, copiilor curente ale informaţiilor procesate de sistem şi kit-urilor de instalare ale aplicaţiilor MD-CP. Acest lucru permite refacerea de urgenţă a oricărei funcţii a MD-CP în 24 de ore, în locaţia principală a MD-CP, sau în locaţia auxiliară.

3.2 Controlul securităţii organizaţiei

Acest capitol prezintă rolurile ce pot fi atribuite personalului aparţinând MD-CP. De asemenea, tot în acest capitol sunt descrise responsabilităţile şi sarcinile specifice fiecărui rol.

3.2.1 Roluri de încredere

Roluri de încredere în MD-CP

În MD-CP sunt definite următoarele roluri de încredere, care pot fi atribuite uneia sau mai multor persoane:

- **Responsabilul MD-CP**
  - Răspunzător pentru operarea sigura si continua a funcţiei MD-CP,
  - Este reprezentantul organizaţiei si este autorizat sa ia decizii in cadrul organizaţiei MD-CP,
  - Nu este direct implicat in implementarea proceselor de afaceri, dar este responsabil pentru respectarea si evaluarea masurilor de securitate, ca si pentru managementul MD-CP,
  - Accepta responsabilitatea pentru managementul schimbării.
- **Administrator de securitate** – Responsabilitate globală pentru implementarea politicilor şi procedurilor de securitate.
  - Iniţiază instalarea, configurarea şi managementul aplicaţiilor software şi hardware (inclusiv resursele de reţea) ale MD-CP; iniţiază şi suspendă serviciile oferite de MD-CP; coordonează administratorii, iniţiază şi supraveghează generarea de chei şi secrete partajate; atribuie drepturi din punct de vedere al securităţii şi privilegiilor de acces ale utilizatorilor; atribuie parole pentru conturile utilizatorilor noi; verifică jurnalele de evenimente; supervizează auditurile interne şi externe; primeşte şi răspunde la rapoartele de audit; supervizează eliminarea deficienţelor constatate în urma auditului.
  - Supraveghează operatorii;
  - Configurează sistemele şi reţeaua, activează şi configurează mecanismele de protecţie a reţelei; creează conturile pentru utilizatorii MD-CP; verifică log-urile de sistem; verifică respectarea Codului de Practici şi Proceduri; generează secrete partajate şi chei; creează copiile de siguranţă de urgenţă; modifică numele şi adresele serverelor.

- **Administratorul de sistem** – Autorizat să instaleze, configureze şi să întreţină sistemele de încredere ale MD-CP pentru managementul cardurilor si al cheilor. Instalează dispozitivele hardware şi sistemele de operare; instalează şi configurează echipamentele de reţea.
- **Operator** – Responsabil de operarea zilnică a sistemelor de încredere ale MD-CP; la parte in procesul de personalizare logica si optica a cardurilor.
- **HSM Administrator**
  - Autorizează accesul la HSM pentru procesul de management al cheilor,
- **Auditorul de sistem** – autorizat să acceseze arhivele şi log-urile de audit ale sistemelor de încredere ale MD-CP. Responsabil de efectuarea de audituri interne pentru respectarea Codului de Practici şi Proceduri de către personalul MD-CP;

*În cadrul MD-CP, rolul de **auditor** nu poate fi combinat cu nici un alt rol. O entitate care are un rol diferit de cel de auditor nu poate prelua responsabilităţile auditorului.*

3.2.2 Numărul de persoane necesare pentru îndeplinirea unei sarcini

Procesul de generare de chei – pentru certificatele cardurilor de tahograf sau pentru generarea KDR si importul KDM este una din operaţiile ce necesită o atenţie deosebită. Generarea necesită prezenţa persoanelor care deţin următoarele roluri:

I. Acţiunea de personalizare carduri: 3 operatori CP si un administrator de sistem,
II. Acţiunea de generare KDR si import KDM: un administrator de securitate, 3 administratori de HSM si un administrator de sistem.

3.2.3 Identificarea şi autentificarea pentru fiecare rol

Personalul MD-CP este supus identificării şi autentificării în următoarele situaţii:

- plasarea pe lista de persoane care au dreptul de a accesa locaţiile MD-CP,
- plasarea pe lista de persoane care au acces fizic la sisteme şi resurse de reţea aparţinând MD-CP,
- emiterea confirmării care autorizează îndeplinirea rolului asignat,
- asignarea unui cont şi a unei parole în sistemul informatic al MD-CP,

Fiecare cont asignat:

- trebuie să fie unic şi asignat direct unei anumite persoane,
- nu poate fi folosit în comun cu nici o altă persoană,
- trebuie restricţionat conform funcţiei (ce reiese din rolul îndeplinit de persoana respectivă) pe baza software-ului de sistem al MD-CP, a sistemului de operare şi a controalelor de aplicaţii.

Operaţiile efectuate în MD-CP care necesită acces la resurse de reţea comune sunt protejate prin mecanisme de autentificare sigură şi de criptare a informaţiilor transmise.

3.3 Controlul personalului

MD-CP trebuie să se asigure că persoana care îndeplineşte responsabilităţile funcţiei, conform cu rolul atribuit în cadrul MD-CP:

- a absolvit cel puţin liceul,
- este cetăţean român,
- a semnat un contract care descrie rolul şi responsabilităţile sale în cadrul sistemului,
- a beneficiat de un stagiu de pregătire avansată în conformitate cu obligaţiile şi sarcinile asociate funcţiei sale,
- a fost instruit cu privire la protecţia datelor personale şi informaţiilor confidenţiale sau private,
- a semnat un contract ce conţine clauze referitoare la protejarea datelor confidenţiale (din punctul de vedere al securităţii MD-CP),

3.3.1 Experienţa personală, calificările şi clauzele de confidenţialitate necesare

Personalul angajat al MD-CP care îndeplineşte un rol de încredere, trebuie să obţină avizul responsabilului de securitate. Avizul nu este necesar în cazul persoanelor care nu exercită un rol de încredere.

Îndeplinirea unei funcţii de încredere permite accesul la informaţiile clasificate. Dezvăluirea neautorizată a acestor informaţii poate cauza pierderea sau compromiterea intereselor, apărate de lege, ale unei persoane fizice sau ale unei organizaţii.

Procedurile de acces la informaţiile nepublice şi de verificare a încrederii în personal sunt în conformitate cu Legea Protecţiei Datelor cu Caracter Personal.

3.3.2 Cerinţele de pregătire a personalului

Personalul care îndeplineşte roluri şi sarcini ca urmare a angajării la MD-CP, trebuie să fie instruit cu privire la:

- reglementările Codului de Practici şi Proceduri al MD-CP,
- reglementările Politicii de certificare a MD-CA,
- procedurile şi controalele de securitate folosite de MD-CA,
- aplicaţiile software ale MD-CP,
- responsabilităţile ce decurg din rolurile şi sarcinile executate în sistem,
- procedurile ce trebuie executate ca urmare a apariţiei unei defecţiuni în funcţionarea sistemului.

După încheierea pregătirii, participanții semnează un document prin care confirmă familiarizarea lor cu Codul de Practici și Proceduri, Politica de certificare și acceptă restricțiile și obligațiile impuse.

3.3.3 Frecvența stagiilor de pregătire

Pregătirea descrisă în paragraful 3.3.2 trebuie repetată de fiecare dată când apar modificări semnificative în MD-CP.

3.3.4 Rotația funcțiilor

Acest Cod de Practici și Proceduri nu specifică nici un fel de cerințe în această privință.

3.3.5 Sancționarea acțiunilor neautorizate

În cazul descoperirii sau existenței suspiciunii unui acces neautorizat, administratorul de sistem împreună cu administratorul de securitate poate suspenda accesul persoanei respective la sistemul MD-CP. Măsurile disciplinare pentru astfel de incidente trebuie descrise în regulamente corespunzătoare și trebuie să fie conforme cu prevederile legale.

3.3.6 Personalul angajat pe baza de contract

Personalul angajat pe baza de contract (servicii externe, dezvoltatori de subsisteme sau aplicații etc.) fac obiectul unor verificări similare ca și în cazul angajaților MD-CP. În plus, personalul angajat pe bază de contract, pe timpul cât își desfășoară activitatea în locația MD-CP, trebuie permanent însoțit de către un angajat al MD-CP, cu excepția celor care au primit avizare din partea administratorului de securitate și care poate accesa informații clasificate intern sau în conformitate cu normele legale în vigoare.

3.3.7 Documentația oferită personalului

MD-CP trebuie să ofere personalului său accesul la următoarele documente:

- Politica de certificare a MSA,
- Codul de Practici și Proceduri al MD-CP,
- Responsabilitățile și obligațiile asociate rolului deținut în sistem.
- Manuale ale aplicațiilor.
- Manuale de operare.
- Proceduri operaționale.

4 AUDITURILE PENTRU STABILIREA CONFORMITATII SI ALTE EVALUARI

Auditurile au ca obiectiv verificarea consistenței acțiunilor MD-CP sau a entităților delegate de aceasta cu declarațiile și procedurile acestora (inclusiv cu prezentul Cod de Practici și Proceduri).

Auditurile desfășurate la MD-CP urmăresc în principal centrele de procesare a datelor, gestiunea cardurilor si a PIN-urilor, procedurile de gestiune a cheilor.

Auditurile desfășurate la MD-CP pot fi efectuate de echipe interne (audit intern) sau de MD-MSA sau organizații independente (audit extern) angajate de aceasta. În toate aceste cazuri, auditul se desfășoară sub supravegherea administratorului de securitate.

Frecvența auditării

Auditul extern prin care se verifică compatibilitatea cu reglementările legale și procedurale (Codul de Practici și Proceduri) se desfășoară anual, în timp ce un audit intern este efectuat ori de cate ori administratorul de securitate considera necesar.

4.1 Identitatea / calificările auditorului

Auditul extern trebuie realizat de personal având cunoștințe și experiență tehnică corespunzătoare (să dispună de documente care să certifice acest lucru) în domeniul infrastructurilor de chei publice, tehnologiilor și dispozitivelor de securitate informatică și de auditare a securității sistemelor. De asemenea auditorul trebuie sa posede cunoștințe solide ale reglementarilor UE, CE si MD-MSA referitoare la sistemul tahografelor digitale.

Auditul intern este realizat de către departamentul de calitate și audit al MD-CP.

4.2 Relația auditorilor cu entitatea auditată

Vezi paragraful anterior. Auditorul nu trebuie sa depindă in nici un fel de entitatea auditata si nici sa nu fi fost in vreun fel implicat in activitățile de planificare si operare ale sistemelor ITC ale entității auditate.

4.3 Domeniile supuse auditării

Auditurile interne și externe se desfășoară conform regulilor și procedurilor acceptate pe plan internațional și vizează:

- securitatea fizică a MD-CP,
- procedurile de furnizare a serviciilor,
- securitatea aplicațiilor software și a accesului la rețea,
- securitatea personalului MD-CP,
- securitatea gestiunii cardurilor,
- jurnalele de evenimente și procedurile de monitorizare a sistemului,

- arhivarea şi restaurarea datelor,
- procedurile de arhivare,
- înregistrările referitoare la modificarea parametrilor de configurare pentru MD-CP,
- înregistrările referitoare la analizele şi verificările efectuate pentru aplicaţiile software şi dispozitivele hardware.

4.4 Analiza vulnerabilităţilor

MD-CP face anual o analiză a vulnerabilităţilor pentru fiecare procedură internă, aplicaţie şi sistem informatic. Cerinţele de analiză pot, de asemenea, să fie stabilite de către o instituţie externă, autorizată să auditeze MD-CP. Administratorul de securitate are sarcina de a solicita audituri interne prin care să verifice conformitatea înregistrărilor din jurnalul de securitate, corectitudinea copiilor de backup, activităţile executate în cazul apariţiei unei ameninţări şi conformitatea cu Codul de Practici şi Proceduri.

Instituţia externă care efectuează auditul de securitate, trebuie să desfăşoare această activitate respectând recomandările ISO/IEC 13335 (Guidelines for Management of IT Security) şi ISO/IEC 17799 (Code of Practice for Information Security Management).

4.5 Măsurile întreprinse ca urmare a descoperirii unei deficienţe

In cazul descoperirii unor deficiente se pot lua trei tipuri de masuri:

1. continuarea operaţiilor
2. continuarea limitata a operaţiilor;
3. suspendarea operaţiilor.

Auditorul, împreuna cu MD-MSA, decide ce acţiune trebuie întreprinsa. Decizia se bazează pe gravitatea deficientelor si a posibilului impact.

In cazul in care se decide acţiunea de tipul 1, managementul MD-CP este răspunzător pentru implementarea masurilor corective specificate in raportul de audit, in limitele de timp din acelaşi raport.

In cazul in care se decide acţiunea de tipul 2, MD-CP continua operaţiile in modul restrâns indicat in raportul de audit.

In cazul in care se decide acţiunea de tipul 3, toate cardurile afectate trebuie trecute pe un backlist. Managementul MD-CP trebuie sa raporteze săptămânal stadiul masurilor de remediere către auditor. MD-MSA si auditorul determina când trebuie făcuta o noua evaluare de securitate. Daca deficientele sunt considerate ca remediate după reevaluare, atunci MD-CP îşi poate relua operaţiile.

9.6 Comunicarea rezultatelor

Rezultatele auditului anual sunt comunicate către MD-MSA. In cazul acţiunilor de tipul 1 sau 2, MD-MSA se asigura de faptul ca toate entităţile care trebuie notificate primesc informaţiile in conformitate cu prezentul document.

Sistemul de Tahograf Digital pentru Republica Moldova

Codul de Practici şi Proceduri pentru implementarea Politicii de Certificare a MD-CA si operarea MD-CA

certSIGN®

CUPRINS

1 INTRODUCERE

Agentia Nationala Transport Auto este responsabila pentru funcţia de Autoritate Naţionala de Certificare a infrastructurii de management a cheilor criptografice din cadrul sistemului de tahografe digitale introdus prin Reglementarea Consiliului UE nr. 3821/85, revizuita prin Reglementarea Comisiei CE nr. 1360/2002 si Reglementarea Comisiei CE nr. 432/2004.

Aceasta infrastructura de chei publice consta din sisteme, produse si servicii care asigura:

- Certificate pentru chei publice pentru componente de tahograf (carduri, unitati de vehicul si senzor de mişcare);
- Chei de criptare pentru datele senzorilor de mişcare.

Scopul acestui document este acela de a descrie practicile de certificare implementate de MD-CA.

Documentul a fost creat pentru a asigura conformitatea cu cerinţele enunţate in Politica de Certificare a MD-CA si se bazează pe cadrul creat prin IETF RFC 3647.

1.1 Descriere generala

Scopul principal al acestui document este acela de a fi folosit de către MD-MSA si de către cei care doresc sa evalueze gradul de încredere care poate fi acordat serviciilor oferite de MD-CA, sau sa determine măsura in care acestea respecta cerinţele sistemului pentru tahografe digitale.

Sistemul de management al cheilor criptografice (vezi figura următoare) este necesar pentru a implementa mecanismele de securitate definite in:

- Reglementarea Comisiei CE nr. 1360/2002, Anexa I(B), Appendix 11 Common Security Mechanisms
- ISO / IEC 16844-3 Road vehicles, Tachograph systems, Part 3: Motion sensor interface.

MD-CA si MD-CP sunt operate sub responsabilitatea si autoritatea autoritatilor nationale sau a furnizorilor de servicii externi autorizaţi.

MD-CA are rolul de a certifica cheile RSA care sunt introduse in cardurile pentru tahografe de către MD-CP.

Mai multe tipuri de carduri sunt emise şoferilor, atelierelor, organelor de control si firmelor de transport.

MD-CA isi schimba cheile la intervale regulate.

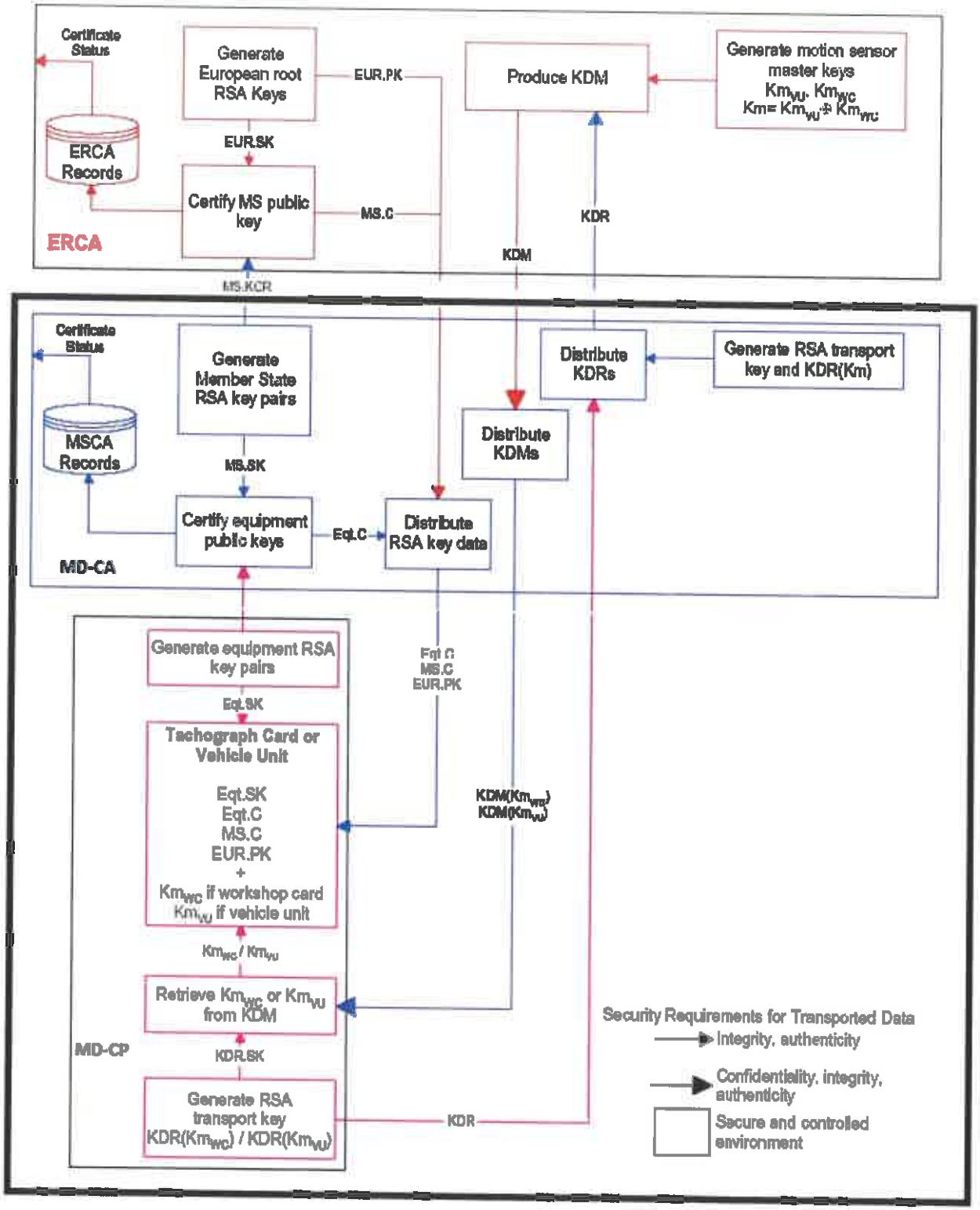
Formatul certificatelor digitale folosite este proprietar si incompatibil cu formatul X.509, al certificatelor digitale a caror utilizare este presupusa , dar nu ceruta obligatoriu de catre IETF RFC 3647.

MD-CA genereaza, separa si distribuie o singura cheie criptografica simetrica, necesara pentru securizarea datelor de miscare ale vehiculelor, in conformitate cu mecanismele definite de standardul ISO / IEC 16844-3.

Cheia master Km este separata in doua parti , Km_{VU} si Km_{WC}. Km_{WC} sunt inserate in cardurile de atelier de catre personalizatorii de carduri.

Pentru a asigura confidențialitatea cheii Km_{WC} in timpul transportului de la ERCA la MD-CA, ERCA o criptează folosind o cheie publica de criptare RSA, pentru a produce un mesaj de distribuție a cheii (KDM). Același lucru este valabil si pentru transportul aceleiași cheii Km_{WC} de la MD-CA la MD-CP. Cheile RSA folosite la crearea mesajelor KDM sunt create de MD-CA sau MD-CP si trimise catre ERCA sau respectiv MD-CA printr-o cerere de distribuție (KDR).

Necesitatea ca MD-CA sau MD-CP sa primească cheia Km_{WC} este definita intr-un acord semnat de ERCA si MD-MSA.


Certificate Status
Generate European root RSA Keys
EUR.PK
Produce KDM
Generate motion sensor master keys
Km_VU, Km_WC
Km= Km_VU * Km_WC
ERCA Records
EUR.SK
Certify MS public key
MS.C
KDR
ERCA
KDM
MS.KCR
Certificate Status
Generate Member State RSA key pairs
Distribute KDRs
Generate RSA transport key and KDR(Km)
MSCA Records
Distribute KDMs
MS.SK
Certify equipment public keys
Eqt.C
Distribute RSA key data
MD-CA
Generate equipment RSA key pairs
Eqt.C
MS.C
EUR.PK
Eqt.SK
Tachograph Card or Vehicle Unit
Eqt.SK
Eqt.C
MS.C
EUR.PK
+
Km_WC if workshop card
Km_VU if vehicle unit
KDM(Km_WC)
KDM(Km_VU)
Km_WC / Km_VU
Retrieve Km_WC or Km_VU from KDM
MD-CP
KDR.SK
Generate RSA transport key KDR(Km_WC) / KDR(Km_VU)
KDR
Security Requirements for Transported Data
Integrity, authenticity
Confidentiality, integrity, authenticity
Secure and controlled environment

1.2 Numele si Identificarea Documentului

Acest document poarta denumirea de "Practicile si Procedurile de Certificare ale Autoritatii de Certificare Moldovene pentru Sistemul Tahografelor Digitale" si va fi referit in continuare simplu ca CPP.

1.3 Participanti

Acest CPP este creat doar pentru a îndeplini cerinţele sistemului pentru tahografe digitale.

1.3.1 Autoritatea de Certificare

MD-CA si MD-CP sunt operate sub autoritatea si responsabilitatea autoritatilor moldovene responsabile, sau a furnizorilor de servicii autorizaţi. MD-CA este certificat de ERCA.

1.3.2 Autoritatea de Înregistrare

Autoritatea Nationale de Înregistrare implementează sisteme, produse si servicii necesare pentru emiterea de carduri de tahograf. RA-ul naţional este responsabil pentru a menţine legătura între identificatorii subiecţilor certificatelor (cardurile) si persoanele fizice sau juridice care le folosesc. In Moldova, funcţia RA pentru emiterea de certificate digitale pentru carduri de tahograf si cheii Km_{wc} este asigurata de MD-CIA.

1.3.3 Abonaţi

Abonaţii serviciilor de certificare oferite de MD-CA sunt cardurile de tahograf.

1.3.4 Entităţile partenere

1.3.5 Destinatarii Cheilor pentru Senzorii de Miscare

Destinatarii cheilor Km_{wc} sunt organizaţiile care personalizează cardurile de atelier. Acestea sunt identificate in acordul semnat intre ERCA si MD-CA.

1.4 Utilizarea certificatului

Certificatele de cheie publica pentru tahografe trebuie inserate in componentele tahografelor digitale, aşa cum se cere in procesul de autentificare mutuala descris in cerinţa CSM_020 Reglementarea 1360/2002, Annex I(B) Appendix 11 Common Security Mechanism.

Certificatele pentru tahografele digitale pot fi folosite in aplicaţii in legătura sistemul tahografelor digitale (de exemplu: Echipamente de calibrare utilizate in ateliere, echipamente pentru descărcarea de date folosite de organele de control, sisteme de management al flotelor auto si/sau mărfurilor folosite de firmele de transport etc.).

Certificatele pentru tahografe digitale nu pot fi folosite pentru nici un alt scop.

1.5 Utilizarea Mesajului pentru Distribuirea Cheii (KDM)

Mesajele KDM trebuie folosite doar in scopul transmiterii securizate a cheii Km_{wc} intre ERCA si MD-CA si intre MD-CA si MD-CP.

1.6 Administrarea CPP

1 Acest CPP este creat, menţinut si revizuit de catre S.C. CERTSIGN S.A., care indeplineşte funcţia de

furnizor de servicii de certificare pentru MD-CA, fiind declarat ca "service agency for MD-CA" conform politicii de securitate "MD CA Policy", aprobata de catre ERCA:

Autoritatea de Certificare pentru Sistemul Moldovean de Tahografe Digitale

S.C. CERTSIGN S.A.

Sediu Social: Sos. Oltenitei nr. 107 A, clădirea C1, parter

Sector 4, CP 041303, Bucureşti, Romania

Sediu: Bulevardul Tudor Vladimirescu, nr. 29 A, AFI Tech Park 1,

Sector 5, Bucureşti, România, CP 050881

Tel. (+4031)1011870

Fax: (+4021)3119905

2. Orice întrebare referitoare la prezentul CPP trebuie trimisa catre S.C. CERTSIGN S.A.
3. Orice întrebare referitoare la operarea MD-CA trebuie trimise catre S.C. CERTSIGN S.A.
4. Autoritatea Naţionala, MD-MSA, trebuie sa stabilească daca acest CPP este conform cu Politica de Certificare a MSA.
5. Stabilirea conformităţii se bazează pe o evaluare de securitate realizata fie chiar de catre MD-MSA, fie de un terţ autorizat.

1.7 Definiţii si Acronime

Criptare Asimetrica: procesul de criptare in care o cheie este folosita pentru a cripta mesajul si o cheie diferita este utilizata pentru decriptarea mesajului.

Detectarea intruziunii: detectarea unei intruziuni fizice de catre un agent de paza, sau a uneia informatice de catre un sistem care cuprinde un senzor, un mediu de transmisie si un panou de alarma unde se trimite alarma.

Escrow-ul cheii: trimiterea unei copii a cheii catre o entitate autorizata sa folosească aceasta copie pentru alt scop decât acela de a-l returna entităţii care a generat cheia.

Criptare simetrica: procesul de criptare in care aceeaşi chei este folosita si la criptarea mesajului si la decriptarea lui.

CAR	Certification Authority Reference
CHA	Certificate Holder Authorisation
CHR	Certificate Holder Reference
CP	Component Personaliser
CPI	Certificate Profile Identifier
CPS	Certification Practices Statement
CRL	Certificate Revocation List
CSP	Certification Service Provider
DES	Data Encryption Standard (symmetric encryption scheme)
EA	European Authority
ENI	ESSOR Nuclear Island
EOV	End Of Validity
ERCA	European Root Certification Authority
ETSI	European Telecommunications Standards Institute
KCR	Key Certification Request
KDR	Key Distribution Request
KDM	Key Distribution Message
Km	Motion sensor master key
Km_{wc}	Motion sensor master key inserted in workshop card
NCA	National Certification Authority
MD-MSA	Moldavia Authority
MD-CA	Moldavia Certification Authority
MD-CIA	Moldavia Card Issuance Authority

OA	Operating Agent
OE	Operational Entity (used to refer to both a NCA and a CP)
OM	Operations Manager
PK	RSA public key
PKI	Public Key Infrastructure
PR	Permanent Representation of Member State
RSA	Rivest, Shamir, Adleman (asymmetric encryption scheme)
SAS	Single access system
SK	RSA secret key
TDES	Triple DES

2 PUBLICAREA INFORMATIEI MD-CA

2.1 Depozitele de informații

Informații publice cu privire la politica națională se găsesc pe site-ul http://www.anta.gov.md/.

2.2 Publicarea informației MD-CA

MD-CA publica următoarele informații pe website-ul sau:

- Politica de Certificare MD-CA;
- Codul de Practici si Proceduri al MD-CA (acest document);
- Propunerile de modificare al CP si CPP MD-CA;
- MD-CA public key;

Conformitatea Politicii de Certificare a MD-CA este stabilita de catre ERCA la sfârșitul procesului de revizuire a politicii nationale, definit in Politica ERCA.

2.3 Frecventa publicării

Informațiile referitoare la modificările CP si CPS sunt publicate in conformitate cu planificările făcute in cadrul procedurilor de schimbare din fiecare document.

3 IDENTIFICAREA SI AUTENTIFICAREA

3.1 Nume

Conceptul de nume ca un identificator al unei persoane fizice sau juridice nu se aplica in cazul certificatelor produse de MD-CA.

Emitentul certificatului si subiectul certificatului sunt identificaţi prin stringuri de lungime fixa de 8 octeti care conţin informaţia ceruta de protocolul mutual de autentificare dintre componentele tahografice, definit in Reglementarea Comisie nr 1360/2002, Annex I(B) Appendix 11, cerinţa CSM020.

3.1.1 Tipuri de Nume

Emitentul Certificatului si al KDM

Identificarea emitentului certificatului si al KDM se face prin referinţa Certification Authority Reference (CAR), un string de 8 octeti definit in Reglementarea Comisiei nr. 1360/2002, Annex I(B) Appendix 1 - Data Dictionary, Section 2.36 CertificationAuthorityKID.

CAR este de asemenea folosita in timpul procedurii mutuale de autentificare dintre componentele tahografului pentru a identifica cheia publica folosita la verificarea certificatului.

Subiectul Certificatului

Acesta este format din:

- Certificate Holder Reference (CHR), un string de 8 octeti string definit in Reglementarea Comisiei nr. 1360/2002 Annex I(B) Appendix 1, Section 2.36 CertificationAuthorityKID;
- Certificate Holder Authorisation (CHA), un string de 7 octetistring definit in Reglementarea Comisiei nr. 1360/2002, Annnex I(B) Appendix 1, Section 2.34 si include EquipmentType, 1 octet as definit in Reglementarea Comisiei nr. 1360/2002 Annex I(B) Appendix 1, Section 2.52. Pentru certificatele de chele publica emise de MD-CA, EquipmentType desemnează o cartela de tahograf.

CHR apare in materialele printate si in datele descărcate din unitatea de vehicul. EquipmentType codificat in CHA este folosit in timpul procedurii mutuale de autentificare si selectează unul dintre cele patru moduri de operare ale unitatii de vehicul (operare, calibrare, control sau companie).

Key Distribution Message Recipient

Destinatarul final al cheii senzorului de miscare Km_{wc} este MD-CP. In scopul distribuției acesteia, fiecare cerere KDR este identificata astfel:

- Key Identifier (KID): un string de 8 octeti definit in Politica ERCA [3] Annex D. 1.
- Message Recipient Authorisation (MRA): un string de 7 octeti definit in Politica ERCA [3] AnnexD.1.

KID identifica unic cheia publica RSA folosita la criptarea cheii senzorului de miscare. MRA identifica cheia senzorului de miscare.

3.1.2 Necesitatea ca numele sa albă inteles

Intelesul pe care il au:

- Emitentul certificatului
- Subiectul certificatului
- Destinatarul KDM
- Sunt definite in Reglementarea Comisiei nr. 1360/2002 Annex I(B) Appendix 1; si in Politica ERCA, Annex D.

3.1.3 Anonimatul sau folosirea pseudonimelor pentru abonati

Legatura dintre nume si persoanele fizice sau juridice este asigurata de RA; ea nu poate fi stabilita din continutul certificatelor de cheie publica.

Ca urmare, numele utilizate de MD-CA pentru certificarea si distribuirea cheilor folosite in tahografele digitale sunt pseudonime pentru abonatii MD-CA.

Anonimatul abonatilor nu este permis.

3.1.4 Reguli pentru interpretarea diferitelor forme ale numelor

Nu se stipulează nimic.

3.1.5 Unicitatea numelor

Pentru ca procesul autentificării mutuale sa funcționeze corect, identificatorul emitentului certificatului trebuie sa ide notifice unic o pereche de chei RSA.

3.1.6 Recunoașterea, autentificare si rolul brandurilor

Nu se stipulează nimic.

3.2 Validarea inițiala a identitatii

3.2.1 Metoda pentru a demonstra posesia cheii private

Abonatii care trimit cereri KCR trebuie sa demonstreze posesia cheii private corespunzătoare. Protocolul KCR este definit in Politica ERCA.

Mesajele KCR constau din doua parti: o parte de text necodificat si semnătura digitala a acelui text. Întotdeauna textul include o cheie publica RSA. Semnătura digitala a textului este creata cu cheia privata

corespunzătoare.

Verificarea semnăturii digitale realizata cu cheia publica demonstrează:

- Posesia cheii private;
- Integritatea textului.

Verificarea semnăturii este făcuta la MD-CA. Daca verificarea eşuează, cererea de certificat este respinsa.

3.2.2 Autentificarea identitatii individuale

Subiecţii la care se refera MD-CA nu sunt persoane fizice. Aceasta secţiune se refera doar la cerinţele de identificare si autentificare pentru cererile de certificate de chele pentru carduri si pentru certificatele de cheie publica schimbate intre MD-CP si MD-CA.

Trebuie creata o legătura intre aplicat (driver/firma de transport/atelier/politie), card chele privata si certificat.

Daca generarea cheii are loc in afara cardului, atunci MD-CA creează certificatul cerut daca cel care face solicitarea demonstrează printr-o procedura agreata ca este in posesia cheii private.

3.3 Identificarea si Autentificarea pentru Cererile de Re-key

3.3.1 Identificarea si autentificarea pentru cererile de re-key de rutina

La fel ca la secţiunea 3.2 Validarea iniţiala a identitatii.

3.3.2 Identificarea si autentificarea pentru cererile de re-key după revocare

Nu se aplica

3.4 Identificarea si Autentificarea pentru Cererile de Revocare

Certificatele pentru cardurile de tahograf nu se revoca. Pierderea cartelei trebule raportata de catre posesorii acesteia la MD-CIA.

4 CERINTELE OPERATIONALE PENTRU CICLUL DE VIATA AL CERTIFICATELOR

4.1 Cererea de Certificat

4.1.1 Cine poate face o cerere de certificat

Viitorii posesori de carduri nu fac cereri de certificate, ci certificatele sunt emise pe baza informațiile furnizate in cererea pentru cardurile de tahograf si preluate din registrul MD-CIA. Cheia publica care trebuie certificata este extrasa din cererea de certificat. MD-CA accepta doar cererile de certificat primite de la MD-CP. Aplicațiile software de la MD-CA si cele de la MD-CP asigura ca o cerere de certificat este generata doar pentru acele carduri pentru care exista o cerere si ca cel care a făcut cererea este autentificat si autorizat.

4.1.2 Procesul de înregistrare si responsabilitățile asociate

Procesul de înregistrare este administrat la MD-CIA.

4.2 Procesarea Cererilor de Certificat

4.2.1 Identificarea si autentificarea

Funcțiile de identificare si autentificare sunt implementate la MD-CIA. MD-CP asigura prin aplicațiile sale software ca datele de intrare conțin informații care fac Certificate Holder Reference (CHR) unic.

4.2.2 Aprobarea sau respingerea cererilor de certificate

Daca cererile sunt semnate cu cheia privata asociata cheii publice care trebuie certificata, atunci cererea este acceptata. In caz contrar, ea este respinsa.

4.2.3 Timpul necesar pentru prelucrarea cererilor de certificate

După primirea unei cereri valide de certificat, acesta este emis in maxim 24 de ore.

4.3 Emiterea Certificatului

4.3.1 Acțiunile MD-CA în timpul emiterii certificatului

Următoarele informații sunt înregistrate în baza de date a MD-CA pentru fiecare operație de certificare de cheie:

- certificatul complet;
- modulul RSA (n) si exponentul public (e) ale cheii publice;
- perioada de validitate a certificatului;
- Certificate Holder Reference (pentru identificarea cheii publice RSA);
- Hashul SHA-1 pentru datele certificatului în format binar;
- Hashul SHA-1 pentru datele mesajului KCR în format binar;
- timestamp.

4.4 Acceptarea certificatului

4.4.1 Comportament care semnifica acceptarea certificatului

Acceptarea cardului înseamnă si acceptarea certificatului asociat.

4.4.2 Distribuirea certificatelor de carduri si a informației aferente

MD-CA trebuie sa exporte toate datele referitoare la certificat catre registrul MD-CIA în așa fel incat certificatele, cardurile si utilizatorii acestora sa fie asociați. MD-CIA se asigura ca informația aferenta devine disponibila celor care au nevoie de ea.

4.5 Folosirea Perechii de Chei si a Certificatului

4.5.1 Folosirea Perechii de Chei si a Certificatului

Certificatele pentru componentele sistemului de tahografe digitale sunt destinate numai in cadrul acestuia.

Utilizarea perechilor de chei	Ciclu de viata	Validitate certificat
Şofer	5 ani	5 ani
Companie	5 ani	5 ani
Controlor	2 ani	2 ani
Atelier	1 an	1 an

Utilizarea cheilor pentru cardurile de tahograf

4.5.2 Folosirea cheii publice si a certificatului de catre entităţile partenere

Vezi 4.4.2.

4.6 Reinnoirea Certificatului

Nu se aplica.

4.7 Re-key

Nu se aplica.

4.8 Modificarea Certificatului

Nu se aplica.

4.9 Revocarea Certificatului

Nu se aplica.

4.9.1 Cerinţe speciale referitoare la compromiterea cheii

Compromiterea cheii este un incident de securitate care cere o serie de acţiuni.

Daca cheia MD-CA este compromisa, sau se suspectează ca este compromisa, atunci MD-CA trebuie sa raporteze incidentul la MD-MSA. Investigaţiile care urmează si eventualele acţiuni sunt descrise in Politica de certificare naţionala.

4.9.2 Suspendarea certificatului

Nu se aplica.

4.10 Servicii de Verificare a Stării Certificatului

Nu se aplica.

4.11 Escrow-ul si Recuperarea Cheii

Escrow-ul cheii este strict interzisa de catre Politica ERCA.

5 CERINTELE CICLULUI DE VIATA AL CHEII SENZORULUI DE MISCARE

Mecanismele de securitate referitoare la senzorul de miscare al tahografului digital sunt descrise in ISO / IEC 16844-3. Cheile senzorului de miscare sunt generate de ERCA si trebuie distribuite in mod sigur catre MD-CA. Mai departe MD-CA le va distribui la cerere catre MD-CP.

Cheile de transport RSA transport trebuie sa aibă modul de 1024 biți. Generarea cheilor de transport este realizata intr-un mediu controlat si sigur de catre MD-CP, in conformitate cu Politica de Certificare MD-CA si cu Codul de Practici si Proceduri al MD-CP. Nu exista si nici nu se întrevăd pe viitor servicii similare cu suspendarea, revocarea sau verificarea stării pentru mesajele KDM.

5.1 Cererile pentru Serviciile de Distribuire a Cheii Senzorului de Miscare

5.1.1 Cine poate trimite o cerere de distribuire a cheii senzorului de miscare

MD-CA accepta cereri de distribuție doar de la MD-CP.

5.1.2 Procesul de înregistrare si responsabilitățile asociate

Procedura de inregistrare pentru destinatarii cheilor master ale senzorului de miscare este aceeași ca cea pentru serviciile de certificare ale MD-CA, descrise la secțiunea 4.1.2.

5.2 Procesarea cererilor KDR pentru cheia senzorului de miscare

Prin trimiterea de cererii KDR, destinatarii cheii senzorului de miscare adera la termenii prezentului CPP.

5.2.1 Identificarea si autentificarea

Aplicațiile de interfațare MD-CA cu MD-CP de la MD-CA si MD-CP cu MD-CA de la MD-CP creează un canal securizat (autentificarea sursei si criptarea mesajului) prin care circula cererile KDR de la MD-CP si răspunsurile KDM de la MD-CA. In plus cheia publica RSA de transport a cheii senzorului de miscare Km_{wc} generata la MD-CP este distribuita in mod sigur in mod offline catre MD-CA apoi încredințata curierului de încredere al MSA. La primirea cererii KDR, MD-CP răspunde cu un KDM in care cheia Km_{wc} este criptata cu cheia RSA de transport.

5.2.2 Timpul in care se procesează cererile de distribuţie KDR

5.3 Distribuirea KDM a cheii senzorului de miscare

5.3.1 Acţiunile MD-CA in timpul emiterii mesajului de distribuire a cheii senzorului de miscare

Următoarele informaţii sunt înregistrate in baza de date MD-CA pentru fiecare operaţie KDM:

- modulul RSA *(n)* si exponentul public *(e)* pentru cheia publica a mesajului KDM;
- Key Identifier (pentru identificarea cheii publice RSA);
- Hashul SHA-1 pentru mesajul KDM in format binar;
- Hashul SHA-1 pentru mesajul KDR;
- KDM status "Pending acceptance";
- timestamp;
- un flag de distribuţie one-time pentru cheia senzorului de miscare

5.4 Folosirea Cheii Senzorului de Miscare

5.4.1 Folosirea cheii de catre destinatar

Folosirea cheii senzorului de miscare este restricţionata la acele scopuri autorizate de Politicile ERCA si MD-CA pentru sistemul tahografelor digitale si in conformitate cu prezentul CPP.

Destinatarii folosesc cheia de transport RSA doar pentru a crea o cerere KDR si pentru a recupera cheia senzorului de miscare din KDM.

Nu exista nici o prevedere referitoare la perioadele de folosire a cheii master a senzorului de miscare.

5.4.2 Responsabilităţile Entităţilor Partenere

Nu exista nici o prevedere.

5.5 Cerinţe speciale referitoare la compromiterea cheii

Compromiterea cheii este un incident de securitate care reclama o serie de acţiuni.

Daca o copie a unei chei a senzorului de miscare a fost compromisa sau se suspectează ca este compromisa, atunci MD-CP trebuie sa raporteze incidentul catre MD-MSA pentru investigaţii si pentru acţiuni in conformitate cu politica naţionala. Rezultatul acestor investigaţii se raportează catre ERCA.

6 Controale de securitate fizică, organizaţională şi de personal

Acest capitol descrie cerinţele generale privind securitatea fizică şi organizaţională, precum şi activitatea personalului MD-CA în activitatea de generare de chei, verificarea autenticităţii entităţilor, emiterea şi publicarea certificatelor, revocarea certificatelor, audit şi crearea de copii de siguranţă.

6.1 Controale de securitate fizică

6.1.1 Controale de securitate fizică în cadrul MD-CA

Sistemele de calcul, terminalele operatorilor şi resursele informaţionale ale MD-CA sunt dispuse într-o zonă dedicată, protejată fizic împotriva accesului neautorizat, distrugerilor sau perturbării activităţii. Aceste locaţii sunt monitorizate. Fiecare intrare şi ieşire este înregistrată în jurnalul de evenimente (log-urile sistemului); stabilitatea sursei de electricitate precum şi temperatura sunt de asemenea monitorizate şi controlate.

Amplasarea locaţiei

MD-CA este localizată în Bucureşti, la următoarea adresă:

S.C. CERTSIGN S.A.

Bulevardul Tudor Vladimirescu, nr. 29 A, AFI Tech Park 1,

Sector 5, Bucureşti, România, CP 050881

Accesul fizic

Accesul fizic în cadrul MD-CA este controlat şi monitorizat de un sistem de alarmă integrat. MD-CA dispune de sisteme de prevenire a incendiilor, sisteme de detectare a intruşilor şi sisteme de alimentare cu energie electrică în caz de urgenţă.

Accesul in sediul MD-CA este permis numai persoanelor autorizate de către conducerea MD-CA. Vizitatorii locaţiilor aparţinând MD-CA trebuie să fie însoţiţi permanent de persoane autorizate.

Zonele ocupate de MD-CA se împart în:

- zona serverelor,
- zona operatorilor CA
- zona administratorilor,
- zona de dezvoltare şi testare.

Zona serverelor este echipată cu un sistem de securitate monitorizat continuu, alcătuit din senzori de mişcare, efracţie şi incendiu. Accesul în această zonă este permis numai personalului autorizat, de exemplu, administratorul de securitate, administratorul MD-CA şi administratorul de sistem. Monitorizarea drepturilor de acces se face folosind carduri şi cititoare, montate lângă punctul de acces. Fiecare intrare şi ieşire din zonă este înregistrată automat în jurnalul de evenimente.

Controlul accesului în *zona operatorilor şi administratorilor* se face prin intermediul cârdurilor şi a cititoarelor de carduri. Deoarece toate informaţiile senzitive sunt protejate prin folosirea unor seifuri, iar accesul la terminalele operatorilor şi administratorilor necesită în prealabil autorizarea acestora, securitatea fizică în această zonă este considerată ca fiind adecvată. Cheile de acces pot fi ridicate numai de personalul autorizat. În această zonă au acces numai angajaţii MD-CA şi persoanele autorizate.

Zona de dezvoltare şi testare este protejată într-o manieră similară cu zona operatorilor şi administratorilor. În această zonă este permisă şi prezenţa persoanelor neînsoţite. Programatorii şi dezvoltatorii nu au acces la informaţii senzitive. Dacă este necesar un astfel de acces, atunci el se poate face numai în prezenţa administratorului de securitate. Proiectele în curs de implementare şi software-ul aferent este testat în mediul de testare al MD-CA.

Sursa de alimentare cu electricitate şi aerul condiţionat

Zona operatorilor şi administratorilor, precum şi zona de dezvoltare şi testare sunt prevăzute cu aer condiţionat. Din momentul întreruperii alimentării cu energie, sursele de electricitate de urgenţă (UPS) permit continuarea neperturbată a activităţii până la intervenţia automată a grupului electrogen al clădirii.

Expunerea la apă

Riscul de inundaţie în zona serverelor este foarte mic, deoarece distanţa faţă de conductele de apă este mare. Locaţia MD-CA dispune de sistem de prevenire a inundaţiilor, fiind utilizaţi senzori amplasati la nivelul podelelor în conformitate cu standardele şi reglementările în domeniu.

Prevenirea incendiilor

Locaţia MD-CA dispune de sistem de prevenire şi protecţie împotriva incendiilor în conformitate cu standardele şi reglementările în domeniu.

Depozitarea mediilor de stocare a informaţiilor

În funcţie de sensibilitatea informaţiilor, mediile electronice care conţin arhivele şi copiile de siguranţă ale datelor curente sunt stocate în seifuri metalice, localizate într-o camera cu grad ridicat de securitate. Accesul la camera şi seifuri este permis numai persoanelor autorizate.

Aruncarea deşeurilor

Hârtiile şi mediile electronice care conţin informaţii importante din punct de vedere al securităţii MD-CA sunt distruse după expirarea perioadei de păstrare. Modulele de securitate hardware sunt resetate şi şterse

conform recomandărilor producătorului. Aceste dispozitive sunt, de asemenea, resetate şi şterse atunci când sunt trimise în service sau reparate.

Depozitarea backup-urilor în afara locaţiei

Copiile parolelor, codurile PIN şi cardurile criptografice sunt stocate în containere speciale, situate în afara locaţiei MD-CA.

Stocarea în afara locaţiei se aplică şi în cazul arhivelor, copiilor curente ale informaţiilor procesate de sistem şi kit-urilor de instalare ale aplicaţiilor MD-CA. Acest lucru permite refacerea de urgenţă a oricărei funcţii a MD-CA în 24 de ore, în locaţia principală a MD-CA, sau în locaţia auxiliară.

6.2 Controlul securităţii organizaţiei

Acest capitol prezintă rolurile ce pot fi atribuite personalului aparţinând MD-CA. De asemenea, tot în acest capitol sunt descrise responsabilităţile şi sarcinile specifice fiecărui rol.

6.2.1 Roluri de încredere

Roluri de încredere în MD-CA

În MD-CA sunt definite următoarele roluri de încredere, care pot fi atribuite uneia sau mai multor persoane:

- **Responsabil MD-CA**
  - responsabil pentru operarea in siguranţa si in parametrii ai MD-CA ca organizaţie.
  - este un reprezentant al organizaţiei şi este autorizat să dea instrucţiuni în cadrul organizaţiei MD-CA.
  - direct implicat în punerea în aplicare a proceselor de afaceri, dar este responsabil pentru respectarea şi evaluarea măsurilor de securitate, împreună cu conducerea MD-CA.
  - Îşi asuma responsabilitatea pentru Managementul schimbării.
- **Administrator de securitate** – Responsabilitate globală pentru implementarea politicilor şi procedurilor de securitate. În plus poate aproba/revoca/suspenda certificate.
  - Iniţiază instalarea, configurarea şi managementul aplicaţiilor software şi hardware (inclusiv resursele de reţea) ale MD-CA; iniţiază şi suspendă serviciile oferite de MD-CA; coordonează administratorii, iniţiază şi supraveghează generarea de chei şi secrete partajate; atribuie drepturi din punct de vedere al securităţii şi privilegiilor de acces ale utilizatorilor; atribuie parole pentru conturile utilizatorilor noi; verifică jurnalele de evenimente; supervizează auditurile interne şi externe; primeşte şi răspunde la rapoartele de audit; supervizează eliminarea deficienţelor constatate în urma auditului.
  - Supraveghează operatorii Autorităţii de Certificare; configurează sistemele şi reţeaua, activează şi configurează mecanismele de protecţie a reţelei; creează conturile pentru utilizatorii MD-CA; verifică log-urile de sistem; verifică respectarea Politicii de certificare şi a

Codului de Practici şi Proceduri; generează secrete partajate şi chei;creează copiile de siguranţă de urgenţă; modifică numele şi adresele serverelor.

- **Administratorul de sistem** – Autorizat să instaleze, configureze şi să întreţină sistemele de încredere ale Autorităţii de Certificare pentru înregistrarea, generarea de certificate, iniţializarea dispozitivelor. Instalează dispozitivele hardware şi sistemele de operare; instalează şi configurează echipamentele de reţea.
- **Ofiţer de Securitate CA (CAO)** – Responsabil de operarea zilnică a sistemelor de încredere ale Autorităţii de Certificare.
- **Administrator CA (CAA)**- Autorizat să execute operaţiile de backup şi restaurare a sistemului. Are acces la certificatele Abonaţilor; asigură continuitatea copiilor de siguranţă şi arhivelor bazelor de date şi a creării log-urilor de sistem; administrează bazele de date; are acces la informaţii confidenţiale despre Abonaţi, dar nu poate accesa fizic nici o altă resursă a sistemului; transferă copiile de siguranţă ale arhivei şi ale datelor curente în afara locaţiei MD-CA.
- **HSM Operator (HSMO)** – ia parte la procesul de semnare a certificatelor MSCA.
- **HSM Administrator (HMA)**
  - Execuţia în condiţii de siguranţă a proceselor de gestionare a cheilor,
  - Generarea certificatelor, administrarea şi ştergerea de chei asimetrice ale MD-CA.

Funcţia HSMA poate fi pusă în aplicare numai pe baza principiului 'four-eyes-principle'.

- **Auditorul de sistem** – autorizat să acceseze arhivele şi log-urile de audit ale sistemelor de încredere ale MD-CA. Responsabil de efectuarea de audituri interne pentru respectarea Codului de Practici şi Proceduri de către MD-CA; această responsabilitate se extinde şi asupra fiecărei Autorităţi de Înregistrare care operează în cadrul MD-CA.

*În cadrul MD-CA, rolul de **auditor** nu poate fi combinat cu nici un alt rol. O entitate care are un rol diferit de cel de auditor nu poate prelua responsabilităţile auditorului.*

6.2.2 Numărul de persoane necesare pentru îndeplinirea unei sarcini

Procesul de generare de chei – pentru semnarea certificatelor sau pentru transportul Km_{wc}– este una din operaţiile ce necesită o atenţie deosebită. Generarea necesită prezenţa a cel puţin trei persoane: un administrator de securitate, un administrator de HSM si un Operator CA.

Prezenţa Operatorului Autorităţii de Certificare şi a unui număr corespunzător de operatori HSM este necesară şi la încărcarea cheii criptografice a Autorităţii de Certificare în modulul hardware de securitate. Orice altă operaţiune sau rol, descris în cadrul CPP poate fi efectuată de o singură persoană, special desemnată în acest sens.

6.2.3 Identificarea şi autentificarea pentru fiecare rol

Personalul MD-CA este supus identificării şi autentificării în următoarele situaţii:

- plasarea pe lista de persoane care au dreptul de a accesa locaţiile MD-CA ,
- plasarea pe lista de persoane care au acces fizic la sisteme şi resurse de reţea aparţinând MD-CA,
- emiterea confirmării care autorizează îndeplinirea rolului asignat,
- asignarea unui cont şi a unei parole în sistemul informatic al MD-CA,

Fiecare cont asignat:

- trebuie să fie unic şi asignat direct unei anumite persoane,
- nu poate fi folosit în comun cu nici o altă persoană,
- trebuie restricţionat conform funcţiei (ce relese din rolul îndeplinit de persoana respectivă) pe baza software-ului de sistem al MD-CA, a sistemului de operare şi a controalelor de aplicaţii.

Operaţiile efectuate în MD-CA care necesită acces la resurse de reţea comune sunt protejate prin mecanisme de autentificare sigură şi de criptare a informaţiilor transmise.

6.3 Controlul personalului

MD-CA trebuie să se asigure că persoana care îndeplineşte responsabilităţile funcţiei, conform cu rolul atribuit în cadrul MD-CA:

- a absolvit cel puţin liceul,
- este cetăţean român,
- a semnat un contract care descrie rolul şi responsabilităţile sale în cadrul sistemului,
- a beneficiat de un stagiu de pregătire avansată în conformitate cu obligaţiile şi sarcinile asociate funcţiei sale,
- a fost instruit cu privire la protecţia datelor personale şi informaţiilor confidenţiale sau private,
- a semnat un contract ce conţine clauze referitoare la protejarea informaţiilor senzitive (din punctul de vedere al securităţii MD-CA) şi a datelor confidenţiale şi private ale Abonaţilor,
- nu îndeplineşte sarcini care pot genera conflicte de interese între Autoritatea de Certificare MD-CA şi Autoritatea de Înregistrare MD-CIA, care acţionează în numele acesteia.

6.3.1 Experienţa personală, calificările şi clauzele de confidenţialitate necesare

Personalul angajat al MD-CA care îndeplineşte un rol de încredere, trebuie să obţină avizul responsabilului de securitate. Avizul nu este necesar în cazul persoanelor care nu exercită un rol de încredere.

Îndeplinirea unei funcţii de încredere ca administrator de securitate, administrator al Autorităţii de Certificare şi administrator HSM permite accesul la informaţiile clasificate. Dezvăluirea neautorizată a acestor informaţii poate cauza pierderea sau compromiterea intereselor, apărate de lege, ale unei persoane fizice sau ale unei organizaţii.

Procedurile de acces la informaţiile nepublice şi de verificare a încrederii în personal sunt în conformitate cu Legea Protecţiei Datelor cu Caracter Personal.

6.3.2 Cerinţele de pregătire a personalului

Personalul care îndeplineşte roluri şi sarcini ca urmare a angajării la MD-CA, trebuie să fie instruit cu privire la:

- reglementările Codului de Practici şi Proceduri,
- reglementările Politicii MSA,
- procedurile şi controalele de securitate folosite de Autoritatea de Certificare,
- aplicaţiile software ale Autorităţii de Certificare,
- responsabilităţile ce decurg din rolurile şi sarcinile executate în sistem,
- procedurile ce trebuie executate ca urmare a apariţiei unei defecţiuni în funcţionarea sistemului Autorităţii de Certificare.

După încheierea pregătirii, participanţii semnează un document prin care confirmă familiarizarea lor cu Codul de Practici şi Proceduri, Politica MSA şi acceptă restricţiile şi obligaţiile impuse.

6.3.3 Frecvenţa stagiilor de pregătire

Pregătirea descrisă în paragraful 6.3.2 trebuie repetată de fiecare dată când apar modificări semnificative în MD-CA.

6.3.4 Rotaţia funcţiilor

Acest Cod de Practici şi Proceduri nu specifică nici un fel de cerinţe în această privinţă.

6.3.5 Sancţionarea acţiunilor neautorizate

În cazul descoperirii sau existenţei suspiciunii unui acces neautorizat, administratorul de sistem împreună cu administratorul de securitate poate suspenda accesul persoanei respective la sistemul MD-CA. Măsurile disciplinare pentru astfel de incidente trebuie descrise în regulamente corespunzătoare şi trebuie să fie conforme cu prevederile legale.

6.3.6 Personalul angajat pe baza de contract

Personalul angajat pe baza de contract (servicii externe, dezvoltatori de subsisteme sau aplicaţii etc.) fac obiectul unor verificări similare ca şi în cazul angajaţilor MD-CA . În plus, personalul angajat pe bază de contract, pe timpul cât îşi desfăşoară activitatea în locaţia MD-CA, trebuie permanent însoţit de către un angajat al MD-CA , cu excepţia celor care au primit avizare din partea administratorului de securitate şi care poate accesa informaţii clasificate intern sau în conformitate cu normele legale în vigoare.

6.3.7 Documentaţia oferită personalului

MD-CA trebuie să ofere personalului său accesul la următoarele documente:

- Politica MSA,
- Codul de Practici şi Proceduri,
- Responsabilităţile şi obligaţiile asociate rolului deţinut în sistem.
- Manuale ale aplicaţiilor.
- Proceduri operaţionale.

7 CONTROALE TEHNICE DE SECURITATE

Acest capitol descrie procedurile de generare şi management a perechii de chei criptografice a Autorităţii de Certificare şi Abonatului, inclusiv cerinţele tehnice asociate.

7.1 Generarea si Instalarea Perechii de Chei a MD-CA

7.1.1 Generarea perechii de chei a MD-CA

Procedurile de management a cheii se referă la păstrarea şi folosirea în siguranţă de către proprietar a cheilor sale. O atenţie deosebită se acordă generării şi protecţiei cheii private a MD-CA, care influenţează funcţionarea în siguranţă a întregului sistem de certificare a cheilor publice din cadrul MD-CA.

Autoritatea de Certificare **MD-CA** deţine mai multe certificate semnate de catre ERCA Cheia privată corespunzătoare cheii publice conţinută de aceste certificate este folosită exclusiv în scopul semnării certificatelor pentru cardurile tahograf si pentru generarea cererii criptografice a MSCA adresate ERCA.

Generarea perechii de chei MD-CA (MD.SK si MD.PK) este realizata intr-un server criptografic cu participarea activa a cel puţin trei persoane. Modulul HSM al serverului criptografic este conform cu cerinţele FIPS 140-2 Nivel 3. Cheia privata este menţinuta în permanenţă criptata pe dispozitivul HSM.

Acţiunile întreprinse în momentul generării perechii de chei sunt înregistrate, datate şi semnate de fiecare persoană prezentă în timpul generării. Înregistrările sunt păstrate din motive de audit sau pentru verificările obişnuite ale sistemului.

7.1.2 Distribuirea cheii private catre entităţi

MD-CA nu genereaza cheile private RSA pentru carduri. Acestea sunt generate la MD-CP.

7.1.3 Trimiterea cheii publice catre emiţătorul certificatului (ERCA)

Conform politicii ERCA.

7.1.4 Distribuirea cheilor publice ale MD-CA si ERCA catre entităţile partenere

Cheia publica a MD-CA este distribuita catre MD-CP sub forma de certificat semnat cu cheia privata a ERCA. Cheia publica a ERCA este distribuita catre MD-CP ca atare. Distribuirea lor se face împreuna cu certificatul care va fi scris pe card ca urmare a unei cererii KCR primite de MD-CA de la MD-CP.

7.1.5 Mărimile cheilor

Cheile RSA au lungimea modulului de 1024 de biţi, iar lungimea exponentului cheii public de 64-biti.

7.1.6 Parametrii de generare ai cheilor publice

Cel care generează o cheie este responsabil de verificarea calităţii parametrilor cheii generate. Acesta trebuie să verifice:

- posibilitatea de a efectua operaţii de criptare şi decriptare, inclusiv creare de semnături electronice şi verificare a acestora,

- procesul de generare a cheii trebuie să se bazeze pe generatoare puternice de numere aleatoare – surse fizice de zgomot alb, dacă este posibil,
- imunitatea la atacuri cunoscute (în cazul algoritmilor RSA şi DSA).

7.1.7 Verificarea calităţii parametrilor

Se folosesc module HSM certificate, configurate pentru a genera chei RSA cu modulul de 1024-biti.

7.1.8 Generarea Hardware/software a cheii

Cheile MD-CA sunt generate in module HSM certificate.

7.1.9 Utilizarea perechii de chei a MD-CA

Cheia privata RSA a MD-CA este utilizata doar pentru semnarea certificatelor cheilor publice pentru tahografe si pentru crearea cererii de certificat a MSCA catre ERCA.

7.2 Protecţia Cheii Private

7.2.1 Standarde si controale pentru modulele criptografice

MD-CA utilizează pentru generarea si stocarea cheilor sale private RSA si a cheilor Km_{wc} doar module HSM certificate.

Operarea modulului HSM este verificata periodic prin teste interne, iar upgrade-ul de firmware pentru HSM este realizat anual de administratorul HSM, daca este cazul.

7.2.2 Controlul k din n al cheii private

Generarea si backup-ul cheii private sunt realizate de cel puţin trei persoane autorizate.

Operaţiile de certificare a cheii publice si de distribuire a cheii master a senzorului de miscare necesita participarea unui operator HSM si a unui operator CA.

7.2.3 Escrow-ul cheii private

Escrow-ul cheii este interzis de politica de certificare a MD-CA.

7.2.4 Backup-ul cheii private

MD-CA creează o copie de siguranţă a cheilor sale private. Copiile sunt folosite în cazul punerii în aplicare a procedurilor standard, sau de urgenţă (de exemplu, după dezastru) de recuperare a cheii. Copiile cheilor private sunt protejate prin secrete partajate. Ele sunt criptate si stocate in cardurile modulului HSM.

Copiile cheilor sunt verificate o data pe an prin încercarea de restaurare a lor intr-un HSM identic din centrul de recuperare in caz de dezastru. Verificarea se face intr-o incinta cu acelaşi grad de siguranţa ca si mediul de producţie in prezenta unui administrator de sistem, a doi administratori de HSM si a unui auditor.

Daca verificarea nu reuşeşte, noi copii sunt create in cel mai scurt timp.

7.2.5 Arhivarea cheii private

Ca la 7.2.4

7.2.6 Transferul cheii private din sau intr-un modul HSM

7.2.7 Păstrarea cheii private intr-un modul HSM

Cheile private ale MD-CA sunt păstrate in modulul HSM in care au fost generate. Cheile pot fi importate in modulul HSM găzduit de sistemul din centrul de recuperare in caz de dezastru doar in mod securizat, respectând procedura de restaurare a sistemului si in prezenta unui administrator de sistem, a doi administratori de HSM si a unui auditor.

7.2.8 Metoda de activare a cheii private

Activarea cheii se face după principiul K din N, cu K>=2. La operaţie participa doi operatori HSM.

7.2.9 Metoda dezactivării cheii private

Metoda de dezactivare a cheii private se referă la dezactivarea cheii după folosirea acesteia sau ca urmare a terminării unei sesiuni în timpul căreia a fost folosită cheia.

În cazul MD-CA, dezactivarea unei chei private se face de către ofiţerul de securitate numai în cazul în care o sesiune de lucru a fost încheiată, perioada de validitate a cheii a expirat, cheia a fost revocată sau este necesar să se suspende imediat activităţile sistemului. Dezactivarea unei chei private se face conform procedurii de inactivare a unei CA si a ştergerii securizate a cheilor acesteia. Acţiunile întreprinse în acest proces sunt înregistrate, datate şi semnate de fiecare persoană prezentă în timpul inactivări si ştergerii securizate. Înregistrările sunt păstrate din motive de audit sau pentru verificările obişnuite ale sistemului.

7.2.10 Metoda distrugerii cheii private

Ştergerea cheii private se face respectând procedura de ştergere securizata a cheilor de pe modulul HSM, conform metodelor recomandate de producătorul dispozitivului.

Fiecare distrugere de cheie privată este înregistrată în jurnalul de evenimente.

7.2.11 Certificarea modulului HSM

MD-CA foloseşte module criptografice certificate FIPS 140-2 Level 3.

7.3 Alte Aspecte ale Managementului Perechii de Chei

7.3.1 Arhivarea Cheii Publice

7.3.2 Perioadele de validitate pentru cheile publice si private ale MD-CA

Perioada de validitate a cheii private MD-CA este stabilita la 2 ani prin Politica de Certificare a MD-CA.

Perioada de validitate a cheii publice MD-CA este de 7 ani, iar a cheilor master ale senzorului de miscare este nelimitata.

7.4 Datele de Activare

Metodele de activare a cheii private se referă la activarea cheii înainte de orice folosire a sa, sau de începerea unei sesiunii de lucru ce necesită folosirea cheii respective. O cheie odată activată poate fi folosită până la dezactivare.

Executarea procedurilor de activare (şi dezactivare) a unei chei private depinde de intervalul de timp în care cheia trebuie să rămână activă (pe timpul unei singure operaţiuni, sesiuni sau pentru o perioadă nelimitată).

Cheia privata a MD-CA rămâne în stare activă până la ştergerea ei fizică de pe modul sau până la scoaterea ei din serviciile MD-CA. Activarea cheii private este întotdeauna precedată de autentificarea operatorilor. Autentificarea este realizată pe baza cardurilor criptografice deţinute de operatori. După introducerea cardurilor în modulul criptografic şi folosirea codurilor PIN, cheia privată rămâne în stare activă până dezactivarea acesteia.

7.5 *Controale de Securitate a Calculatoarelor*

Sarcinile operatorilor si administratorilor care lucrează în cadrul MD-CA sunt realizate prin intermediul unor dispozitive hardware şi aplicaţii software de încredere.

7.5.1 Cerinţele tehnice specifice securităţii calculatoarelor

Cerinţele tehnice prezentate în acest capitol se referă la controalele de securitate specifice calculatoarelor şi aplicaţiilor, folosite în cadrul MD-CA. Măsurile de securitate care protejează sistemele de calcul sunt aplicate la nivelul sistemului de operare, al aplicaţiilor precum şi din punct de vedere fizic.

Calculatoarele aparţinând MD-CA dispun de următoarele mijloace de securitate:

- autentificarea obligatorie la nivelul sistemului de operare şi al aplicaţiilor,
- control discreţionar al accesului,
- posibilitatea de a fi auditate din punct de vedere al securităţii,
- calculatorul este accesibil doar personalului autorizat, cu roluri de încredere în MD-CA,
- separarea sarcinilor, conform rolului în cadrul sistemului,
- identificarea şi autentificarea rolurilor şi a personalului care îndeplineşte aceste roluri,
- prevenirea refolosirii unui obiect de către un alt proces după eliberarea acestuia de către procesul autorizat,
- protecţia criptografică a schimburilor de informaţii şi protecţia bazelor de date,
- arhivarea istoricului operaţiunilor executate pe un calculator şi a datelor necesare auditării,
- o cale sigură ce permite identificarea şi autentificarea rolurilor şi a personalului care îndeplineşte aceste roluri,
- metode de restaurare a cheilor (numai în cazul modulelor hardware de securitate), a aplicaţilor şi a sistemului de operare,
- mijloace de monitorizare şi alertare în cazul accesului neautorizat la resursele de calcul.

7.5.2 Evaluarea securităţii calculatoarelor

Sistemele de calcul ale MD-CA respectă cerinţele descrise în standardul CEN CWA 14167 (Cerinţele de Securitate pentru Sistemele de Încredere care asigură Managementul Certificatelor).

7.5.3 Controale tehnice specifice ciclului de viaţa

Controale specifice dezvoltării sistemului

Fiecare aplicaţie, înainte de a fi folosita în producţie de catre MD-CA, este instalata astfel încât să se permită controlul versiunii curente şi să se prevină instalarea neautorizată de programe sau falsificarea celor existente.

Reguli similare se aplică în cazul înlocuirii componentelor hardware, cum ar fi:

- dispozitivele fizice sunt furnizate în aşa fel încât să poată fi urmărita şi evaluată ruta fiecărula, până la locul său de instalare,
- livrarea unui dispozitiv fizic pentru înlocuire se realizează într-un mod similar celui de livrare al dispozitivului original; înlocuirea se realizează de către personal calificat şi de încredere.

Controale pentru managementul securităţii

Scopul controalelor pentru managementului securităţii este acela de a superviza funcţionalitatea sistemelor MD-CA, garantând astfel că acestea operează corect şi în concordanţă cu configurarea acceptată şi implementată.

Configuraţia curentă a sistemelor MD-CA, precum şi orice modificare şi actualizare a acestora, este înregistrată şi controlată.

Controalele aplicate sistemelor MD-CA permit verificarea continuă a integrităţii aplicaţiilor, versiunii şi autentificarea şi verificarea originii dispozitivelor hardware.

7.5.4 Controale de securitatea a reţelei

Serverele şi staţiile de lucru de încredere aparţinând MD-CA sunt conectate prin intermediul unei reţele locale (LAN), divizate în mai multe subretele, cu acces controlat. Accesul dinspre alte reţele este protejat prin intermediul unui firewall inteligent.

Controalele de securitate sunt dezvoltate pe baza firewall-ului şi a filtrelor de trafic aplicate la nivelul ruterelor.

Mijloacele de asigurare a securităţii reţelei acceptă doar mesajele transmise prin protocoale securizate. Evenimentele (log-urile) sunt înregistrate în jurnalele de sistem şi permit supravegherea folosirii corecte a serviciilor furnizate de MD-CA.

7.5.5 Controale specifice modulelor criptografice

Controalele modulelor criptografice includ cerinţele impuse pentru dezvoltarea, producţia şi livrarea modulelor. MD-CA nu defineşte cerinţe specifice în acest domeniu. Totuşi, MD-CA acceptă şi utilizează numai module criptografice care corespund cerinţelor din Capitolul 6 din Politica de Certificare a MD-CA.

7.5.6 Înregistrarea evenimentelor şi procedurile de auditare

Pentru a gestiona eficient sistemele MD-CA şi pentru a putea audita acţiunile utilizatorilor şi personalului MD-CA, toate evenimentele care apar în sistem sunt înregistrate. Informaţiile înregistrate alcătuiesc jurnalele (log-urile) de evenimente şi trebuie păstrate în aşa fel încât să permită, daca este cazul, să se acceseze informaţiile corespunzătoare şi necesare rezolvării disputelor, sau să detecteze tentativele de compromitere a securităţii MD-CA. Evenimentele înregistrate fac obiectul procedurilor de arhivare. Arhivele sunt păstrate în afara incintei MD-CA.

Când este posibil, log-urile sunt create automat. Dacă înregistrările nu pot fi create automat, se vor folosi jurnalele de evenimente pe hârtie. Fiecare înregistrarea în log, electronic sau de mână, este păstrata şi dezvăluita atunci când se desfăşoară un audit.

Tipuri de evenimente înregistrate

Fiecare activitate critică din punctul de vedere al securităţii MD-CA este înregistrată în log-urile de evenimente şi arhivată. Arhivele sunt depozitate pe medii de stocare ce nu pot fi suprascrise pentru a preveni modificarea sau falsificarea lor.

Log-urile de evenimente MD-CA conţin înregistrări ale tuturor activităţilor generate de componentele software din cadrul sistemului. Aceste înregistrări sunt împărţite în trei categorii separate:

- **înregistrări de sistem** – conţin informaţii despre cererile clienţilor software şi răspunsurile server-ului (sau invers) la nivelul protocolului de reţea (de exemplu https); datele concrete care se înregistrează sunt: adresa IP a staţiei sau a server-ului, operaţiunile executate (de exemplu: căutare, editare, scriere etc.) şi rezultatele lor (de exemplu introducerea cu succes a unei înregistrări în baza de date),
- **erori** – conţine informaţii despre erori la nivelul protocoalelor de reţea şi la nivelul modulelor aplicaţiilor;
- **audit** – conţin informaţii specifice serviciilor de certificare, de exemplu: cererea de certificat, emiterea de certificat etc.

Jurnalele de evenimente de mai sus sunt comune fiecărei componente instalate pe un server sau staţie de lucru şi au o capacitate prestabilită. Atunci când se depăşeşte această capacitate, este creată automat o nouă versiune de jurnal. Jurnalul anterior este arhivat şi şters de pe disc.

Fiecare înregistrare, automată sau manuală, conţine următoarele informaţii:

- tipul evenimentului,

- identificatorul evenimentului,
- data şi ora apariţiei evenimentului,
- identificatorul persoanei responsabile de eveniment.

Conţinutul înregistrărilor se refera la:

- alertele firewall-urilor şi IDS-urilor,
- operaţiile asociate înregistrării, certificării etc.,
- modificări ale structurii hard sau soft,
- modificări ale reţelei şi conexiunilor,
- înregistrările fizice în zonele securizate şi violările de securitate,
- schimbările de parole, drepturi asupra codurilor PIN, rolurile personalului,
- accesul reuşit şi nereuşit la baza de date MD-CA şi la aplicaţiile serverului,
- generarea de chei pentru CA, etc.,
- fiecare cerere primită şi decizia emisă în format electronic,
- istoria creării copiilor de backup şi a arhivelor cu înregistrări.

Accesul al jurnalele de evenimente (log-uri) este permis în exclusivitate administratorului de securitate, operatorilor Autorităţilor de Certificare şi auditorilor.

Frecvența analizei jurnalelor de evenimente

Înregistrările din jurnalul de evenimente trebuie revăzute în detaliu cel puțin o dată pe lună. Orice eveniment având o importanță semnificativă trebuie explicat și descris într-un jurnal. Procesul de verificare a jurnalului include verificarea unor eventuale falsificări, sau modificări și verificarea fiecărei alerte sau anomalii consemnată în log-uri. Orice acțiune executată ca rezultat al funcționări defectuoase detectate trebuie înregistrată în jurnal.

Perioada de retenție a jurnalelor de evenimente

Înregistrările evenimentelor sunt stocate în fișiere pe discul sistem până când acestea ajung la capacitatea maximă permisă.

Protecția jurnalelor de evenimente

Fiecare înregistrare din jurnale face obiectul arhivării pe un server de log centralizat. După depășirea numărului acceptat de înregistrări pentru un jurnal, conținutul acestuia este arhivat. Arhivele pot fi semnate criptate. O cheie folosită pentru criptarea arhivelor este plasată sub controlul administratorului de securitate.

Un jurnal de evenimente poate fi revăzut numai de administratorului de securitate, administratorul Autorității de Certificare, sau de către un auditor. Accesul la jurnalul de evenimente este configurat în așa fel încât:

- numai entitățile de mai sus au dreptul să citească înregistrările jurnalului,
- numai administratorul de securitate poate arhiva sau șterge fișiere (după arhivarea acestora) care conțin evenimentele înregistrate,
- este posibilă detectarea oricărei violări de integritate; acest lucru asigură faptul că înregistrările nu conțin goluri sau falsuri,
- nici o entitate nu are dreptul să modifice conținutul unui jurnal.

În plus, procedurile de protecție a jurnalului sunt implementate în așa fel încât, chiar și după arhivarea jurnalului, este imposibil să ștergi înregistrări, sau să ștergi jurnalul înaintea expirării perioadei de retenție a jurnalului.

Procedurile de backup pentru jurnalele de evenimente

Procedurile de securitate MD-CA solicita ca jurnalul de evenimente să facă obiectul backup-ului lunar. Aceste backup-uri sunt stocate în locații auxiliare ale MD-CA.

Notificarea entităţilor responsabile de tratarea evenimentelor

Modulul de analiză a jurnalului de evenimente implementat în sistem examinează evenimentele curente şi sesizează automat activităţile suspecte sau pe cele care au ca scop compromiterea securităţii. În cazul activităţilor care au influenţă asupra securităţii sistemului, sunt notificaţi automat administratorul de securitate şi administratorul Autorităţii de Certificare. În celelalte cazuri, notificarea este direcţionată numai către administratorul de sistem. Transmiterea informaţiilor către persoanele autorizate despre situaţiile critice – din punctul de vedere al securităţii sistemului – se face prin alte mijloace de comunicare, protejate corespunzător, de exemplu: telefon mobil, poştă electronică. Entităţile notificate iau măsurile corespunzătoare pentru a proteja sistemul faţă de ameninţarea detectată.

Procedura de backup si restaurare

Copiile de siguranţă permit restaurarea completă (dacă este necesar, de exemplu, după distrugerea sistemului) a datelor esenţiale pentru activitatea MD-CA. Pentru a realiza acest lucru, sunt copiate următoarele aplicaţii şi fişiere:

- discurile de instalare a aplicaţiilor sistem (de exemplu sistemul de operare),
- discurile de instalare a aplicaţiilor pentru Autoritatea de Certificare,
- istoricul cheilor si certificatelor,
- datele privind personalul MD-CA,
- jurnalele de evenimente.

Metoda de creare a copiilor de backup are o influenţă deosebită asupra timpului şi costului restaurării Autorităţii de Certificare după defectarea, sau distrugerea sistemului. MD-CA foloseşte atât backup-uri full (zilnice) toate copiile sunt clonate şi clonele sunt păstrate în altă locaţie secundara, în aceleaşi condiţii de securitate ca şi cele din locaţia primară.

Procedura de restaurare va fi verificata cel puţin o data la 6 luni, pentru a se verifica utilitatea backup-ului, in caz de dezastru. Va trebui sa se verifice daca datele salvate sunt suficiente pentru restaurarea sistemului in cel mai scurt timp posibil. Concluziile testelor vor fi înregistrate.

7.5.7 Arhivarea înregistrărilor

Este necesar ca toate datele şi fişierele referitoare la informaţiile despre securitatea sistemului, cererile de certificate, certificatele emise, cheile folosite de Autoritatea de Certificare să fie arhivate.

Pe baza arhivelor se creează copiile de siguranţă care sunt ţinute în afara locaţiei MD-CA.

Tipurile de date arhivate

Următoarele date sunt incluse în procesul de arhivare:

- informaţiile rezultate în urma examinării şi evaluării (ca urmare a unui audit) măsurilor de protecţie logica şi fizica ale Autorităţii de Certificare,
- cererile de certificate primite şi certificatele emise,

- baza de date cu certificate, (sau evenimente legate de emiterea de certificate)
- evenimente legate de distribuirea cheii Km_{wc}
- istoria cheii Autorității de Certificare, de la generare până la distrugere,

7.6 Compromiterea cheilor si Recuperarea in Caz de Dezastru

7.6.1 Procedurile de tratare a incidentelor de securitate si a cazurilor de compromitere a cheilor

Procedurile sunt descrise in manualul de tratare a incidentelor care este distribuit doar administratorilor si auditorilor.

La detectarea unui incident, MD-CA poate fi trecut in carantina si operațiile sale suspendate pana la stabilirea gradului de compromitere.

7.6.2 Defecțiuni ale echipamentelor, software-ului sau pierderea integrității datelor

In funcție de natura dezastrului, pașii de recuperare sunt următorii:

1. Se înlocuiește imediata CA-ul cu sistemele de rezerva
2. Se restaurează aplicațiile software folosind mediile de instalare
3. Se restaurează datele folosind copiile de siguranța
4. Se restaurează cheile RSA folosind HSM-ul de rezerva si cardurile de HSM de rezerva

7.6.3 Procedurile in cazul compromiterii cheii private

In cazul in care cheia privata a MD-CA sau cheia senzorului de miscare au fost compromise, sau se suspectează ca au fost compromise, se notifica imediat MD-MSA si ERCA.

7.6.4 Continuarea afacerii in caz de dezastru

Folosind copiile de siguranța se restaurează datele si aplicațiile si se recreează un mediu de lucru securizat intr-o locație alternativa.

7.7 Scoaterea din uz a MD-CA

Încheierea serviciului MD-CA service se realizează astfel:

1. Toate datele sunt distruse in mod securizat prin ștergerea securizata a discurilor folosind programe specializate si prin ștergerea securizata a datelor modulului HSM;
2. Toate copiile cheilor MD-CA sunt distruse.
3. Arhiva MD-CA si înregistrările auditurilor sunt predate catre MD-MSA.

Procedura de scoatere din uz se desfasoara sub controlul dual al MD-CA si al MD-MSA.

8 AUDITURILE PENTRU STABILIREA CONFORMITATII SI ALTE EVALUARI

Auditurile au ca obiectiv verificarea consistenței acțiunilor MD-CA sau a entităților delegate de aceasta cu declarațiile și procedurile acestora (inclusiv Politica de certificare și Codul de Practici și Proceduri).

Auditurile desfășurate la MD-CA urmăresc în principal centrele de procesare a datelor și procedurile de gestiune a cheilor. De asemenea, aceste audituri au în vedere și Autoritatea de Certificare MD-CA.

Auditurile desfășurate la MD-CA pot fi efectuate de echipe interne (audit intern) sau de MD-MSA sau organizații independente (audit extern) angajate de aceasta. În toate aceste cazuri, auditul se desfășoară sub supravegherea administratorului de securitate.

Frecvența auditării

Auditul extern prin care se verifică compatibilitatea cu reglementările legale și procedurale (în special cu Politica de certificare și Codul de Practici și Proceduri) se desfășoară anual, în timp ce un audit intern este efectuat ori de cate ori administratorul de securitate considera necesar.

9.1 Identitatea / calificările auditorului

Auditul extern trebuie realizat de personal având cunoștințe și experiență tehnică corespunzătoare (să dispună de documente care să certifice acest lucru) în domeniul infrastructurilor de chei publice, tehnologiilor și dispozitivelor de securitate informatică și de auditare a securității sistemelor. De asemenea auditorul trebuie sa posede cunoștințe solide ale reglementarilor UE, CE si MD-MSA referitoare la sistemul tahografelor digitale.

Auditul intern este realizat de către departamentul de calitate și audit al MD-CA.

9.2 Relația auditorilor cu entitatea auditată

Vezi paragraful anterior. Auditorul nu trebuie sa depindă in nici un fel de entitatea auditata si nici sa nu fi fost in vreun fel implicat in activitățile de planificare si operare ale sistemelor ITC ale entității auditate.

9.3 Domeniile supuse auditării

Auditurile interne și externe se desfășoară conform regulilor și procedurilor acceptate pe plan internațional și vizează:

- securitatea fizică a MD-CA,
- procedurile de verificare a identității aplicantilor,
- serviciile de certificare și procedurile de furnizare a serviciilor,
- securitatea aplicațiilor software și a accesului la rețea,
- securitatea personalului MD-CA,
- jurnalele de evenimente și procedurile de monitorizare a sistemului,
- arhivarea și restaurarea datelor,
- procedurile de arhivare,

- înregistrările referitoare la modificarea parametrilor de configurare pentru MD-CA,
- înregistrările referitoare la analizele şi verificările efectuate pentru aplicaţiile software şi dispozitivele hardware.

9.4 Analiza vulnerabilităţilor

Autoritatea de Certificare face anual o analiză a vulnerabilităţilor pentru fiecare procedură internă, aplicaţie şi sistem informatic. Cerinţele de analiză pot, de asemenea, să fie stabilite de către o instituţie externă, autorizată să auditeze certSIGN. Administratorul de securitate are sarcina de a solicita audituri interne prin care să verifice conformitatea înregistrărilor din jurnalul de securitate, corectitudinea copiilor de backup, activităţile executate în cazul apariţiei unei ameninţări şi conformitatea cu Codul de Practici şi Proceduri. Instituţia externă care efectuează auditul de securitate, trebuie să desfăşoare această activitate respectând recomandările ISO/IEC 13335 (Guidelines for Management of IT Security) şi ISO/IEC 17799 (Code of Practice for Information Security Management).

9.5 Măsurile întreprinse ca urmare a descoperirii unei deficienţe

In cazul descoperirii unor deficiente se pot lua trei tipuri de masuri:

1. continuarea operaţiilor
2. continuarea limitata a operaţiilor;
3. suspendarea operaţiilor.

Auditorul, împreuna cu MD-MSA, decide ce acţiune trebuie întreprinsa. Decizia se bazează pe gravitatea deficientelor si a posibilului impact.

In cazul in care se decide acţiunea de tipul 1, managementul MD-CA este răspunzător pentru implementarea masurilor corective specificate in raportul de audit, in limitele de timp din acelaşi raport.

In cazul in care se decide acţiunea de tipul 2, MD-CA continua operaţiile in modul restrâns indicat in raportul de audit.

Nivelul de servicii poate include sau exclude oricare dintre următoarele activităţi:

- aprobarea si întreţinerea politicii MD-CA;
- operaţii de întreţinere a MD-CA;
- certificarea cheilor publice pentru cardurile de tahograf;
- operaţiuni de distribuţie a cheilor pentru senzorul de miscare.

In cazul in care se decide acţiunea de tipul 3, toate cardurile afectate trebuie trecute pe un backlist. Managementul MD-CA trebuie sa raporteze saptamânal stadiul masurilor de remediere catre auditor. MD-MSA si auditorul determina când trebuie făcuta o noua evaluare de securitate. Daca deficientele sunt considerate ca remediate după reevaluare, atunci MD-CA isi poate relua operaţiile.

9.6 *Comunicarea rezultatelor*

Rezultatele auditului anual sunt comunicate catre MD-MSA. In cazul acțiunilor de tipul 1 sau 2, MD-MSA se asigura de faptul ca toate entitățile care trebuie notificate primesc informațiile in conformitate cu prezentul document.

Kraftfahrt-Bundesamt

Kraftfahrt-Bundesamt · D-24932 Flensburg

Trüb AG
Herrn Peter Tiesnes
Hintere Bahnhofstrasse 12
5001 AARAU
SCHWEIZ

Ihr Zeichen: Peter Tiesnes
Ihre Nachricht vom: 13.09.2010
Bei Antwort bitte angeben: 423-131
Ansprechpartner: Dirk Hansen
Telefon: (04 61) 3 16-15 65
Telefax: (04 61) 3 16-17 40
E-Mail: kba-sgb423@kba.de

Datum: 02.12.2010

Funktionszertifikat für Karten des digitalen Kontrollgerätes gemäß dem Europäischen Übereinkommen über die Arbeit des im internationalen Straßenverkehr beschäftigten Fahrpersonals (AETR), Anhang IB, Anlage 9

Anlagen: Funktionszertifikat

Sehr geehrte Damen und Herren,

auf der Grundlage des hier vorliegenden Prüfberichtes des Landesbetriebes Mess- und Eichwesen Nordrhein-Westfalen wird der Trüb AG das Funktionszertifikat für die Kontrollgerätkarten, Typ TCOS Tachograph-AETR, erteilt.

Mit freundlichen Grüßen

Kraftfahrt-Bundesamt

Kraftfahrt-Bundesamt

D-24932 Flensburg

Funktionszertifikat
Functional Certificate

gemäß dem Europäischen Übereinkommen über die Arbeit des im internationalen Straßenverkehr beschäftigten Fahrpersonals (AETR)
(Dokument: ECE/TRANS/SC.1/2006/2 vom 9. August 2006 und ECE/TRANS/SC.1/2006/2/Add.1 vom 28. Februar 2008)

in respect of the European Agreement Concerning the Work of Crews of Vehicles Engaged in International Road Transport (AETR)
(Document: ECE/TRANS/SC.1/2006/2 of 9 August 2006 and ECE/TRANS/SC.1/2006/2/Add.1 of 28 February 2008)

Mitteilung über die gemäß Anhang IB durchgeführten Funktionsprüfungen an Kontrollgerätkarten - Fahrerkarte - Werkstattkarte - Unternehmenskarte - Kontrollkarte
Communication concerning the functional tests for the control device cards - driver card - workshop card - company card - inspector's card - carried out in accordance to annex IB

1. Hersteller- oder Handelsmarke:
   Manufacturing or commercial mark:
   Trüb AG

2. Modellbezeichnung:
   Name of model:
   TCOS Tachograph-AETR

   Version:
   Release:
   TCOS Tachograph Card Version 1.0

3. Name des Herstellers:
   Name of manufacturer:
   Trüb AG

4. Anschrift des Herstellers:
   Address of manufacturer:
   CH-5001 Aarau

S.C. CERTSIGN S.A.

5. Prüfstelle(n):
Test laboratory or laboratories:
Landesbetrieb Mess- und Eichwesen Nordrhein-Westfalen
DE-50829 Köln

6. Datum und Nummer des Prüfberichts:
Date and number of reports:
25.11.2010 61.17-XXVIII-6

7. Durchgeführte Funktionsprüfungen an Kontrollgerätkarten:
Performed control device cards functional tests:
1. Administrative Prüfung / Administrativ examination
1.1 Dokumentation / Documentation
2. Sichtprüfung / Visual inspection
2.1
3. Physische Prüfungen / Physical tests
3.1
4. Protokollprüfungen / Protocol tests
4.1 ATR
4.2 T=0
4.3 PTS
4.4 T=1
5. Kartenstruktur / Card structure
5.1
6. Funktionsprüfungen / Functional tests
6.1 Normale Verarbeitung / Normal processing
6.2 Fehlermeldungen / Error messages
7. Umweltprüfungen / Environmental tests
7.1

Erzielte Ergebnisse:
Obtained results:
Die geprüften Kontrollgerätkarten erfüllen hinsichtlich der ausgeführten Funktionen, der Messgenauigkeit und der Umwelteigenschaften die Anforderungen der Anlage IX.
The control device cards fulfil the requirements of the Sub-Appendix IX in terms of functions performed, measurement accuracy and environmental characteristics.

8. Bemerkungen:
Remarks:
Karten mit folgenden Unterscheidungszeichen:
cards with the following distinguishing signs:

Fahrerkarte **driver card**	**„UA", „MD"**
Werkstattkarte **workshop card**	**„UA", „MD"**
Unternehmenskarte **company card**	**„UA", „MD"**
Kontrollkarte **inspector's card**	**„UA", „MD"**

Fahrerkarte, Werkstattkarte, Unternehmenskarte und Kontrollkarte in der Moldawien-Ausführung (MD) kommen hinzu
driver card, workshop card, company card and inspector's card in Moldova-version (MD) are added

9. Ort:
Place: **DE-24944 Flensburg**

10. Datum:
Date: **02.12.2010**

11. Unterschrift: **Im Auftrag**

Signature:

Dirk Hansen

KRAFTFAHRT-BUNDESAMT 496

S.C. CERTSIGN S.A.

JRC
EUROPEAN COMMISSION

DTLab

14 December 2010

Council Regulation (EC) 1360/2002
Interoperability Certificate N°. JRC_DTC/AC-040/058/MA01/2010

Manufacturer :	Trueb AG Hintere Bahnhofstrasse 12 CH-5001 Aarau Switzerland

Specimen under Test	Digital Tachograph Cards– AETR - personalized for the Republic of Moldova.
Based on	TCOS Version 1.0 R2.0

Test Specification:	Interoperability Test Specification v2.0 (JRC S&T Reports: EUR 23061 EN - 2008) Interoperability of this set of tachograph cards has been demonstrated with all type of recording equipment (VU) and motion sensors (MS)in our possess.

Vehicle Unit	Security Certificate
Actia SMARTACH STDII v.6.08	DCSSI 2005/14 and M-2006/10
Continental Automotive GmbH - DTCO 1381 R1.3a	BSI-DSZ-ITSEC-0509-2008 MA-01
EFKON AG - EFAS-3 version 01.01	BSI-DSZ-CC-0474-2008
Stoneridge Electronics AB - SE5000 Revision 7.1	BSI-DSZ-ITSEC-0605-2009

Motion Sensors	
Actia IS2000 SMARTACH LXRY	Siemens VDO KITAS 2171

Certificate's validity until:	13 June 2011	(EC) 1360/2002 requirements 286[1] and 289[2]
Public web site:	http://dtc.jrc.ec.europa.eu	(EC) 1360/2002 requirement 290
Remarks :	Maintenance certificate based on JRC-DTC/AC-040/2007 (03/08/2007)	

Technical Responsible
D. Landat

Acting Head of TRVA Unit
M. Sironi

[1] Requirement [286]: The interoperability certificate is valid for six months. It is revoked at the end of this period if the manufacturer has not received a corresponding type approval certificate. It is forwarded by the manufacturer to the type approval authority of the Member State who has delivered the functional certificate.

[2] Requirement [289]:The type approval certificate shall be copied by the type approval authority to the laboratory in charge of the interoperability tests at the time of deliverance to the manufacturer.

Kraftfahrt-Bundesamt

DE-24932 Flensburg

BAUARTGENEHMIGUNG
APPROVAL CERTIFICATE

gemäß dem Europäischen Übereinkommen über die Arbeit des im internationalen Straßenverkehr beschäftigten Fahrpersonals (AETR)
(Dokument: ECE/TRANS/SC.1/2006/2 vom 9. August 2006 und ECE/TRANS/SC.1/2006/2/Add.1 vom 28. Februar 2008)

in respect of the European Agreement Concerning the Work of Crews of Vehicles Engaged in International Road Transport (AETR)
(Document: ECE/TRANS/SC.1/2006/2 of 9 August 2006 and ECE/TRANS/SC.1/2006/2/Add.1 of 28 February 2008)

BAUARTGENEHMIGUNGSBOGEN FÜR PRODUKTE, DIE DIE ANFORDERUNGEN VON ANHANG IB ERFÜLLEN
APPROVAL CERTIFICATE FOR PRODUCTS IN ACCORDANCE WITH APPENDIX IB

Kraftfahrt-Bundesamt / Federal Motor Transport Authority

Mitteilung betreffend:
Communication concerning:

- [x] die Bauartgenehmigung –
  Approval
- [ ] den Entzug der Bauartgenehmigung –
  Withdrawal of an approval
- [ ] für das Modell eines Kontrollgerätes –
  Of a control device model
- [ ] für die Kontrollgerätkomponente –
  Of a control device component
- [x] für eine Fahrerkarte –
  Of a driver card
- [x] für eine Werkstattkarte –
  Of a workshop card
- [x] für eine Unternehmenskarte –
  Of a company card
- [x] für eine Kontrollkarte –
  Of a inspector's card

Bauartgenehmigung Nr. / Approval No.: e1*209*01

1. Hersteller- oder Handelsmarke:
   Manufacturing or commercial mark:
   Trüb AG

Nummer der Genehmigung: e1*209*01
Approval No.:

2. Modellbezeichnung:
Name of model:
TCOS Tachograph-AETR

Version:
Release:
TCOS Tachograph Card Version 1.0

3. Name des Herstellers:
Name of manufacturer:
Trüb AG

4. Anschrift des Herstellers:
Address of manufacturer:
CH-5001 Aarau

5. Vorgelegt zur Bauartgenehmigung am:
Submitted for approval on:
30.11.2010

6. Prüfstelle(n):
Test laboratory or laboratories:
Landesbetrieb Mess- und Eichwesen Nordrhein-Westfalen
DE-50829 Köln

7. Datum und Nummer des Prüfberichts:
Date and number of reports:
25.11.2010 61.17-XXVIII-6

8. Datum der Bauartgenehmigung:
Date of approval:
28.07.2010

9. Datum des Entzugs der Bauartgenehmigung:
Date of withdrawal of approval:
entfällt
not applicable

10. Modell(e) der Kontrollgerätkomponente(n), für die die Komponente bestimmt ist:
Model(s) of component(s) of control device with which the component is intended to be used:
für alle bauartgenehmigten Kontrollgeräte
for all type-approved recording equipments

Kraftfahrt-Bundesamt
DE-24932 Flensburg

Nummer der Genehmigung: e1*209*01
Approval No.:

11. Ort: **DE-24944 Flensburg**
Place:

12. Datum: **02.12.2010**
Date:

13. Anlagen:
Descriptive documents annexed:
Nebenbestimmungen und Rechtsbehelfsbelehrung
Collateral clauses and instruction on right to appeal

1 Prüfbericht nebst Anlage(n)
1 Test report with annex(es)

14. Bemerkungen:
Remarks:
Karten mit folgenden Unterscheidungszeichen:
cards with the following distinguishing signs:

Fahrerkarte **driver card**	**„UA", „MD"**
Werkstattkarte **workshop card**	**„UA", „MD"**
Unternehmenskarte **company card**	**„UA", „MD"**
Kontrollkarte **inspector's card**	**„UA", „MD"**

Fahrerkarte, Werkstattkarte, Unternehmenskarte und Kontrollkarte in der Moldawien-Ausführung (MD) kommen hinzu
driver card, workshop card, company card and inspector's card in Moldova-version (MD) are added

Unterschrift: **Im Auftrag**
Signature:

Dirk Hansen

KRAFTFAHRT-BUNDESAMT 496

S.C. CERTSIGN S.A. certSIGN 2/8 BUCUREȘTI - ROMÂNIA

Kraftfahrt-Bundesamt

DE-24932 Flensburg

Nr. der Genehmigung: e1*209*01
Approval No.:

- Anlage -

Nebenbestimmungen und Rechtsbehelfsbelehrung

Nebenbestimmungen

Die Einzelerzeugnisse der reihenweisen Fertigung müssen mit den Genehmigungsunterlagen genau übereinstimmen. Die in der bisherigen Genehmigung enthaltenen Auflagen gelten auch für diese Erweiterung.

Rechtsbehelfsbelehrung

Gegen diese Genehmigung kann innerhalb eines Monats nach Bekanntgabe Widerspruch erhoben werden. Der Widerspruch ist **beim Kraftfahrt-Bundesamt, Fördestraße 16, DE-24944 Flensburg**, schriftlich oder zur Niederschrift einzulegen.

- Attachment -

Collateral clauses and instruction on right to appeal

Collateral clauses

The individual production of serial fabrication must be in exact accordance with the approval documents. The requirements contained in the previous approval are also valid for this amendment.

Instruction on right to appeal

This approval can be appealed within one month after notification. The appeal is to be filed in writing or as a transcript at the **Kraftfahrt-Bundesamt, Fördestraße 16, DE-24944 Flensburg.**

S.C. CERTSIGN S.A.

Certification Report

Bundesamt für Sicherheit in der Informationstechnik

BSI-DSZ-CC-0272-2004

for

TCOS Tachograph Card Version 1.0
Release 2

from

T-Systems International GmbH
Service Line SI, T-Telesec

Deutsches IT-Sicherheitszertifikat

erteilt vom

Bundesamt für Sicherheit in der Informationstechnik

Bundesamt für Sicherheit
in der Informationstechnik

BSI-DSZ-CC-0272-2004

Smart Card with Tachograph Application

TCOS Tachograph Card Version 1.0 Release 2

from

T-Systems International GmbH Service Line SI, T-Telesec

IT Security Certified

SOGIS-MRA

The IT product identified in this certificate has been evaluated at an accredited and licensed/ approved evaluation facility using the *Common Methodology for IT Security Evaluation, Part 1 Version 0.6, Part 2 Version 1.0* extended by advice of the Certification Body for components beyond EAL4 and smart card specific guidance for conformance to the *Common Criteria for IT Security Evaluation, Version 2.1 (ISO/IEC 15408:1999)* and including final interpretations for compliance with Common Criteria Version 2.2 and Common Methodology Part 2, Version 2.2.

Evaluation Results:

PP Conformance:	**Protection Profile PP/9911 and PP BSI-PP-0002-2001**
Functionality:	**Product specific Security Target according to Appendix 10 of Annex 1B of Regulation (EC) no. 1360/2002, amending Regulation (EEC) no. 3821/85 on recording equipment in road transport; Common Criteria Part 2 extended**
Assurance Package:	**Common Criteria Part 3 conformant, EAL4 augmented by ADO_IGS.2, ADV_IMP.2, ALC_DVS.2, ATE_DPT.2, AVA_MSU.3 and AVA_VLA.4; Equivalent to ITSEC E3 high as required by Appendix 10 of Annex 1B of Regulation (EC) no. 1360/2002**

This certificate applies only to the specific version and release of the product in its evaluated configuration and in conjunction with the complete Certification Report.

The evaluation has been conducted in accordance with the provisions of the certification scheme of the German Federal Office for Information Security (BSI) and the conclusions of the evaluation facility in the evaluation technical report are consistent with the evidence adduced.

The notes mentioned on the reverse side are part of this certificate.

Bonn, 22 July 2004

The President of the Federal Office
for Information Security

Common Criteria

Dr. Helmbrecht

L.S.

Bundesamt für Sicherheit in der Informationstechnik
Godesberger Allee 185-189 - D-53175 Bonn - Postfach 20 03 63 - D-53133 Bonn
Telefon (0228) 9582-0 - Telefax (0228) 9582-455 - Infoline (0228) 9582-111

The rating of the strength of functions does not include the cryptoalgorithms suitable for encryption and decryption (see BSIG Section 4, Para. 3, Clause 2)

This certificate is not an endorsement of the IT product by the Federal Office for Information Security or any other organisation that recognises or gives effect to this certificate, and no warranty of the IT product by the Federal Office for Information Security or any other organisation that recognises or gives effect to this certificate, is either expressed or implied.

Preliminary Remarks

Under the BSIG[1] Act, the Federal Office for Information Security (BSI) has the task of issuing certificates for information technology products.
Certification of a product is carried out on the instigation of the vendor or a distributor, hereinafter called the sponsor.

A part of the procedure is the technical examination (evaluation) of the product according to the security criteria published by the BSI or generally recognised security criteria.

The evaluation is normally carried out by an evaluation facility recognised by the BSI or by BSI itself.

The result of the certification procedure is the present Certification Report. This report contains among others the certificate (summarised assessment) and the detailed Certification Results.

The Certification Results contain the technical description of the security functionality of the certified product, the details of the evaluation (strength and weaknesses) and instructions for the user.

[1] Act setting up the Federal Office for Information Security (BSI-Errichtungsgesetz, BSIG) of 17 December 1990, Bundesgesetzblatt I p. 2834

Contents

A Certification

1 Specifications of the Certification Procedure

The certification body conducts the procedure according to the criteria laid down in the following:

- BSIG[2]
- BSI Certification Ordinance[3]
- BSI Schedule of Costs[4]
- Special decrees issued by the Bundesministerium des Innern (Federal Ministry of the Interior)
- DIN EN 45011 standard
- BSI certification: Procedural Description (BSI 7125)
- Common Criteria for IT Security Evaluation (CC), Version 2.1[5]
- Common Methodology for IT Security Evaluation (CEM)
  - Part 1, Version 0.6
  - Part 2, Version 1.0
- BSI certification: Application Notes and Interpretation of the Scheme (AIS)
- Advice from the Certification Body on methodology for assurance components above EAL4

The use of Common Criteria Version 2.1, Common Methodology, part 2, Version 1.0 and final interpretations as part of AIS 32 results in compliance of the certification results with Common Criteria Version 2.2 and Common Methodology Part 2, Version 2.2 as endorsed by the Common Criteria recognition arrangement committees.

---

2 Act setting up the Federal Office for Information Security (BSI-Errichtungsgesetz, BSIG) of 17 December 1990, Bundesgesetzblatt I p. 2834

3 Ordinance on the Procedure for Issuance of a Certificate by the Federal Office for Information Security (BSI-Zertifizierungsverordnung, BSIZertV) of 7 July 1992, Bundesgesetzblatt I p. 1230

4 Schedule of Cost for Official Procedures of the Federal Office for Information Security (BSI-Kostenverordnung, BSI-KostV) of 29th October 1992, Bundesgesetzblatt I p. 1838

5 Proclamation of the Bundesministerium des Innern of 22nd September 2000 in the Bundesanzeiger p. 19445

2 Recognition Agreements

In order to avoid multiple certification of the same product in different countries a mutual recognition of IT security certificates - as far as such certificates are based on ITSEC or CC - under certain conditions was agreed.

2.1 ITSEC/CC - Certificates

The SOGIS-Agreement on the mutual recognition of certificates based on ITSEC became effective on 3 March 1998. This agreement was signed by the national bodies of Finland, France, Germany, Greece, Italy, The Netherlands, Norway, Portugal, Spain, Sweden, Switzerland and the United Kingdom. This agreement on the mutual recognition of IT security certificates was extended to include certificates based on the CC for all evaluation levels (EAL 1 – EAL 7).

2.2 CC - Certificates

An arrangement (Common Criteria Arrangement) on the mutual recognition of certificates based on the CC evaluation assurance levels up to and including EAL 4 was signed in May 2000. It includes also the recognition of Protection Profiles based on the CC. The arrangement was signed by the national bodies of Australia, Canada, Finland France, Germany, Greece, Italy, The Netherlands, New Zealand, Norway, Spain, United Kingdom and the United States. Israel joined the arrangement in November 2000, Sweden in February 2002, Austria in November 2002, Hungary and Turkey in September 2003, Japan in November 2003.

3 Performance of Evaluation and Certification

The certification body monitors each individual evaluation to ensure a uniform procedure, a uniform interpretation of the criteria and uniform ratings.

The product TCOS Tachograph Card Version 1.0, Release 2 has undergone the certification procedure at BSI. This is a re-certification based on BSI-DSZ-CC-0242-2004.

The evaluation of the product TCOS Tachograph Card Version 1.0, Release 2 was conducted by TÜV Informationstechnik GmbH (ITSEF)[6]. TÜV Informationstechnik GmbH is an evaluation facility recognised by BSI.

The sponsor and vendor and distributor is T-Systems International GmbH, Service Line SI, T-Telesec.

The certification is concluded with

- the comparability check and
- the production of this Certification Report.

This work was completed by the BSI on 22 July 2004.

The confirmed assurance package is only valid on the condition that

- all stipulations regarding generation, configuration and operation, as given in the following report, are observed,
- the product is operated in the environment described, where specified in the following report.

This Certification Report only applies to the version of the product indicated here. The validity can be extended to new versions and releases of the product, provided the sponsor applies for re-certification of the modified product, in accordance with the procedural requirements, and the evaluation does not reveal any security deficiencies.

For the meaning of the assurance levels and the confirmed strength of functions, please refer to the excerpts from the criteria at the end of the Certification Report.

6 Information Technology Security Evaluation Facility

4 Publication

The following Certification Results contain pages B-1 to B-28 and D-1 to D-6.

The product TCOS Tachograph Card Version 1.0, Release 2 has been included in the BSI list of the certified products, which is published regularly (see also Internet: http:// www.bsi.bund.de). Further information can be obtained from BSI-Infoline 0228/9582-111.

Further copies of this Certification Report can be requested from the vendor[7] of the product. The Certification Report can also be downloaded from the above-mentioned website.

[7] T-Systems International GmbH, Service Line SI, T-Telesec, Untere Industriestr. 20, 57250 Netphen

B Certification Results

The following results represent a summary of

- the security target of the sponsor for the target of evaluation,
- the relevant evaluation results from the evaluation facility, and
- complementary notes and stipulations of the certification body.

Contents of the certification results

1 Executive Summary

Target of Evaluation (TOE) and subject of the Security Target (ST) [6] and [7] is the smart card product "TCOS Tachograph Card Version 1.0, Release 2".

The evaluation was performed as a re-evaluation process based on Version 1.0 of the TCOS Tachograph Card, certified under BSI-DSZ-CC-0242-2004.

The design changes of the versions 1.0, release 2 are mostly shifting TOE code from EEPROM into the ROM mask and including the concept of card initialisation by an external initialisation company (i.e. the company Trüb AG, see table 1 and part D, Annex B of this report).

The TOE will be used within the Tachograph System as a security medium which carries a specific Tachograph Application intended for its use with the recording equipment.

The basic functions of the Tachograph Card are:

- to store card identification and card holder identification data. These data are used by the vehicle unit to identify the cardholder, provide accordingly functions and data access rights, and ensure cardholder accountability for his activities,
- to store cardholder activities data, events and faults data and control activities data, related to the cardholder.

A Tachograph Card is therefore intended to be used by a card interface device of a vehicle unit. It may also be used by any card reader (e.g. of a personal computer) which shall have full read access right on any user data. During the end-usage phase of a Tachograph Card life cycle (phase 7 of life-cycle as described), vehicle units only may write user data to the card. A Tachograph Card is either of the type Driver Card or Control Card or Workshop Card or Company Card as outlined in the ST [7], chapter 2.1.

The TOE comprises the following components:

- Integrated Circuit (IC) "Infineon Smart Card Controller SLE66CX322P m1484 b14" provided by Infineon Technologies AG
- Smartcard Embedded Software provided by T-Systems International GmbH, Service Line SI, T-Telesec.

The smart card embedded software consists of a native operating system based on TCOS V3.0 with additional Tachograph Application commands and the Tachograph Card's file system. The configuration of the Tachograph Card to be performed in a secure environment concerns the following points:

- Completion of the operating system and tachograph application code
- Loading of the Tachograph Card's specific file system for either a complete Driver Card, Control Card, Workshop Card or Company Card

- Loading of the security keys to protect delivery and for authentication prior to personalisation

The TOE is developed and constructed in full accordance with the Tachograph Card Specification [8], Annex 1B main body, Appendix 2, Appendix 10 (Tachograph Card Generic Security Target) and Appendix 11. In particular, this implies the conformance of the Tachograph Card with the following standards: ISO/IEC 7810 Identification cards – Physical characteristics, ISO/IEC 7816 Identification cards - Integrated circuits with contacts: part 1, part 2, part 3, part 4 and part 8; ISO/IEC 10373 Identification cards – Test methods.

In order to achieve the required system security, the Tachograph Card and the corresponding ST [6] and [7] meet all the security requirements and evaluation conditions defined in the Tachograph Card's "Generic Security Target" in [8], Appendix 10 under consideration of the interpretations in [9].

The life-cycle of the TOE conforms to the smart card life cycle described in Appendix 10 of [8] referring to PP/9911 [13]. The following table outlines the life-cycle as applied for the TOE:

Phase		Description
Phase 1	Smart Card Embedded Software Development	The Smart Card Embedded Software Developer (T-Systems International GmbH - T-Telesec, Siegen) is in charge of the Smart Card Embedded Software (Basic Software, Application Software) development and the specification of IC initialisation and pre-personalisation requirements.
Phase 2	IC Development	The IC Designer (Infineon Technologies AG[8]) designs the IC, develops IC Dedicated Software, provides information, software or tools to the Smart Card Embedded Software Developer, and receives the Smart Card Embedded Software (only ROM code) from the developer through trusted delivery and verification procedures. The IC Designer constructs the smart card IC database, necessary for the IC photo mask fabrication.
Phase 3	IC Manufacturing and Testing	The IC Manufacturer (Infineon Technologies AG[9]) generates the masks for the IC manufacturing based upon an output from the smart card IC database. He is esponsible for producing the IC through two main steps: IC manufacturing and IC testing.
Phase 4	IC Packaging and Testing	The IC Packaging Manufacturer (Infineon Technologies AG[10]) is responsible for the IC packaging (production of modules) and testing.

8 for evaluated development sites see [18]
9 for evaluated manufacturing site see [18]
10 for evaluated packaging site see [18]

Phase		Description
Phase 5	Smart Card Product Finishing Process	The Smart Card Product Manufacturer is responsible for embedding the modules into a plastic card.
Phase 6.1	Smart Card Initialisation	The initialisation of the TOE (in form of initialisation of the embedded modules) and its testing is done by T-Systems International GmbH – T-Telesec Trust Center, Siegen or by an external initialisation company (i.e. Trüb AG, Aarau, Switzerland). In this phase the TOE becomes either the type Driver Card or Control Card or Workshop Card or Company Card. (Note: The initialisation phase is indicated in PP/9911 as part of phase 5)
Delivery of the TOE		The TOE is delivered from the initialisation organisation to the customer which is the personalisation organisation in form of a complete (initialised) smart card.
Phase 6.2	Smart Card Personalisation	The Personaliser is responsible for the smart card personalisation and final tests to be done in a secure environment. (Note: The personalisation phase is indicated as phase 6 in PP/9911)
Phase 7	Smart Card End-usage	The Smart Card Issuer is responsible for the smart card product delivery to the smart card end-user, and the end of life process.

Table 1: Life cycle of the TOE

The evaluation of the TOE was conducted as a composition evaluation making use of the platform evaluation results of the CC evaluation of the underlying semiconductor "Infineon Smart Card Controller SLE66CX322P m1484b14" provided by Infineon Technologies AG [18] updated by an actual re-assessment, which had been successfully carried out by TÜV Informationstechnik GmbH. The RSA2048 cryptographic library as part of [18] was not used by the embedded software developer.

The IC was evaluated according to Common Criteria EAL 5 augmented with a minimum strength level for its security functions of SOF-high for specific functionality based on the Protection Profile BSI-PP-0002 [12] and as outlined in [18]. These platform evaluation was performed by TÜV Informationstechnik GmbH.

The Embedded Software of the "TCOS Tachograph Card Version 1.0, Release 2" and the overall composition was evaluated by TÜV Informationstechnik GmbH, too.

The concept for composition as outlined in CC Supporting Document [4, AIS 36] was used.

The evaluation was completed on 16 July 2004. TÜV Informationstechnik GmbH is an evaluation facility (ITSEF)[11] recognised by BSI. The sponsor,

[11] Information Technology Security Evaluation Facility

vendor and distributor of the Tachograph Card Version 1.0, Release 2 is T-Systems International GmbH, Service Line SI, T-Telesec.

1.1 Assurance package

The TOE security assurance requirements are based entirely on the assurance components defined in part 3 of the Common Criteria (see Part C or [1], part 3 for details).

The TOE meets the assurance requirements of assurance level EAL4+ (Evaluation Assurance Level 4 augmented). The following table shows the augmented assurance components.

Requirement	Identifier
EAL4	TOE evaluation: Methodically designed, tested, and reviewed
+: ADO_IGS.2	Delivery and operation - Generation log
+: ADV_IMP.2	Development - Implementation of the TSF
+ ALC_DVS.2	Life cycle support - Sufficiency of security measures
+: ATE_DPT.2	Tests - Testing: low-level design
+ AVA_MSU.3	Vulnerability assessment – Analysis and testing for insecure states
+: AVA_VLA.4	Vulnerability assessment – Highly resistant

Table 2: Assurance components and EAL-augmentation

The level of assurance and the augmentations (ADO_IGS.2, ADV_IMP.2, ATE_DPT.2 and AVA_VLA.4) are chosen in order to allow the confirmation of equivalence to ITSEC [10] E3 high as required by Appendix 10 of Annex 1B of Regulation (EC) no. 1360/2002 [8] and outlined in JIL Security Evaluation and Certification of Digital Tachographs [9]. ALC_DVS.2 and AVA_MSU.3 are augmented in addition for PP conformance.

1.2 Functionality

The TOE Security Functional Requirements (SFR) and TOE Security Functions are based on Appendix 10 of Annex 1B of Regulation (EC) no. 1360/2002 [8] specified in the document JIL Security Evaluation and Certification of Digital Tachographs [9].

The TOE Security Functional Requirements selected in the Security Target are Common Criteria Part 2 extended as shown in the following tables.

Security Functional Requirement	Identifier	Source from PP or added in ST-IC
FCS	**Cryptographic support**	
FCS_COP.1	Cryptographic operation	ST-IC [19]
FCS_CKM.1	Cryptographic key generation	ST-IC [19]
FDP	**User data protection**	
FDP_ACC.1	Subset access control	ST-IC [19]
FDP_ACF.1	Security attribute based access control	ST-IC [19]
FDP_IFC.1	Subset information flow control	PP [12]
FDP_ITT.1	Basic internal transfer protection	PP [12]
FMT	**Security Management**	
FMT_MSA.1	Management of security attributes	ST-IC [19]
FMT_MSA.3	Static attribute initialisation	ST-IC [19]
FPT	**Protection of the TOE Security Functions**	
FPT_FLS.1	Failure with preservation of secure state	PP [12]
FPT_ITT.1	Basic internal TSF data transfer protection	PP [12]
FPT_PHP.3	Resistance to physical attack	PP [12]
FPT_SEP.1	TSF domain separation	PP [12]
FRU	**Resource utilisation**	
FRU_FLT.2	Limited fault tolerance	PP [12]

Table 3: Security Functional Requirements for the IC part of the TOE (see [18] and [19] for BSI-DSZ-CC-0223-2003) taken from CC Part 2

Security Functional Requirement	Identifier	Source from PP or added in ST-IC
FAU	**Security Audit**	
FAU_SAS.1	Audit storage	PP [12] /ST-IC [19] [12]
FCS	**Cryptographic support**	
FCS_RND.1	Quality metric for random numbers	PP [12] / ST-IC [19]
FMT	**Security management**	
FMT_LIM.1	Limited capabilities	PP [12]
FMT_LIM.2	Limited availability	PP [12]
FPT	**Protection of the TOE Security Functions**	
FPT_TST.2	Subset TOE testing	ST-IC [19]

12 PP/ST-IC: component is described in the PP but operations are performed in the ST.

Table 4: Security Functional Requirements for the IC part of the TOE (see [18] and [19] for BSI-DSZ-CC-0223-2003) CC part 2 extended

Security Functional Requirement[13]	Identifier	Source from PP or added in ST
FAU	**Security audit**	
FAU_SAA.1	Potential violation analysis	[9] and PP [13]
FCO	**Communication**	
FCO_NRO.1	Selective Proof of origin	ST [7] and [9]
FCS	**Cryptographic support**	
FCS_CKM.1	Cryptographic Key Generation	ST [7] and [9]
FCS_CKM.2	Cryptographic Key Distribution	ST [7] and [9]
FCS_CKM.3	Cryptographic Key Access	[9] and PP [13]
FCS_CKM.4	Cryptographic Key Destruction	[9] and PP [13]
FCS_COP.1	Cryptographic operation (Triple-DES and RSA)	[9] and PP [13]
FDP	**User data protection**	
FDP_ACC.2	Complete access control	[9] and PP [13]
FDP_ACF.1	Security attribute based access control	[9] and PP [13]
FDP_DAU.1	Basic data authentication	[9] and PP [13]
FDP_ETC.1	Export of user data without security attributes	[9] and PP [13]
FDP_ETC.2	Export of user data with security attributes	ST [7] and [9]
FDP_ITC.1	Import of user data without security attributes	[9] and PP [13]
FDP_RIP.1	Subset residual information protection	[9] and PP [13]
FDP_SDI.2	Stored data integrity monitoring and action	[9] and PP [13]
FIA	**Identification and authentication**	
FIA_AFL.1-1	Authentication failure handling	[9] and PP [13]
FIA_AFL.1 WS-Card	Authentication failure handling (of workshop card)	ST [7] and [9]
FIA_ATD.1	User attribute definition	[9] and PP [13]
FIA_UAU.1	Timing of authentication	[9] and PP [13]
FIA_UAU.3	Unforgeable authentication	[9] and PP [13]
FIA_UAU.4	Single-use authentication mechanisms	[9] and PP [13]
FIA_UID.1	Timing of identification	[9] and PP [13]
FIA_USB.1	User-subject binding	[9] and PP [13]
FMT	**Security management**	
FMT_MOF.1	Management of security functions behaviour	[9] and PP [13]

[13] The indicator +n after a component name indicates a specific iteration of the component

Security Functional Requirement[13]	Identifier	Source from PP or added in ST
FMT_MSA.1	Management of security attributes	[9] and PP [13]
FMT_MSA.2	Secure security attributes	[9] and PP [13]
FMT_MSA.3	Static attribute initialisation	[9] and PP [13]
FMT_MTD.1	Management of TSF data	[9] and PP [13]
FMT_SMF.1	Specification of management functions	ST [7]
FMT_SMR.1	Security roles	[9] and PP [13]
FPR	**Privacy**	
FPR_UNO.1	Unobservability	[9] and PP [13]
FPT	**Protection of the TSF**	
FPT_FLS.1	Failure with preservation of secure state	[9] and PP [13]
FPT_PHP.3	Resistance to physical attack	[9] and PP [13]
FPT_SEP.1	TSF domain separation	[9] and PP [13]
FPT_TDC.1	Inter-TSF basic TSF data consistency	[9] and PP [13]
FPT_TST.1	TSF testing	[9] and PP [13]
FTP	Trusted path/channels	
FTP_ITC.1	Inter-TSF trusted channel	ST [7] and [9]

Table 5: Security Functional Requirements for the Embedded SW part of the TOE taken from CC Part 2

Note: Only the titles of the Security Functional Requirements are provided. For more details please refer to the Security Target [7] and [19] and PP [12] and [13].

These Security Functional Requirements are implemented by the following TOE Security Functions:

TOE Security Functions (IC part)	Description
SF1-IC	Operating state checking
SF2-IC	Phase management with test mode lock-out
SF3-IC	Protection against snooping
SF4-IC	Data encryption and data disguising
SF5-IC	Random number generation
SF6-IC	TSF self test
SF7-IC	Notification of physical attack
SF8-IC	Memory Management Unit (MMU)
SF9-IC	Cryptographic support

Table 6: TOE Security Functions for the IC part of the TOE (see [18] and [19] for BSI-DSZ-CC-0223-2003)

TOE Security Functions (SW part)	Description
SF1-SW	Authentication based on PIN verification and retry counter
SF2-SW	Identification & Authentication based on Challenge-Response
SF3-SW	Data exchange under secure messaging
SF4-SW	Data exchange with digital signature
SF5-SW	Access Control of stored data objects
SF6-SW	Accuracy and Audit
SF7-SW	Reliability

Table 7: TOE Security Functions of the Embedded SW part of the TOE

Note: Only the titles of the TOE Security Functions are provided. For more details please refer to the Security Target [7] and [19].

All TOE Security Functions are applicable from TOE delivery to phase 7 of the smart card life cycle model.

1.3 Strength of Function

The TOE's strength of functions is rated 'high' (SOF-high) for the following functions:

- SF1-SW (Authentication based on PIN verification and retry counter)
- SF2-SW (Identification & authentication based on Challenge-Response)
- SF3-SW (Data exchange under secure messaging)
- SF4-SW (Data exchange with digital signature)

For SOF ratings of IC part of the TOE please refer to the certification report [18].

The rating of the strength of functions does not include the cryptoalgorithms suitable for encryption and decryption (see BSIG Section 4, Para. 3, Clause 2).

1.4 Summary of threats and Organisational Security Policies (OSPs) addressed by the evaluated IT product

The threats are subdivided into three groups affecting the IC, the general, or the Tachograph Card specific Embedded Software:

Name	Definition
T.Leak-Inherent	Inherent Information Leakage
T.Phys-Probing	Physical Probing
T.Malfunction	Malfunction due to Environmental Stress
T.Phys-Manipulation	Physical Manipulation

Name	Definition
T.Leak-Forced	Forced Information Leakage
T.Abuse-Func	Abuse of Functionality
T.RND	Deficiency of Random Numbers

Table 8: Threats of IC part of the TOE (see [19] and [12])

Name	Definition
Threats on all Phases	
T.CLON	Cloning of the TOE
Threats on Phase 1	
T.DIS_INFO	Disclosure of IC Assets
T.DIS_DEL	Disclosure of the Smart Card Embedded Software / Application Data during Delivery
T.DIS_ES1	Disclosure of the Smart Card Embedded Software / Application Data within the Development Environment
T.DIS_TEST_ES	Disclosure of Smart Card Embedded Software Test Programs / Information
T.T_DEL	Theft of the Smart Card Embedded Software / Application Data during delivery
T.T_TOOLS	Theft or unauthorised use of the Smart Card Embedded Software Development Tools
T.T_SAMPLE2	Theft or Unauthorised Use of TOE Samples
T_MOD_DEL	Modification of the Smart Card Embedded Software / Application Data during Delivery
T.MOD	Modification of the Smart Card Embedded Software / Application Data within the Development Environment
Threats on Delivery from Phase 1 to Phases 4 / 5 / 6	
T.DIS_DEL1	Disclosure of Application Data during Delivery
T.DIS_DEL2	Disclosure of Delivered Application Data
T.MOD_DEL1	Modification of Application Data during Delivery
T.MOD_DEL2	Modification of Delivered Application Data
Threats on Phases 4 to 7	
T.DIS_ES2	Disclosure of the Smart Card Embedded Software / Application Data
T.T_ES	Theft or Unauthorised Use of TOE
T.T_CMD	Use of TOE Command-Set
T.MOD_LOAD	Program Loading
T.MOD_EXE	Program Execution

Name	Definition
T.MOD_SHARE	Modification of Program Behaviour
T.MOD_SOFT	Modification of Smart Card Embedded Software / Application Data

Table 9: Threats of the TOE-ES parts of the TOE taken from PP/9911 [13]

Name	Definition
T.Ident_Data	Modification of Identification Data
T.Activity_Data	Modification of Activity Data
T.Data_exchange	Modification of Activity Data during Data Transfer

Table 10: Threats of the TOE-ES (Tachograph Card Specific Threats)

Note: Only the titles of the threats are provided. For more details please refer to the Security Target [7] and [19] and PP [12] and [13].

1.5 Special configuration requirements

The TOE is delivered at the initialisation process (see above) in form of complete cards, i.e. after the initialisation process of the TOE has been successfully finished, final tests have been successfully conducted and the card production has been fulfilled.

A Tachograph Card may be of the following types: Driver Card, Control Card, Workshop Card or Company Card as defined in [8] depending on the specific data structure loaded into the card.

The personalisation of the Tachograph Card requires a preceding authentication of the external world (personalisation unit). At the end of the personalisation process, the card is switched to the end-user operational phase.

There are no special security measures for the start-up of the TOE besides the requirement that the TOE has to be used under the well-defined operating conditions and that the requirements on the personalisation and usage have to be applied as described in the user documentation [15], [16] and [17].

1.6 Assumptions about the operating environment

The TOE is intended to be used within the Tachograph System as a security medium which carries a specific Tachograph Application intended for its use with the recording equipment as specified in [8].

The following general assumptions are made based on the PP/9911 [13] and PP/9806 [14] referenced in Appendix 10 of Annex 1B of Regulation (EC) no. 1360/2002 [8] (Generic Security Target). As the TOE is delivered at the end of phase 6.1, the assumptions up to phase 6.1 are covered by this evaluation. Therefore the following assumptions taken from PP/9911 are relevant after delivery of the TOE and are to be covered by the operational environment:

Name	Definition
Assumptions on the TOE Delivery Process (for Phases 6 to 7)	
A.DLV_PROTECT	Protection of the TOE under Delivery and Storage
A.DLV_AUDIT	Audit of Delivery and Storage
A.DLV_RESP	Responsibility within Delivery
Assumptions on Phases 6	
A.USE_TEST	Testing of the TOE
A.USE_PROD	Protection of the TOE under Testing and Manufacturing
Assumptions on Phase 7	
A.USE_DIAG	Secure Communication

Table 11: General assumptions for the TOE

The security target [7] specifically mentions the assumption A.Process-Card taken from ST-IC [19] and A.Personalisation relevant for phase 6.2.

With A.Personalisation an assumption on secure generation and handling of personalisation data is made because the establishment of a secure environment for the personalisation process with adequate personnel, organisational and technical security measures is in the responsibility of the personalisation centre itself. This assumptions contains also the three assumptions A.DLV_PROTECT*, A.DLV_AUDIT* and A.DLV_RESP* during phase 6.2.

The assumption A.Process-Card (Protection during Packaging, Finishing and Personalisation) applies for the phases 6.2 up to delivery to the end-user to maintain confidentiality and integrity of the TOE.

1.7 Disclaimers

The Certification Results only apply to the version of the product indicated in the Certificate and on the condition that all the stipulations are kept as detailed in this Certification Report. This certificate is not an endorsement of the IT product by the Federal Office for Information Security (BSI) or any other organisation that recognises or gives effect to this certificate, and no warranty of the IT product by BSI or any other organisation that recognises or gives effect to this certificate, is either expressed or implied.

2 Identification of the TOE

The Target of Evaluation (TOE) is called:

TCOS Tachograph Card Version 1.0, Release 2

The following table outlines the TOE deliverables:

No	Type	Identifier	Release	Date	Form of Delivery
1	HW / SW	Tachograph Smart Card Consisting of: - Infineon Smart Card Controller SLE66CX322P m1484 b14 with production line indicator: "2" (Dresden) including IC Dedicated STS Self Test Software and RMS Resource Management System software - Embedded Software, Version 1.0, Release 2 (Native operating system and Tachograph Application with Application Data depending on card type)	Version 1.0, Release 2 See [18] TCOSV30R2		Initialised and tested smart cards SW implemented in ROM of the IC SW implemented in ROM and EEPROM of the IC
2	DOC	Administrator manual TCOS Tachograph Card [15]	V1.03	6 July 2004	Document in paper / electronic form
3	DOC	User Manual TCOS Tachograph Card [16]	V1.02	6 July 2004	Document in paper / electronic form
4	SW	Log-files for personalisation proceedure [17]		14. April 2004	Delivered together with [15]
5	Keys	Keys for verification of the TOE and for personalisation (transport code, personalisation key)	Customer specific		In electronic format

Table 12: Deliverables of the TOE

To ensure that the customer receives this evaluated version, the procedures to start the personalisation process as described in the administrator manual [15] [15] have to be followed.

3 Security Policy

The TOE will be employed within the Tachograph System as a security medium which carries a specific Tachograph Application intended for its use with the recording equipment.

The TOE is the composition of the IC, IC Dedicated Software and Smart Card Embedded Software. The security policy is to provide:

- protection against leakage of information (e.g. to ensure the confidentiality of cryptographic keys during cryptographic functions performed by the TOE), against physical probing, against malfunctions, against physical manipulations, against access for code and data memory and against abuse of functionality
- secure storage of user data and TSF data
- access control to user data and TSF data according to the specified rules
- secure communication to the vehicle unit of the Tachograph System

as specified in Appendix 10 of Annex 1B of Regulation (EC) no. 1360/2002 [8].

4 Assumptions and Clarification of Scope

The TOE is intended to be used within the Tachograph System as a security medium which carries a specific Tachograph Application intended for its use with the recording equipment as specified in [8].

General assumptions are made based on the PP/9911 [13] and PP/9806 [14] referenced in Appendix 10 of Annex 1B of Regulation (EC) no. 1360/2002 [8] (Generic Security Target). These general assumptions are structured according to the phases of the life cycle. Some of these assumptions are related to procedures in phases 1 to 6.1. These phases were part of the TOE evaluation. As delivery of the TOE is defined at the end of phase 6.1 of the life cycle. (see table 1), the phases 6.2 and 7 are the usage phases of the TOE. Procedures related to assumptions on these phases and the additional assumptions A.Process-Card taken from ST-IC [19] and A.Personalisation relevant for phase 6.2 are outlined in the user documentation.

For further assumptions on the card holder of the workshop card and on the Certification Authorities (CA) including the Root-CA see chapter 10 of this part of the report.

There do not exist more Tachograph Card specific assumptions as the definition of the card type is done before the TOE personalisation in phase 6.2 before delivery.

The TOE is the TCOS Tachograph Card Version 1.0, Release 2 providing security functions as required in Appendix 10 of Annex 1B of Regulation (EC) no. 1360/2002 [8] (Generic Security Target). Threats on the overall Tachograph

System which are not related to the Tachograph Smart Cards were not addressed by this product evaluation.

5 Architectural Information

The TOE is a product. It is composed from an Integrated Circuit (IC) with its proprietary IC Dedicated Software and a Smart Card Embedded Software (ES), consisting of a native operating system and application software and data structures. The four different card types are distinguished as they contain specific data structures and data.

The embedded software is composed of the following main components:

The kernel is responsible for the communication between the different components of the ES. It checks memory areas, provides resources and controls the overall operation.

The administration component provides administrative functions of the ES as functionality for generation and deletion of files and directories and for reading and writing of files. It provides the ES with capabilities for finding and selection of files and for modification of object attributes. Furthermore, it controls access rules on objects within the file system.

A cryptographic component provides the cryptographic functionality used by the ES. It controls access to keys and passwords

The IO-component is responsible for the communication with the external world via the IO-Interface of the card. It handles the protocols T=0 and T=1 and checks APDUs on syntactical conformance.

The ROM TCOS Tachograph-Type Task contains the Tachograph specific parts of the ES. It analyses APDUs and calls the required kernel functions.

For information on the IC part of the TOE please refer to [18] and [19].

As all parts of TOE software are running inside the IC, the external interface of the TOE to its environment can be defined as the external interface of this IC. The external interface is divided into a physical / electrical interface and a logical interface.

The physical / electrical interface of the IC are the pads to connect the lines supply voltage, reset input, clock input, ground and I/O. An external voltage and timing supply as well as a data interface are necessary for the operation of the IC. Beyond the physical behaviour, the data interface is defined by the Smart Card Embedded Software (ES). A user would use the physical interface via the Chip card contacts. The electrical and physical characteristics fulfilled are given in the Tachograph Cards Specification [8]. The location and dimensions of the Chip card contacts comply with the ISO/IEC 7816-2. The electronic signals, the working of the card as well as the power consumption are in accordance with ISO/IEC 7816.

The logical interface consists of two parts: (i) everything below the command level and (ii) the accessing of the Tachograph Cards by commands via the command interface. Commands and protocols of the Tachograph Application for phase 7 are fully described in the Tachograph Cards Specification [8]. Specific commands for the personalisation phase (phase 6.2) are described in the Administrator Manual [15].

The TOE Summary Specification (chapter 6 of the ST [7]) describes the TOE Security Functions with relation to the IC and the Embedded Software.

6 Documentation

The user of the TOE is

(i) the developer of a vehicle unit who needs information how the TOE interacts with the vehicle unit

(ii) the personaliser of the Tachograph Cards who needs information about security procedures and how the TOE supports the personalisation process

(iii) the issuer of the Tachograph Cards who needs information how to use the 4 different card types after personalisation, information on specific aspects of the issuance of the Tachograph Cards and information to be passed to the end-user of the Tachograph Cards (card-holder, e.g. the driver).

For these three types of users the guidance documentation is provided (see [15], [16] and [17]). Information for the issuer is provided within the administrator manual and has to be forwarded to the issuer by the personaliser.

7 IT Product Testing

Tests of the TOE were done (i) with real cards using a card reader and a PC and (ii) in an simulation test environment using an emulator for specific cases. Source code analysis supported specific test scenarios.

For those tests, where real cards are used, the specified method was used to identify the Tachograph Card version and the correct card configuration for every test. The real cards used for testing were either in initialised state (i. e. ready for personalisation) or in operational state (I. e. personalisation completed). Using specific commands, the life cycle state of the ES and the type of the card could be determined.

For identification of the correct versions of the electronic data used for tests in the emulator test environment, and to determine whether the initial condition of each test is satisfied, the methods of the evaluated Configuration Management System were used. The version control mechanism can guarantee that the

design files and the initial data used for testing are those provided by the developers for the specific version of the TOE under evaluation.

As specific subsystems are the same in all card types and others are different, some tests had to be performed on all four card types, others could be re-used. Tests after modifications of the TOE during the evaluation process were re-done as necessary depending on the specific change.

Functional tests of the developer:

The developer tests were performed on all four card types. The developer has performed the functional tests of the TOE in phase 7 and covered all security functions of the TOE including their sub-functions. The test cases were implemented based on the functional specification to verify conformance of the TOE with the expected behaviour. The tests were performed by using Tachograph smart cards and in specific cases a simulation environment. Initialisation (phase 6.1) and personalisation tests (phase 6.2) were performed by using the specified commands for administration. In addition, tests according to Appendix 9 of the EU Tachograph Card Commission Regulation [8] have been performed. In this course all tests on ATR, the protocols T=0 and T=1, the PPS command for switching from T=0 to T=1, the card structure and of the functionality was performed (see Annex A of this report). The analysis on test coverage and test depth showed that the TOE was tested on the level of functional specification, high level design and low level design. All test results were documented in log-files. All tests were performed correctly.

Independent functional evaluator tests:

The evaluator has selected a subset of functional tests on security functions. All security functions were covered by these tests. Expected behaviour as well as error conditions was tested. The evaluator selected a subset of the developer tests for re-testing. This subset covered all security functions and were performed on chip cards or using the simulation environment. In addition, personalisation tests were repeated on all four card types. The subset of tests and the re-testing of developer tests showed that the TOE operates as specified.

Penetration testing

Based on the independent vulnerability analysis penetration tests were performed by the evaluator. These tests covered the life cycle phases, information on operational use of the security functions, random number generation, non-existing APDUs, composite TOE aspects and current consumption of the card. Side channel attacks on DES (SPA, DPA and Timing attacks) were tested and analysed during the evaluation of BSI-DSZ-CC-0223-2003. The result of these analysis was re-assessed and is still valid. It showed that secret keys could not be extracted. Side channel attacks on RSA (SPA, DPA and Timing attacks) were tested by the developer and supplemented by the evaluator. It showed that secret keys could not be extracted. Any identified potential vulnerability was assessed for its exploitability. As a result, the TOE operated as specified during the independent penetration testing. The identified

potential vulnerabilities are not exploitable in the intended operational environment of the TOE.

For re-evaluation most of the developer tests and independent evaluator test as well as specific penetration tests were re-done. Results of other tests could be re-used from the previous evaluation procedure BSI-DSZ-CC-0242-2004. TOE smart cards initialised by the external initialisation company were used for tests.

8 Evaluated Configuration

The TOE is delivered at the end of phase 6.1 in form of initialised and tested complete cards (see table 1). A Tachograph Card may be of the following types: Driver Card, Control Card, Workshop Card or Company Card depending on the specific data structures and data loaded into the card. These four different card types are considered as different configurations of the TOE.

All procedures for personalisation and configuration for the end-user necessary after delivery are described in the administrator manual [15].

9 Results of the Evaluation

The Evaluation Technical Report (ETR) [11] was provided by the ITSEF TÜV Informationstechnik GmbH according to the Common Criteria [1], the Methodology [2], the requirements of the Scheme [3] and all interpretations and guidelines of the Scheme (AIS) [4] as relevant for the TOE.

As the evaluation of the TOE was conducted as a composition evaluation, the ETR [11] includes also the evaluation results of the composite evaluation activities in accordance with CC Supporting Document, ETR-lite for Composition: Annex A Composite smart card evaluation [4, AIS 36].

The ETR [11] builds up on the *ETR-lite for Composition* document of the evaluation of the underlying Infineon Smart Card Controller SLE66CX322P m1484 b14. These *ETR-lite for Composition* document was provided by the ITSEF TÜV Informationstechnik GmbH according to CC Supporting Document, ETR-lite for Composition ([4, AIS 36]). In the course of this composite evaluation the ETR for the Infineon Smart Card Controller SLE66CX322P m1484 b14 as certified in 2003 (see [18]) was updated and the evaluation results were confirmed.

The evaluation methodology CEM [2] was used for those components identical with EAL4. For components beyond EAL4 the methodology was defined in co-ordination with the Certification Body. For smart card specific methodology the scheme interpretations AIS 25, AIS 26 and AIS 36 (see [4]) were used. For specific methodology on random number generator evaluation the scheme interpretations AIS 20 (see [4]) was used.

The assurance refinements outlined in the Security Target were followed in the course of the evaluation of the TOE.

The verdicts for the CC, Part 3 assurance components (according to EAL4 augmented and the class ASE for the Security Target evaluation) are summarised in the following table.

Assurance classes and components		Verdict
Security Target evaluation	CC Class ASE	PASS
TOE description	ASE_DES.1	PASS
Security environment	ASE_ENV.1	PASS
ST introduction	ASE_INT.1	PASS
Security objectives	ASE_OBJ.1	PASS
PP claims	ASE_PPC.1	PASS
IT security requirements	ASE_REQ.1	PASS
Explicitly stated IT security requirements	ASE_SRE.1	PASS
TOE summary specification	ASE_TSS.1	PASS
Configuration management	CC Class ACM	PASS
Partial CM automation	ACM_AUT.1	PASS
Generation support and acceptance procedures	ACM_CAP.4	PASS
Problem tracking CM coverage	ACM_SCP.2	PASS
Delivery and operation	CC Class ADO	PASS
Detection of modification	ADO_DEL.2	PASS
Generation log	ADO_IGS.2	PASS
Development	CC Class ADV	PASS
Fully defined external interfaces	ADV_FSP.2	PASS
Security enforcing high-level design	ADV_HLD.2	PASS
Implementation of the TSF	ADV_IMP.2	PASS
Descriptive low-level design	ADV_LLD.1	PASS
Informal correspondence demonstration	ADV_RCR.1	PASS
Informal TOE security policy model	ADV_SPM.1	PASS
Guidance documents	CC Class AGD	PASS
Administrator guidance	AGD_ADM.1	PASS
User guidance	AGD_USR.1	PASS
Life cycle support	CC Class ALC	PASS
Sufficiency of security measures	ALC_DVS.2	PASS
Developer defined life-cycle model	ALC_LCD.1	PASS
Well-defined development tools	ALC_TAT.1	PASS
Tests	CC Class ATE	PASS
Analysis of coverage	ATE_COV.2	PASS

Assurance classes and components		Verdict
Testing: low-level design	ATE_DPT.2	PASS
Functional testing	ATE_FUN.1	PASS
Independent testing - sample	ATE_IND.2	PASS
Vulnerability assessment	CC Class AVA	PASS
Analysis and testing for insecure states	AVA_MSU.3	PASS
Strength of TOE security function evaluation	AVA_SOF.1	PASS
Highly resistant	AVA_VLA.4	PASS

Table 13: Verdicts for the assurance components

According to the analysis of the impact of the changes [20] compared to BSI-DSZ-CC-0242-2004, the re-evaluation was concentrated on

- specific aspects of the classes ACM, ADO and ALC to cover the external initialisation process as well as ATE for testing of the TOE initialised by the external initialisation company
- specific aspects of the families ADV_LLD and ADV_IMP for the code shift from EEPROM to ROM.
- AVA as a confirmation of resistance to the attack potential considered.

The evaluation has shown that:

- the Security Functional Requirements specified for the TOE are Common Criteria Part 2 extended
- the TOE provides the functionality according to Appendix 10 of Annex 1B of Regulation (EC) no. 1360/2002 [8] and stated more precisely in the document JIL Security Evaluation and Certification of Digital Tachographs [9]
- the assurance of the TOE is Common Criteria Part 3 conformant, EAL4 augmented by ADO_IGS.2, ADV_IMP.2, ALC_DVS.2, ATE_DPT.2, AVA_MSU.3 and AVA_VLA.4
- the assurance of the TOE is equivalent to ITSEC [10] E3 high as required by Appendix 10 of Annex 1B of Regulation (EC) no. 1360/2002 [8]
- the TOE fulfils the claimed strength of function SOF-high for the functions as outlined in chapter 1.3. Therefore the scheme interpretations AIS 20, and AIS 26 (see [4]) were used. The rating of the strength of functions does not include the cryptoalgorithms suitable for encryption and decryption (see BSIG Section 4, Para. 3, Clause 2).
- The TOE is conformant to PP/9911 [13] and BSI-PP-0002-2001 [12].
- specific tests required by Appendix 9 of the EU Tachograph Card Commission Regulation [8] are fulfilled (see Annex A of this report).

The underlying hardware had been successfully reassessed by TÜV Informationstechnik GmbH.

The results of the evaluation are only applicable to the TCOS Tachograph Card Version 1.0, Release 2. The validity can be extended to new versions and releases of the product, provided the sponsor applies for re-certification of the modified product, in accordance with the procedural requirements, and the evaluation of the modified product does not reveal any security deficiencies.

10 Comments/Recommendations

The guidance documentation (refer to chapter 6) contains necessary information about the secure usage of the TOE. Additionally, for secure usage of the TOE the fulfilment of the assumptions about the environment in the Security Target [7] and the Security Target as a whole has to be taken into account. Therefore a user/administrator has to follow the guidance in these documents. (see also chapter 1.6 and chapter 4 of this part of the report).

Resulting from the evaluation the following assumptions are of relevance for the operation of the TOE:

- The user of a workshop card has to convince himself before using his PIN authentication code, that no manipulation was performed on tapping the transmission line between the workshop card and the card accepting device (vehicle unit).
- The certification authorities (CA) and the Root-CA acting within the Tachograph PKI-system have to ensure, that omitting a validity check based on the validity date for a certificate issued by them, does not affect the security of the Tachograph-PKI.

11 Annexes

Annex A: Functional Tests according to Appendix 9 of Annex I (B) of Council Regulation (EEC) No. 1360/2002

Annex B: Evaluation results regarding the development and production environment.

For these annexes please refer to part D of this report.

12 Security Target

For the purpose of publishing, the Security Target [7] of the Target of Evaluation (TOE) is provided within a separate document. It is a sanitised version (by editorial changes only) of the complete Security Target [6] used for the evaluation performed.

13 Definitions

13.1 Acronyms

APDU	Application Protocol Data Unit
BSI	Bundesamt für Sicherheit in der Informationstechnik / Federal Office for Information Security
CC	Common Criteria for IT Security Evaluation
CEM	Common Methodology for IT Security Evaluation
DES	Data Encryption Standard; symmetric block cipher algorithm
DFA	Differential Fault Analysis
DOC	Document
DPA	Differential Power Analysis
EAL	Evaluation Assurance Level
EEPROM	Electronically Erasable Programmable Read Only Memory
ES	Embedded Software
ETR	Evaluation Technical Report
IC	Integrated Circuit
IT	Information Technology
ITSEF	Information Technology Security Evaluation Facility
JIL	Joint Interpretation Library
MMU	Memory Management Unit
OS	Operating System
PIN	Personal Identification Number
PP	Protection Profile
PW	Password
RAM	Random Access Memory
RNG	Random Number Generator
ROM	Read Only Memory
RSA	Rivest-Shamir-Adleman Algorithm
SF	Security Function
SFP	Security Function Policy
SFR	Security Functional Requirement
SOF	Strength of Function
SPA	Simple Power Analysis
ST	Security Target
TOE	Target of Evaluation
Triple-DES	Symmetric block cipher algorithm based on the DES
TSC	TSF Scope of Control

TSF	TOE Security Functions
TSP	TOE Security Policy
TSS	TOE Summary Specification
VU	Vehicle Unit

13.2 Glossary

Augmentation - The addition of one or more assurance component(s) from CC Part 3 to an EAL or assurance package.

Extension - The addition to an ST or PP of functional requirements not contained in part 2 and/or assurance requirements not contained in part 3 of the CC.

Formal - Expressed in a restricted syntax language with defined semantics based on well-established mathematical concepts.

Informal - Expressed in natural language.

Object - An entity within the TSC that contains or receives information and upon which subjects perform operations.

Protection Profile - An implementation-independent set of security requirements for a category of TOEs that meet specific consumer needs.

Security Function - A part or parts of the TOE that have to be relied upon for enforcing a closely related subset of the rules from the TSP.

Security Target - A set of security requirements and specifications to be used as the basis for evaluation of an identified TOE.

Semiformal - Expressed in a restricted syntax language with defined semantics.

Strength of Function - A qualification of a TOE security function expressing the minimum efforts assumed necessary to defeat its expected security behaviour by directly attacking its underlying security mechanisms.

SOF-basic - A level of the TOE strength of function where analysis shows that the function provides adequate protection against casual breach of TOE security by attackers possessing a low attack potential.

SOF-medium - A level of the TOE strength of function where analysis shows that the function provides adequate protection against straightforward or intentional breach of TOE security by attackers possessing a moderate attack potential.

SOF-high - A level of the TOE strength of function where analysis shows that the function provides adequate protection against deliberately planned or organised breach of TOE security by attackers possessing a high attack potential.

Subject - An entity within the TSC that causes operations to be performed.

Target of Evaluation - An IT product or system and its associated administrator and user guidance documentation that is the subject of an evaluation.

TOE Security Functions - A set consisting of all hardware, software, and firmware of the TOE that must be relied upon for the correct enforcement of the TSP.

TOE Security Policy - A set of rules that regulate how assets are managed, protected and distributed within a TOE.

TSF Scope of Control - The set of interactions that can occur with or within a TOE and are subject to the rules of the TSP.

14 Bibliography

[1] Common Criteria for Information Technology Security Evaluation, Version 2.1, August 1999

[2] Common Methodology for Information Technology Security Evaluation (CEM), Part 1, Version 0.6; Part 2: Evaluation Methodology, Version 1.0, August 1999

[3] BSI certification: Procedural Description (BSI 7125, Version 5.1, January 1998)

[4] Application Notes and Interpretations of the Scheme (AIS), e.g.

AIS 20: Functionality classes and evaluation methodology for deterministic random number generators AIS 20, Version 1, 2 December, 1999

AIS 25 for: CC-Supporting Document: The application of CC to Integrated Circuits, Version 2, July 2002

AIS 26 for: CC-Supporting Document: Application of Attack Potential to Smartcards, Version 2, August 2002

AIS 32: Use of the international approved CC Final Interpretations into the German Certification Scheme

AIS 35 for: CC-Supporting Document: ST-lite, Version 1.1, July 2002

AIS 36 for: CC-Supporting Documents: ETR-lite for Composition, Version 1.1, July 2002 and
ETR-lite for composition: Annex A Composite smartcard evaluation: Recommended best practice, Version 1.2, March 2002

[5] German IT Security Certificates (BSI 7148, BSI 7149), periodically updated list published also on the BSI Web-site

[6] Specification of the Security Target TCOS Tachograph Card, Version 1.12, 25 June 2004, T-Systems International GmbH, T-Telesec, BSI-DSZ-CC-0272 (confidential)

[7] Specification of the Security Target TCOS Tachograph Card, Version 1.12, 25 June 2004, T-Systems International GmbH, T-Telesec, BSI-DSZ-CC-0272 (public version, only editorial changes from [6])

[8] Annex 1B of Commission Regulation (EC) No.1360/2002 on recording equipment in road transport: Requirements for Construction, Testing, Installation and Inspection (in: Official Journal of the European Communities, L 207 / 1 ff.), 05.08.2002, Commission of the European Communities

Appendix 2 of Annex I (B) of Council Regulation (EEC) No. 1360/2002 – Tachograph Cards Specification

Appendix 7 of Annex I (B) of Council Regulation (EEC) No. 1360/2002 - Data downloading protocols

Appendix 9 of Annex I (B) of Council Regulation (EEC) No. 1360/2002 – Type Approval – List of Minimum Required Tests

Appendix 10 of Annex I (B) of Council Regulation (EEC) No. 1360/2002 - Generic Security Targets

Appendix 11 of Annex I (B) of Council Regulation (EEC) No. 1360/2002 - Common Security Mechanisms

[9] Joint Interpretation Library (JIL) - Security Evaluation and Certification of Digital Tachographs, Version 1.12, June 2003, JIL Working Group (BSI, CESG, DCSSI, NLNCSA)

[10] Information Technology Security Evaluation Criteria (ITSEC), CEC, Version 1.2, June 1991.

[11] Technischer Evaluierungsbericht (ETR), CC Evaluierung der TCOS Tachograph Karte, 16 July 2004, Version 1, TÜV Informationstechnik GmbH (confidential document)

[12] Smart Card IC Platform Protection Profile, Version 1.0, July 2001, registered at the German Certification Body under number BSI-PP-0002-2001

[13] Smart Card Integrated Circuit With Embedded Software Protection Profile - version 2.0 - issue June 99. Registered at French certification body under the number PP/9911.

[14] Smart Card Integrated Circuit Protection Profile - version 2.0 - issue September 1998. Registered at French certification body under the number PP/9806.

[15] Administratorhandbuch TCOS Tachograph Card, Version 1.03, T-Systems International GmbH, T-Telesec, 6 July 2004

[16] Benutzerhandbuch TCOS Tachograph Card, Version 1.02, T-Systems International GmbH, T-Telesec, 6 July 2004

[17] Log-files zu einem beispielhaften Personalisierungsablauf, T-Systems International GmbH, T-Telesec, 14. April 2004

[18] Certification Report, BSI-DSZ-CC-0223-2003 for Infineon Smart Card IC (Security Controller) SLE66CX322P with RSA 2048 / m1484a24, m1484a27 and m1484b14 from Infineon Technologies AG, 7 October 2003, Bundesamt für Sicherheit in der Informationstechnik

[19] Infineon Technologies AG, Security and Chipcard ICs, SLE66CX322P with RSA 2048 / m1484a23, Security Target, Version 1.0.5, 06 May 2002

[20] Änderungsanzeige zur evaluierten Version TCOS Tachograph Card, 19.05.2004, Version 0.5, T-Systems International GmbH, T-Telesec (confidential document)

This page is intentionally left blank.

C Excerpts from the Criteria

CC Part 1:

Caveats on evaluation results (chapter 5.4) / **Final Interpretation 008**

The conformance result indicates the source of the collection of requirements that is met by a TOE or PP that passes its evaluation. This conformance result is presented with respect to Part 2 (functional requirements), Part 3 (assurance requirements) and, if applicable, to a pre-defined set of requirements (e.g., EAL, Protection Profile).

The conformance result consists of one of the following:

Part 2 conformant - A PP or TOE is Part 2 conformant if the functional requirements are based only upon functional components in Part 2

Part 2 extended - A PP or TOE is Part 2 extended if the functional requirements include functional components not in Part 2

plus one of the following:

Part 3 conformant - A PP or TOE is Part 3 conformant if the assurance requirements are based only upon assurance components in Part 3

Part 3 extended - A PP or TOE is Part 3 extended if the assurance requirements include assurance requirements not in Part 3.

Additionally, the conformance result may include a statement made with respect to sets of defined requirements, in which case it consists of one of the following:

***Package name* Conformant** - A PP or TOE is conformant to a pre-defined named functional and/or assurance package (e.g. EAL) if the requirements (functions or assurance) include all components in the packages listed as part of the conformance result.

***Package name* Augmented** - A PP or TOE is an augmentation of a pre-defined named functional and/or assurance package (e.g. EAL) if the requirements (functions or assurance) are a proper superset of all components in the packages listed as part of the conformance result.

Finally, the conformance result may also include a statement made with respect to Protection Profiles, in which case it includes the following:

***PP* Conformant** - A TOE meets specific PP(s), which are listed as part of the conformance result.

CC Part 3:

Assurance categorisation (chapter 2.5)

„The assurance classes, families, and the abbreviation for each family are shown in Table 2.1.

Assurance Class	Assurance Family	Abbreviated Name
Class ACM: Configuration management	CM automation	ACM_AUT
	CM capabilities	ACM_CAP
	CM scope	ACM_SCP
Class ADO: Delivery and operation	Delivery	ADO_DEL
	Installation, generation and start-up	ADO_IGS
Class ADV: Development	Functional specification	ADV_FSP
	High-level design	ADV_HLD
	Implementation representation	ADV_IMP
	TSF internals	ADV_INT
	Low-level design	ADV_LLD
	Representation correspondence	ADV_RCR
	Security policy modeling	ADV_SPM
Class AGD: Guidance documents	Administrator guidance	AGD_ADM
	User guidance	AGD_USR
Class ALC: Life cycle support	Development security	ALC_DVS
	Flaw remediation	ALC_FLR
	Life cycle definition	ALC_LCD
	Tools and techniques	ALC_TAT
Class ATE: Tests	Coverage	ATE_COV
	Depth	ATE_DPT
	Functional tests	ATE_FUN
	Independent testing	ATE_IND
Class AVA: Vulnerability assessment	Covert channel analysis	AVA_CCA
	Misuse	AVA_MSU
	Strength of TOE security functions	AVA_SOF
	Vulnerability analysis	AVA_VLA

Table 2.1 -Assurance family breakdown and mapping“

Evaluation assurance levels (chapter 6)

„The Evaluation Assurance Levels (EALs) provide an increasing scale that balances the level of assurance obtained with the cost and feasibility of acquiring that degree of assurance. The CC approach identifies the separate concepts of assurance in a TOE at the end of the evaluation, and of maintenance of that assurance during the operational use of the TOE.

It is important to note that not all families and components from Part 3 are included in the EALs. This is not to say that these do not provide meaningful and desirable assurances. Instead, it is expected that these families and components will be considered for augmentation of an EAL in those PPs and STs for which they provide utility.

Evaluation assurance level (EAL) overview (chapter 6.1)

Table 6.1 represents a summary of the EALs. The columns represent a hierarchically ordered set of EALs, while the rows represent assurance families. Each number in the resulting matrix identifies a specific assurance component where applicable.

As outlined in the next section, seven hierarchically ordered evaluation assurance levels are defined in the CC for the rating of a TOE's assurance. They are hierarchically ordered inasmuch as each EAL represents more assurance than all lower EALs. The increase in assurance from EAL to EAL is accomplished by *substitution* of a hierarchically higher assurance component from the same assurance family (i.e. increasing rigour, scope, and/or depth) and from the *addition* of assurance components from other assurance families (i.e. adding new requirements).

These EALs consist of an appropriate combination of assurance components as described in chapter 2 of this Part 3. More precisely, each EAL includes no more than one component of each assurance family and all assurance dependencies of every component are addressed.

While the EALs are defined in the CC, it is possible to represent other combinations of assurance. Specifically, the notion of "augmentation" allows the addition of assurance components (from assurance families not already included in the EAL) or the substitution of assurance components (with another hierarchically higher assurance component in the same assurance family) to an EAL. Of the assurance constructs defined in the CC, only EALs may be augmented. The notion of an "EAL minus a constituent assurance component" is not recognised by the CC as a valid claim. Augmentation carries with it the obligation on the part of the claimant to justify the utility and added value of the added assurance component to the EAL. An EAL may also be extended with explicitly stated assurance requirements.

Assurance Class	Assurance Family	Assurance Components by Evaluation Assurance Level						
		EAL1	EAL2	EAL3	EAL4	EAL5	EAL6	EAL7
Configuration management	ACM_AUT				1	1	2	2
	ACM_CAP	1	2	3	4	4	5	5
	ACM_SCP			1	2	3	3	3
Delivery and operation	ADO_DEL		1	1	2	2	2	3
	ADO_IGS	1	1	1	1	1	1	1
Development	ADV_FSP	1	1	1	2	3	3	4
	ADV_HLD		1	2	2	3	4	5
	ADV_IMP				1	2	3	3
	ADV_INT					1	2	3
	ADV_LLD				1	1	2	2
	ADV_RCR	1	1	1	1	2	2	3
	ADV_SPM				1	3	3	3
Guidance documents	AGD_ADM	1	1	1	1	1	1	1
	AGD_USR	1	1	1	1	1	1	1
Life cycle support	ALC_DVS			1	1	1	2	2
	ALC_FLR							
	ALC_LCD				1	2	2	3
	ALC_TAT				1	2	3	3
Tests	ATE_COV		1	2	2	2	3	3
	ATE_DPT			1	1	2	2	3
	ATE_FUN		1	1	1	1	2	2
	ATE_IND	1	2	2	2	2	2	3
Vulnerability assessment	AVA_CCA					1	2	2
	AVA_MSU			1	2	2	3	3
	AVA_SOF		1	1	1	1	1	1
	AVA_VLA		1	1	2	3	4	4

Table 6.1 - Evaluation assurance level summary"

Evaluation assurance level 1 (EAL1) - functionally tested (chapter 6.2.1)

„Objectives

EAL1 is applicable where some confidence in correct operation is required, but the threats to security are not viewed as serious. It will be of value where independent assurance is required to support the contention that due care has been exercised with respect to the protection of personal or similar information.

EAL1 provides an evaluation of the TOE as made available to the customer, including independent testing against a specification, and an examination of the guidance documentation provided. It is intended that an EAL1 evaluation could be successfully conducted without assistance from the developer of the TOE, and for minimal outlay.

An evaluation at this level should provide evidence that the TOE functions in a manner consistent with its documentation, and that it provides useful protection against identified threats."

Evaluation assurance level 2 (EAL2) - structurally tested (chapter 6.2.2)

„Objectives

EAL2 requires the co-operation of the developer in terms of the delivery of design information and test results, but should not demand more effort on the part of the developer than is consistent with good commercial practice. As such it should not require a substantially increased investment of cost or time.

EAL2 is therefore applicable in those circumstances where developers or users require a low to moderate level of independently assured security in the absence of ready availability of the complete development record. Such a situation may arise when securing legacy systems, or where access to the developer may be limited."

Evaluation assurance level 3 (EAL3) - methodically tested and checked (chapter 6.2.3)

„Objectives

EAL3 permits a conscientious developer to gain maximum assurance from positive security engineering at the design stage without substantial alteration of existing sound development practices.

EAL3 is applicable in those circumstances where developers or users require a moderate level of independently assured security, and require a thorough investigation of the TOE and its development without substantial re-engineering."

Evaluation assurance level 4 (EAL4) - methodically designed, tested, and reviewed (chapter 6.2.4)

„Objectives

EAL4 permits a developer to gain maximum assurance from positive security engineering based on good commercial development practices which, though rigorous,

do not require substantial specialist knowledge, skills, and other resources. EAL4 is the highest level at which it is likely to be economically feasible to retrofit to an existing product line.

EAL4 is therefore applicable in those circumstances where developers or users require a moderate to high level of independently assured security in conventional commodity TOEs and are prepared to incur additional security-specific engineering costs."

Evaluation assurance level 5 (EAL5) - semiformally designed and tested (chapter 6.2.5)

„Objectives

EAL5 permits a developer to gain maximum assurance from security engineering based upon rigorous commercial development practices supported by moderate application of specialist security engineering techniques. Such a TOE will probably be designed and developed with the intent of achieving EAL5 assurance. It is likely that the additional costs attributable to the EAL5 requirements, relative to rigorous development without the application of specialised techniques, will not be large.

EAL5 is therefore applicable in those circumstances where developers or users require a high level of independently assured security in a planned development and require a rigorous development approach without incurring unreasonable costs attributable to specialist security engineering techniques."

Evaluation assurance level 6 (EAL6) - semiformally verified design and tested (chapter 6.2.6)

„Objectives

EAL6 permits developers to gain high assurance from application of security engineering techniques to a rigorous development environment in order to produce a premium TOE for protecting high value assets against significant risks.

EAL6 is therefore applicable to the development of security TOEs for application in high risk situations where the value of the protected assets justifies the additional costs."

Evaluation assurance level 7 (EAL7) - formally verified design and tested (chapter 6.2.7)

„Objectives

EAL7 is applicable to the development of security TOEs for application in extremely high risk situations and/or where the high value of the assets justifies the higher costs. Practical application of EAL7 is currently limited to TOEs with tightly focused security functionality that is amenable to extensive formal analysis."

Strength of TOE security functions (AVA_SOF) (chapter 14.3)

AVA_SOF Strength of TOE security functions

„Objectives

Even if a TOE security function cannot be bypassed, deactivated, or corrupted, it may still be possible to defeat it because there is a vulnerability in the concept of its underlying security mechanisms. For those functions a qualification of their security behaviour can be made using the results of a quantitative or statistical analysis of the security behaviour of these mechanisms and the effort required to overcome them. The qualification is made in the form of a strength of TOE security function claim."

Vulnerability analysis (AVA_VLA) (chapter 14.4)

AVA_VLA Vulnerability analysis

„Objectives

Vulnerability analysis is an assessment to determine whether vulnerabilities identified, during the evaluation of the construction and anticipated operation of the TOE or by other methods (e.g. by flaw hypotheses), could allow users to violate the TSP.

Vulnerability analysis deals with the threats that a user will be able to discover flaws that will allow unauthorised access to resources (e.g. data), allow the ability to interfere with or alter the TSF, or interfere with the authorised capabilities of other users."

„Application notes

A vulnerability analysis is performed by the developer in order to ascertain the presence of security vulnerabilities, and should consider at least the contents of all the TOE deliverables including the ST for the targeted evaluation assurance level. The developer is required to document the disposition of identified vulnerabilities to allow the evaluator to make use of that information if it is found useful as a support for the evaluator's independent vulnerability analysis."

„Independent vulnerability analysis goes beyond the vulnerabilities identified by the developer. The main intent of the evaluator analysis is to determine that the TOE is resistant to penetration attacks performed by an attacker possessing a low (for AVA_VLA.2), moderate (for AVA_VLA.3) or high (for AVA_VLA.4) attack potential."

This page is intentionally left blank.

D Annexes

List of annexes of this certification report

This page is intentionally left blank.

Annex A of Certification Report BSI-DSZ-CC-0272-2004:

Functional Tests according to Appendix 9 of Annex I (B) of Council Regulation (EEC) No. 1360/2002

In addition to the ordinary tasks of the Common Criteria evaluation at level EAL4+ (equivalent to ITSEC E3 high), functional tests according to Appendix 9 of the EU Tachograph Card Commission Regulation [8] have been performed.

The following list shows the results of these tests:

N°	Test	Description	Related requirements	Result
1	Administrative examination			
1.1	Docu-mentation	Correctness of documentation	-	**Confirmed**
4	Protocol tests			The evaluators have assured themselves in detail of the fact that the functional tests have been performed successfully.
4.1	ATR	Check that the ATR is compliant.	ISO/IEC 7816-3 TCS 304, 307, 308	**Confirmed**
4.2	T=0	Check that T=0 protocol is compliant.	ISO/IEC 7816-3 TCS 302, 303, 305	**Confirmed**
4.3	PTS	Check that the PTS command is compliant by setting T=1 from T=0.	ISO/IEC 7816-3 TCS 309 to 311	**Confirmed**
4.4	T=1	Check that T=1 protocol is compliant.	ISO/IEC 7816-3 TCS 303, / 306	**Confirmed**
5	Card Structure			
5.1		Test that the file structure of the card is compliant by checking the presence of the mandatory files in the card and their Access Conditions.	TCS 312 TCS 400*, 401, 402, 403*, 404, 405*, 406, 407, 408*, 409, 410*, 411, 412, 413*, 414, 415*, 416, 417, 418*, 419	**Confirmed**

N°	Test	Description	Related requirements	Result
6	Functional tests			
6.1	Normal Processing	Test at least once each allowed usage of each command (ex: test the UPDATE BINARY command with CLA = '00', CLA = '0C' and with different P1,P2 and Lc parameters). Check that the operations have actually been performed in the card (ex: by reading the file the command has been performed on).	TCS 313 to TCS 379	**Confirmed**
6.2	Error Messages	Test at least once each error message (as specified in Appendix 2) for each command. Test at least once every generic error (except '6400' integrity errors checked during security certification).		**Confirmed**

Annex B of Certification Report BSI-DSZ-CC-0272-2004

Evaluation results regarding development and production environment

The IT product, *TCOS Tachograph Card Version 1.0, Release 2* (Target of Evaluation, TOE) has been evaluated at an accredited and licensed/ approved evaluation facility using the Common Methodology for IT Security Evaluation, Part 1 Version 0.6, Part 2 Version 1.0, extended by advice of the Certification Body for components beyond EAL4 and smart card specific guidance, for conformance to the Common Criteria for IT Security Evaluation, Version 2.1 (ISO/IEC15408: 1999) and including final interpretations for compliance with Common Criteria Version 2.2 and Common Methodology Part 2, Version 2.2.

As a result of the TOE certification, dated 22 July 2004, the following results regarding the development and production environment apply. The Common Criteria assurance requirements

- **ACM – Configuration management (i.e. ACM_AUT.1, ACM_CAP.4, ACM_SCP.2),**
- **ADO – Delivery and operation (i.e. ADO_DEL.2, ADO_IGS.2) and**
- **ALC – Life cycle support (i.e. ALC_DVS.2, ALC_LCD.1, ALC_TAT.1),**

are fulfilled for the development and production sites of the TOE listed below ((a) – (c)):

(a) **T-Systems International GmbH, T-Telesec, Untere Industriestr. 20, 57250 Netphen (embedded software development)**

(b) **T-Systems International GmbH, T-Telesec Trust Center, 57076 Siegen (card initialisation site)**

(c) **Trüb AG, Hintere Bahnhofstrasse 12, CH-5001 Aarau, Switzerland (card initialisation site)**

For development and productions sites regarding the Infineon Smart Card Controller SLE66CX322P m1484 b14 refer to the certification report BSI-DSZ-CC-0223-2003.

For the sites listed above, the requirements have been specifically applied in accordance with the "Specification of the Security Target TCOS Tachograph Card, Version 1.12, 25 June 2004, T-Systems International GmbH, T-Telesec, BSI-DSZ-CC-0272" [7]. The evaluators verified, that the threats, policies and security objective for the life cycle phases 1 to 6.1 up to delivery at the end of phase 6.1 as stated in the TOE Security Target [7] are fulfilled by the procedures of these sites.

This page is intentionally left blank.

GUVERNUL ROMÂNIEI
OFICIUL ROMÂN
PENTRU DREPTURILE DE AUTOR

Calea Victoriei 118. Et. 4-5, 010093-Bucureşti, Sector 1
Tel/Fax: 021.317.50.70-80-90

office@orda.gov.ro, www.orda.ro

CERTIFICAT

de înregistrare în
REGISTRUL NAŢIONAL AL
PROGRAMELOR PENTRU CALCULATOR
Seria 571453BS Nr. 10532 din 07.08.2020

SC CERTSIGN SA cu sediul/domiciliul în BUCURESTI, Str. SOSEAUA OLTENITEI, Nr. 107A, Bl. CORP C1, Et. 1, Apt. CAM. 16, Judet/Sector SECTOR4, cod fiscal 18288250, a fost înregistrată urmare a cererii nr. 3305 din data de 29.07.2020 în Registrul Naţional al Programelor pentru Calculator şi desfăşoară activităţi de producere şi comercializare a programelor pentru calculator menţionate în Anexa I la prezentul certificat.

Firma de mai sus îşi desfăşoară activitatea la punctele de lucru şi spaţiile de depozitare menţionate în Anexa II la prezentul certificat.

Durata de valabilitate a certificatului de înregistrare în Registrul Naţional al Programelor pentru Calculator este de un an de zile de la data emiterii.

Mario-Lucian DE MEZZO
DIRECTOR GENERAL

S.C. CERTSIGN S.A. BUCUREŞTI - ROMÂNIA

GUVERNUL ROMÂNIEI
OFICIUL ROMÂN
PENTRU DREPTURILE DE AUTOR

Calea Victoriei 118, Et. 4-5, 010093-Bucureşti, Sector 1
Tel/Fax: 021.317.50.70-80-90

office@orda.gov.ro, www.orda.ro

ANEXA I *a Certificatului seria 571453BS Nr. 10532 din 07.08.2020 RNPC*

Programele înscrise în Registrul Naţional al Programelor pentru Calculator de

SC CERTSIGN SA

Programe producţie proprie

Nr. Crt.	Denumire program	Tip program
1	certSAFE	Aplicatie utilitara
2	Certsign Remote QSCD (PAPERLESS)	Aplicatie utilitara
3	clickSIGN pdf (exceptie Art. 30, Ref. 1, alin. 1)	Aplicatie utilitara
4	emailerSAFE SE	Aplicatie utilitara
5	gateSAFE	Aplicatie utilitara
6	MASH	Aplicatie utilitara
7	persoSAFE	Aplicatie utilitara
8	persoSAFE G2	Aplicatie utilitara
9	RSS (Paperless)	Aplicatie utilitara
10	SERVICIU DE POSTA ELECTRONICA SECURIZATA NEREPUDIABILA CU VALOARE LEGALA – SPENS	Aplicatie utilitara
11	shellSAFE	Aplicatie utilitara
12	Signing Service Application (SSA)	Aplicatie utilitara
13	SISTEM DE SEMNARE LA DISTANTA	Aplicatie utilitara
14	Sistem software de colectare si garantare de continut web	Aplicatie utilitara
15	SRSPIRIM	Aplicatie utilitara. Program exceptat
16	tachoSAFE (exceptie Art. 30, Ref. 1, alin. 1)	Aplicatie utilitara
17	tachoSAFE-CA Gen 2	Aplicatie utilitara
18	Trust4Mobile Enterprise	Aplicatie utilitara

GUVERNUL ROMÂNIEI
OFICIUL ROMÂN
PENTRU DREPTURILE DE AUTOR

Calea Victoriei 118, Et. 4-5, 010093-București, Sector 1
Tel/Fax: 021.317.50.70-80-90

office@orda.gov.ro, www.orda.ro

ANEXA I *a Certificatului seria 571453BS Nr. 10532 din 07.08.2020 RNPC*

Programele înscrise în Registrul Național al Programelor pentru Calculator de

SC CERTSIGN SA

19	WebSigner	Aplicatie utilitara
20	Paperless flowSIGN	Aplicatie utilitara
21	Paperless webSIGN	Aplicatie utilitara
22	Paperless vToken	Aplicatie utilitara
23	Paperless Mobile	Aplicatie utilitara
24	Paperless Authenticator	Aplicatie utilitara

Programe distribuite / comercializate

Nr. Crt.	Denumire program	Producator	Tip program
1	persoSAFE G2	SC CERTSIGN SA	Aplicatie utilitara
2	RSS (Paperless)	SC CERTSIGN SA	Aplicatie utilitara
3	Signing Service Application (SSA)	SC CERTSIGN SA	Aplicatie utilitara
4	SISTEM DE SEMNARE LA DISTANTA	SC CERTSIGN SA	Aplicatie utilitara
5	tachoSAFE-CA Gen 2	SC CERTSIGN SA	Aplicatie utilitara
6	WebSigner	SC CERTSIGN SA	Aplicatie utilitara
7	Paperless flowSIGN	SC CERTSIGN SA	Aplicatie utilitara
8	Paperless webSIGN	SC CERTSIGN SA	Aplicatie utilitara
9	Paperless vToken	SC CERTSIGN SA	Aplicatie utilitara
10	Paperless Mobile	SC CERTSIGN SA	Aplicatie utilitara

GUVERNUL ROMÂNIEI
OFICIUL ROMÂN
PENTRU DREPTURILE DE AUTOR

Calea Victoriei 118, Et. 4-5, 010093-Bucureşti, Sector 1
Tel/Fax: 021.317.50.70-80-90

office@orda.gov.ro, www.orda.ro

ANEXA I *a Certificatului seria 571453BS Nr. 10532 din 07.08.2020 RNPC*

Programele înscrise în Registrul Naţional al Programelor pentru Calculator de

SC CERTSIGN SA

11	Paperless Authenticator	SC CERTSIGN SA	Aplicatie utilitara

Mario-Lucian DE MEZZO
DIRECTOR GENERAL

Darius MARIN
DIRECTOR D.R.G.C.

GUVERNUL ROMÂNIEI
OFICIUL ROMÂN
PENTRU DREPTURILE DE AUTOR

Calea Victoriei 118, Et. 4-5, 010093-București, Sector 1; Tel/Fax: 021.317.50.70-80-90
office@orda.gov.ro, www.orda.ro

Anexa II

a Certificatului Seria 571453BS Nr. 10532 din 07.08.2020 RNPC

Punctele de lucru şi spaţiile de depozitare ale:

SC CERTSIGN SA

Puncte de lucru

Nr. Crt.	Localitate	Strada	Numar	Bloc	Apartament	Judet/Sector
1	BUCURESTI	B-DUL TIMISOARA	5A			SECTOR6
2	BUCURESTI	SOS. OLTENITEI	107A	CORP C1	CAM. 16	SECTOR4

Mario-Lucian DE MEZZO
DIRECTOR GENERAL

Darius MARIN
DIRECTOR D.R.G.C.

DRGC/SRN/2ex/II.A.a.3.

INSTITUTUL NAŢIONAL DE CERCETARE, DEZVOLTARE
ŞI ÎNCERCĂRI PENTRU ELECTROTEHNICĂ
I C M E T CRAIOVA
DIVIZIA ÎNALTĂ TENSIUNE

accredited for TESTING

Laboratorul de Încercări de Joasă şi Înaltă Tensiune
200746 CRAIOVA, B-dul Decebal Nr.118A, ROMÂNIA
Certificat de înmatriculare: J16/312/1999; Cod de înregistrare fiscala RO3871599
Telefon: + 40 0351 404888, 404889; Fax: + 40 0351 404890
www.icmet.ro ; E-mail: market@icmet.ro

RAPORT DE ÎNCERCĂRI
Nr. 46715 / 28.02.2019

1. CLIENT:	**SC CERTSIGN SA** **B-dul Tudor Vladimirescu, 050881, sector 5, Bucureşti, România**
2. PRODUCĂTOR:	**UTI GRUP** **Şoseaua Olteniţei, nr 107-111A, 041303, sector 4, Bucureşti, România**
3. PRODUS ÎNCERCAT:	**Container ecranat model: nowave™ N00-360X240/TB**
4. STANDARD DE REFERINŢĂ:	**IEEE Std. 299: 2006**
5. ÎNCERCĂRI EFECTUATE:	**I. Măsurarea eficienţei ecranării electromagnetice**
6. DATA ÎNCERCĂRILOR:	**21.02.2019**
7. REZULTATUL ÎNCERCĂRII:	**Se comunică la punctul 5, pagina 3**

Raportul conţine 6 pagini şi este editat în 2 exemplare; exemplarul 1 rămâne în laborator, iar exemplarul 2 se transmite clientului

ŞEF DIT – MANAGER TEHNIC,
Ing. Ion BURCIU

ICMET DIVIZIA DE ÎNALTĂ TENSIUNE CRAIOVA

ŞEF COLECTIV ÎNCERCĂRI,
Ing. Ion BADEA

S.C. CERTSIGN S.A. 2/8 BUCUREŞTI - ROMÂNIA

AVERTISMENTE:

a. ***Rezultatele încercărilor se referă numai la produsul încercat.***
b. ***Publicarea sau reproducerea conţinutului acestui report în orice altă formă, exceptând fotocopierea completă, nu este permisă fără aprobarea Diviziei din care face parte laboratorul.***
c. ***Toate semnăturile din prezentul report sunt în original***

CUPRINS

1. IDENTIFICAREA PRODUSULUI ÎNCERCAT (EUT)

Denumire:	Container ecranat
Tip:	N00-360X240/TB
Serie de fabricaţie / an:	002394
Contract:	-
Comanda încercării:	23741 / 10.12.2018

2. CARACTERISTICILE TEHNICE STABILITE DE PRODUCĂTOR

Dimensiune cameră:	3600 x 2400 x 2250 (L x l x h) mm
Dimensiuni uşă:	760 x 1900 (l x h) mm
Grosimea peretelui (la uşă):	53 mm

2.1 Locaţia echipamentului încercat

Bulevardul Tudor Vladimirescu nr. 29A Bucureşti

2.2 Frecvenţa de rezonanţă

75,12 MHz

2.3 Criterii de performanţă

Valorile eficienţei ecranării (atenuarea camerei) nu trebuie să fie mai mici decât valorile impuse de client. Aceste valori sunt prezentate în tabelul de mai jos:

Domeniul de frecvenţă	Eficienţa ecranării [dB]
9 KHz ÷ 4 GHz	55

3. STANDARDELE DE BAZĂ APLICATE

IEEE Std. 299: 2006

4. PROGRAMUL MĂSURĂRILOR

	Măsurarea	Frecvenţa	Limita
I	Măsurarea eficienţei ecranării în domeniul 9 kHz ÷ 20 MHz	15 kHz, 150 kHz, 15 MHz	55 dB
II	Măsurarea eficienţei ecranării în domeniul 20 MHz ÷ 300 MHz	90 MHz, 200 MHz	55 dB
III	Măsurarea eficienţei ecranării în domeniul 300 MHz ÷ 4 GHz	800 MHz, 1.5 GHz, 2.05 GHz	55 dB

5. REZUMATUL REZULTATELOR MĂSURĂRILOR ŞI RESPONSABILII DE ÎNCERCARE

5.1 Rezultatul măsurărilor

	Încercarea	Pagina	Rezultat	Responsabil încercare	Semnătura
I	Măsurarea eficienţei ecranării în domeniul 9 kHz ÷ 20 MHz	4	Eficienţa ecranării mai mare de 55 dB	Ing. Paul Nicoleanu	
II	Măsurarea eficienţei ecranării în domeniul 20 MHz ÷ 300 MHz	6	Eficienţa ecranării mai mare de 55 dB	Ing. Paul Nicoleanu	
III	Măsurarea eficienţei ecranării în domeniul 300 MHz ÷ 4 GHz	8	Eficienţa ecranării mai mare de 55 dB	Ing. Paul Nicoleanu	

6. PARTICIPANŢI LA ÎNCERCARE (DIN PARTEA CLIENTULUI)

Bogdan Ispas

S.C. CERTSIGN S.A. CERTSIGN 2/8

7. DESCRIEREA ÎNCERCĂRILOR ŞI PREZENTAREA REZULTATELOR

7.1 Măsurarea eficienţei ecranării în domeniul 9 kHz ÷ 4 GHz

7.1.1 Măsurarea eficienţei ecranării în domeniul 9 kHz ÷ 20 MHz

Informaţii generale asupra încercării:

Responsabil încercare:	Ing. Paul Nicoleanu
Data încercării:	21.02.2019
Standard de referinţă:	IEEE Std. 299: 2006, punctul 5.6

Echipamente folosite:

Descriere	Producător	Tip	Seria
Generator de semnal	Rohde & Schwarz, Germania	SMY 02	826856/037
Receptor de perturbaţii electromagnetice	Messelektronik Berlin Germania	SMV 42	007
Antenă cadru activă	ETS-Lindgren, SUA	EMCO 6507	00066144
Antenă cadru pasivă	ETS-Lindgren, SUA	EMCO 6509	00069084

Condiţiile atmosferice:

Parametrul	Valoarea impusă	Valoarea măsurată
Temperatura:	5 °C ÷ 40 °C	16,5 °C
Presiunea atmosferică:	-	955 mbar
Umiditatea relativă:	-	48,6 %

Planul de încercare:

Amplasamentul de încercare:	Conform figurilor 1 şi 2 din IEEE Std. 299
Poziţia antenelor:	Orizontală şi verticală – vezi figura 1
Frecvenţele de măsurare:	15 kHz, 150 kHz, 15 MHz
Detectorul receptorului:	Valoare de vârf
Timpul de măsurare / frecvenţă:	1 sec
Lărgimea de bandă:	9 kHz
Zona verificată:	Uşa camerei ecranate

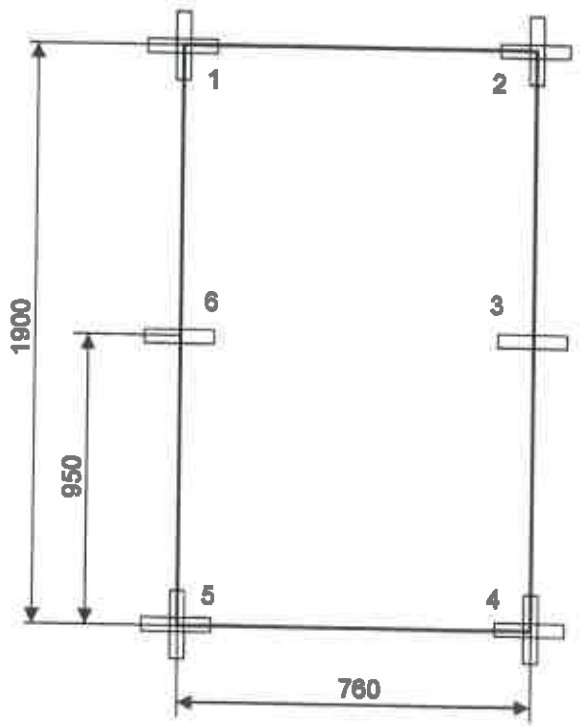


Fig. 1 – Punctele de verificare a eficienţei ecranării în jurul uşii

Modul de lucru
Antenele de emisie şi de recepţie au fost amplasate coplanar, conform figurilor 1 şi 2 din standardul IEEE Std 299 la înălţimea de 1100 mm în poziţie orizontală şi verticală.

Distanţa dintre antena de emisie şi antena de recepţie a fost de 653 mm (300 mm + 53 mm + 300 mm).
S-a realizat o măsurare a nivelului de referinţă cu antenele amplasate faţă în faţă, apoi cu acelaşi parametri ai generatorului de semnal (acelaşi nivel ca la măsurarea nivelului de referinţă) s-a efectuat o măsurare cu antena de recepţie poziţionată în camera ecranată şi antena de emisie în exteriorul camerei ecranate.
Cele două antene au fost poziţionate, pe rând, coliniar în dreptul punctelor specificate în figura 1.

Eficienţa ecranării (atenuarea camerei ecranate) a fost calculată cu formula:
$EE(dB) = N_1(dB\mu A/m) - N_2(dB\mu A/m)$ unde:
EE = Eficienţa ecranării
N_1 = Nivelul de referinţă (măsurat în aer, cu antenele faţă în faţă)
N_2 = Nivelul măsurat (cu antena de emisie în exteriorul şi antena de recepţie în interiorul camerei ecranate)

Rezultatele măsurării eficienţei ecranării electromagnetice în domeniul 9 kHz ÷ 20 MHz

Punctul de măsură	Polarizarea	Frecvenţa MHz	H referinţă dBµA/m	H măsurat dBµA/m	Eficienţa ecranării dB	Limita dB
1	Orizontală	0,015	102,3	42,7	59,6	55
		0,150	98,2	42,5	55,7	55
		15,000	88,7	17,7	71,0	55
	Verticală	0,015	97,7	41,9	55,8	55
		0,150	93,7	38,2	55,5	55
		15,000	85,9	27,7	58,2	55
2	Orizontală	0,015	102,3	45,3	57,0	55
		0,150	98,2	42,6	55,6	55
		15,000	88,7	11,2	77,5	55
	Verticală	0,015	97,7	41,2	56,5	55
		0,150	93,7	38,2	55,5	55
		15,000	85,9	12,2	73,7	55
3	Orizontală	0,015	102,3	45,1	57,2	55
		0,150	98,2	42,8	55,4	55
		15,000	88,7	16,6	72,1	55
4	Orizontală	0,015	102,3	46,8	55,5	55
		0,150	98,2	42,4	55,8	55
		15,000	88,7	17,7	71,0	55
	Verticală	0,015	97,7	42,2	55,5	55
		0,150	93,7	38,4	55,3	55
		15,000	85,9	13,9	72,0	55
5	Orizontală	0,015	102,3	45,9	56,4	55
		0,150	98,2	42,5	55,7	55
		15,000	88,7	25,8	62,9	55
	Verticală	0,015	97,7	42,2	55,5	55
		0,150	93,7	38,6	55,1	55
		15,000	85,9	28,2	57,7	55
6	Orizontală	0,015	102,3	47,1	55,2	55
		0,150	98,2	42,8	55,4	55
		15,000	88,7	18,3	70,4	55

7.1.2 Măsurarea eficienţei ecranării în domeniul 20 MHz ÷ 300 MHz

Informaţii generale asupra încercării:

Responsabil încercare:	Ing. Paul Nicoleanu
Data încercării:	21.02.2019
Standard de referinţă:	IEEE Std. 299: 2006, punctul 5.7

Echipamente folosite:

Descriere	Producător	Tip	Seria
Generator de semnal	Rohde & Schwarz, Germania	SMY 02	826856/037
Receptor de perturbaţii electromagnetice	Messelektronik Berlin Germania	SMV 42	007
Antenă biconică	A.H. Systems, SUA	SAS 545	423
Antenă biconică	A.H. Systems, SUA	SAS 545	424
Antenă dipol	Schwarzbeck Mess-Elektronik Germania	VHAP	1102
Antenă dipol	Schwarzbeck Mess-Elektronik Germania	VHAP	1103

Condiţiile atmosferice:

Parametrul	Valoarea impusă	Valoarea măsurată
Temperatura:	5 °C ÷ 40 °C	16,5 °C
Presiunea atmosferică:	-	955 mbar
Umiditatea relativă:	-	48,6 %

Planul de încercare:

Amplasamentul de încercare:	Conform figurilor 3 şi 4 din IEEE Std. 299
Poziţia antenelor:	Orizontală şi verticală – vezi figura 2
Frecvenţele de măsurare:	90 MHz, 200 MHz
Detectorul receptorului:	Valoare de vârf
Timpul de măsurare / frecvenţă:	1 sec
Lărgimea de bandă:	120 kHz
Zona verificată:	Peretele cu uşa camerei ecranate

Modul de lucru

Antenele de emisie şi de recepţie au fost amplasate la înălţimea de 1100 mm în poziţie orizontală şi verticală. În tabel s-au trecut valorile corespunzătoare poziţiei în care s-a obţinut atenuarea minimă.
Distanţa dintre antena de emisie şi antena de recepţie a fost de 2053 mm (1700 mm + 53 mm + 300 mm), conform figurii 2.
Eficienţa ecranării (atenuarea camerei ecranate) a fost calculată cu formula:
$EE(dB) = N_1(dB\mu V/m) - N_2(dB\mu V/m)$ unde:
EE = Eficienţa ecranării
N_1 = Nivelul de referinţă (măsurat în aer, cu antenele faţă în faţă)
N_2 = Nivelul măsurat (cu antena de emisie în exteriorul şi antena de recepţie în interiorul camerei ecranate)

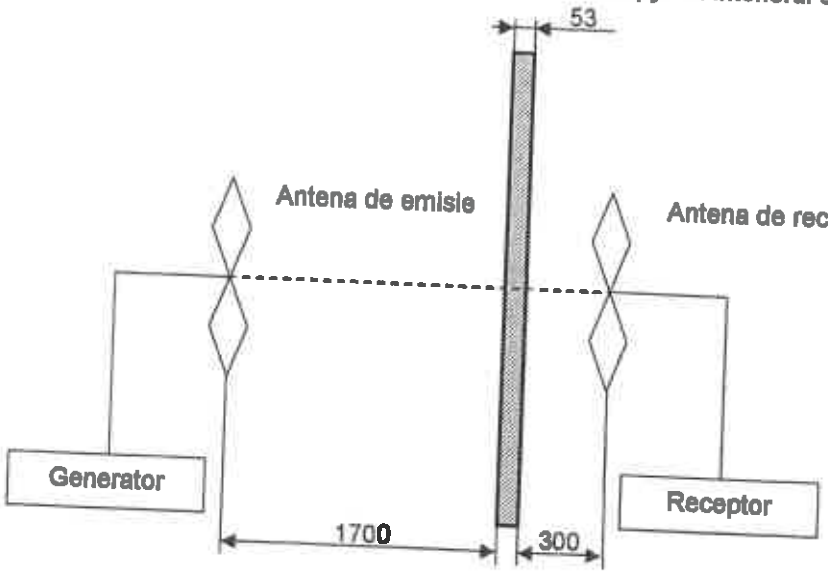


Fig. 2 – Amplasamentul de măsurare a eficienţei ecranării pe peretele cu uşa

S-a realizat o măsurare a nivelului de referinţă cu antenele amplasate faţă în faţă, apoi cu acelaşi parametri ai generatorului de semnal (aceeaşi putere ca la măsurarea nivelului de referinţă) s-a efectuat o măsurare cu antena de recepţie poziţionată în camera ecranată şi antena de emisie în exteriorul camerei ecranate.
Antena de recepţie a fost mutată în interiorul camerei ecranate, pe întreg peretele camerei ecranate, la distanţa de 300 mm faţă de perete, pentru a se obţine un nivel maxim recepţionat.
Cele două antene au fost poziţionate, pe rând atât în polarizare orizontală cât şi verticală.
Rezultatele măsurării eficienţei ecranării electromagnetice, în domeniul de frecvenţă de la 20 MHz până la 300 MHz, sunt prezentate în tabelul următor:

Rezultatele măsurării eficienţei ecranării electromagnetice în domeniul 20 MHz ÷ 300 MHz

Polarizarea	Frecvenţa MHz	E referinţă dBµV/m	E măsurat dBµV/m	Eficienţa ecranării dB	Limita dB
Orizontală	90	97,3	28,2	69,1	55
	200	93,2	22,1	71,1	55
Verticală	90	93,1	25,0	68,1	55
	200	95,7	26,5	69,5	55

7.1.3 Măsurarea eficienţei ecranării în domeniul 300 MHz ÷ 4 GHz

Informaţii generale asupra încercării:

Responsabil încercare:	Ing. Paul Nicoleanu
Data încercării:	21.02.2019
Standard de referinţă:	IEEE Std. 299: 2006, punctul 5.8

Echipamente folosite:

Descriere	Producător	Tip	Seria
Generator de semnal	Rohde & Schwarz, Germania	SMY 02	826856/037
Receptor de perturbaţii electromagnetice	Messelektronik Berlin Germania	SMV 42	007
Antenă dipol	Schwarzbeck Mess-Elektronik Germania	VHAP	1102
Antenă dipol	Schwarzbeck Mess-Elektronik Germania	VHAP	1103
Antenă horn	RF Spin Cehia	DRH-18E	070701A18E
Antenă horn	RF Spin Cehia	DRH-18E	070702A18E

Condiţiile atmosferice:

Parametrul	Valoarea impusă	Valoarea măsurată
Temperatura:	5 °C ÷ 40 °C	16,5 °C
Presiunea atmosferică:	-	995 mbar
Umiditatea relativă:	-	48,6 %

Planul de încercare:

Amplasamentul de încercare:	Conform figurilor 3 şi 4 din IEEE Std. 299
Poziţia antenelor:	Orizontală şi verticală – vezi figura 2
Frecvenţele de măsurare:	800 MHz, 1.5 GHz, 2.05 GHz
Detectorul receptorului:	Valoare de vârf
Timpul de măsurare / frecvenţă:	1 sec
Lărgimea de bandă:	120 kHz
Zona verificată:	Peretele cu uşa camerei ecranate

Modul de lucru
Antenele de emisie şi de recepţie au fost amplasate la înălţimea de 1100 mm în poziţie orizontală şi verticală.
Distanţa dintre antena de emisie şi antena de recepţie a fost de 2053 mm (1700 mm + 53 mm + 300 mm), conform figurii 2.
În tabel s-au trecut valorile corespunzătoare poziţiei în care s-a obţinut atenuarea minimă.

Eficienţa ecranării (atenuarea camerei ecranate) a fost calculată cu formula:
$EE(dB) = N_1(dB\mu V/m) - N_2(dB\mu V/m)$ unde:
EE = Eficienţa ecranării
N_1 = Nivelul de referinţă (măsurat în aer, cu antenele faţă în faţă)
N_2 = Nivelul măsurat (cu antena de emisie în exteriorul şi antena de recepţie în interiorul camerei ecranate)

S-a realizat o măsurare a nivelului de referinţă cu antenele amplasate faţă în faţă, apoi cu aceiaşi parametri ai generatorului de semnal (aceeaşi putere ca la măsurarea nivelului de referinţă) s-a efectuat o măsurare cu antena de recepţie poziţionată în camera ecranată şi antena de emisie în exteriorul camerei ecranate. Antena de recepţie a fost mutată în interiorul camerei ecranate, pe întreg peretele camerei ecranate, la distanţa de 300 mm faţă de perete, pentru a se obţine un nivel maxim recepţionat. Cele două antene au fost poziţionate, pe rând atât în polarizare orizontală cât şi verticală.
Rezultatele măsurării eficienţei ecranării electromagnetice, în domeniul de frecvenţă de la 300 MHz până la 4 GHz, sunt prezentate în tabelul următor:

Rezultatele măsurării eficienţei ecranării electromagnetice în domeniul 300 MHz ÷ 4 GHz

Polarizarea	Frecvenţa MHz	E referinţă dBµV/m	E măsurat dBµV/m	Eficienţa ecranării dB	Limita dB
Orizontală	800	82,3	26,1	56,2	55
	1500	92,3	25,6	66,7	55
	2050	91,8	23,8	68,0	55
Verticală	800	78,2	22,1	56,1	55
	1500	94,3	32,1	62,2	55
	2050	92,3	19,2	73,1	55

DAP-PL-2519.00

ID Card Laboratory

Test laboratory accredited by DAP Deutsches Akkreditierungssystem Prüfwesen GmbH in accordance with the standard DIN EN ISO/IEC 17025 (2005). The accreditation is valid for the tests listed in the certificate.

Contact:

Diana Szegedi
Tel. +49 89. 43 182 - 251
szegedi@fogra.org

2010-10-29

Test report

Digital copy of a test report by Fogra. In cases of doubt only the original written test report is binding.

Order No. (Fogra):	24509
Issued:	2010-10-29
Fogra Expert:	Diana Szegedi
No. of pages :	19 pages
Client:	Trüb AG Herr Siegfried Hintere Bahnhofstraße 12 CH 5001 Aarau
Date of order:	2010-09-08
Type of cards:	PCS-C-ID1-01A/MDA_eTG/TP97172
Cards received:	2010-10-08

Fogra
Forschungsgesellschaft
Druck e.V.

Streitfeldstraße 19
D-81673 München

Tel. +49 89. 431 82 - 0
Fax +49 89. 431 82 - 100

www.fogra.org
info@fogra.org

Sitz der Gesellschaft ist
München, Deutschland

Vereinsregistergericht
München, Vereins-
registernr. 4909
Steuernr. 143/215/00707
VAT-Nr. DE 129 514 828

Geschäftsführer:
Dr. Eduard Neufeld

Dresdner Bank München
BLZ 700 800 00
Konto 308 566 100
BIC DRES DE FF 700
IBAN DE31 7008 0000 0308 5661 00

Order No. (Fogra): 24509

Client: Trüb AG

Type of sample: PCS-C-ID1-01A/MDA_eTG/TP97172

Summary of test results:

Code	Description of test	Standard of test method	No. of samples tested	Complies with requirements of test standard	yes	no
DEL I06	Delamination Driver Card	ISO/IEC 10373-1 (2006)	4	ISO/IEC 7810 (2003)	X	
DEL I06	Delamination Company Card	ISO/IEC 10373-1 (2006)	4	ISO/IEC 7810 (2003)	X	
DEL I06	Delamination Workshop Card	ISO/IEC 10373-1 (2006)	4	ISO/IEC 7810 (2003)	X	
DEL I06	Delamination Control Card	ISO/IEC 10373-1 (2006)	4	ISO/IEC 7810 (2003)	X	
LIE K06	Light fastness Driver Card	PRfGHIC*	5	PRfGHIC*	X	
LIE K06	Light fastness Company Card	PRfGHIC*	5	PRfGHIC*	X	
LIE K06	Light fastness Workshop Card	PRfGHIC*	5	PRfGHIC*	X	
LIE K06	Light fastness Control Card	PRfGHIC*	5	PRfGHIC*	X	

* PRfGHIC: Physical requirements for the German health insurance card

Order No. (Fogra):	24509
Client:	Trüb AG
Type of sample:	PCS-C-ID1-01A/MDA_eTG/TP97172

Remarks:

The test results exclusively refer to the tested samples. The samples submitted to Fogra had been selected by the client. According to the client the samples have been manufactured with the final layout and production process.
Detailed test reports for each performed test are added as appendices to this summarizing test report.
The ID Card Laboratory is not accredited in order to perform tests which are marked by a blackened code. The processing of the order and the monitoring of the test equipment is nevertheless done in compliance to the accredited quality management system.

Fogra
Forschungsgesellschaft Druck e.V.

Arne Müller

Diana Szegedi

DAP-PL-2519.00

Appendix: DEL I06

Order No. (Fogra):	24509
Issued:	2010-10-29
Client:	Trüb AG
Type of sample:	PCS-C-ID1-01A/MDA_eTG/TP97172
Date of testing:	2010-10-26 until 2010-10-27

Description of test: Delamination Driver Card

Standard of test method:	ISO/IEC 10373-1 (2006)
Standard of requirements:	ISO/IEC 7810 (2003)

Complies with requirements:

☒ **yes**

☐ **no**

Appendix: DEL I06

Order No. (Fogra): 24509

Issued: 2010-10-29

Client: Trüb AG

Test results and evaluation of each sample:

Sample no.	Type of sample	Test Section	Peel strength in N/cm	Evaluation
A 1	Driver Card	1 FS	> 3,5 *	X ok
		3 BS	> 3,5 *	☐ fault
A 2	Driver Card	2 FS	> 3,5 *	X ok
		4 BS	> 3,5 *	☐ fault
A 3	Driver Card	3 FS	> 3,5 *	X ok
		1 BS	> 3,5 *	☐ fault
A 4	Driver Card	4 FS	> 3,5 *	X ok
		2 BS	> 3,5 *	☐ fault

Remarks:

* No delamination possible without destruction of the cards.

FS = front side of the card
BS = back side of the card (contact chip)

Card A 1 shows delaminations in the area of the flag (front side of the card, left upper corner) during the preparation for the measurement. These delaminations are not measurable according to ISO/IEC 10373-1.

Appendix: DEL I06

Order No. (Fogra):	24509
Issued:	2010-10-29
Client:	Trüb AG
Type of sample:	PCS-C-ID1-01A/MDA_eTG/TP97172
Date of testing:	2010-10-26 until 2010-10-27

Description of test: Delamination Company Card

Standard of test method:	ISO/IEC 10373-1 (2006)
Standard of requirements:	ISO/IEC 7810 (2003)

Complies with requirements:

☒ **yes**

☐ **no**

Appendix: DEL I06

Order No. (Fogra): 24509

Issued: 2010-10-29

Client: Trüb AG

Test results and evaluation of each sample:

Sample no.	Type of sample	Test Section	Peel strength in N/cm	Evaluation
B 1	Company Card	1 FS	> 3,5 *	X ok
		3 BS	> 3,5 *	☐ fault
B 2	Company Card	2 FS	> 3,5 *	X ok
		4 BS	> 3,5 *	☐ fault
B 3	Company Card	3 FS	> 3,5 *	X ok
		1 BS	> 3,5 *	☐ fault
B 4	Company Card	4 FS	> 3,5 *	X ok
		2 BS	> 3,5 *	☐ fault

Remarks:

* No delamination possible without destruction of the cards.

FS = front side of the card
BS = back side of the card (contact chip)

Card B 1 shows delaminations in the area of the flag (front side of the card, left upper corner) during the preparation for the measurement. These delaminations are not measurable according to ISO/IEC 10373-1.

Appendix: DEL I06

Order No. (Fogra):	24509
Issued:	2010-10-29
Client:	Trüb AG
Type of sample:	PCS-C-ID1-01A/MDA_eTG/TP97172
Date of testing:	2010-10-26 until 2010-10-27

Description of test: Delamination Workshop Card

Standard of test method:	ISO/IEC 10373-1 (2006)
Standard of requirements:	ISO/IEC 7810 (2003)

Complies with requirements:

☒ yes

☐ no

Appendix: DEL I06

Order No. (Fogra): 24509

Issued: 2010-10-29

Client: Trüb AG

Test results and evaluation of each sample:

Sample no.	Type of sample	Test Section	Peel strength in N/cm	Evaluation
C 1	Workshop Card	1 FS	> 3,5 *	[X] ok
		3 BS	> 3,5 *	[ ] fault
C 2	Workshop Card	2 FS	> 3,5 *	[X] ok
		4 BS	> 3,5 *	[ ] fault
C 3	Workshop Card	3 FS	> 3,5 *	[X] ok
		1 BS	> 3,5 *	[ ] fault
C 4	Workshop Card	4 FS	> 3,5 *	[X] ok
		2 BS	> 3,5 *	[ ] fault

Remarks:

* No delamination possible without destruction of the cards.

FS = front side of the card
BS = back side of the card (contact chip)

Card C 1 shows delaminations in the area of the flag (front side of the card, left upper corner) during the preparation for the measurement. These delaminations are not measurable according to ISO/IEC 10373-1.

Appendix: DEL I06

Order No. (Fogra):	24509
Issued:	2010-10-29
Client:	Trüb AG
Type of sample:	PCS-C-ID1-01A/MDA_eTG/TP97172
Date of testing:	2010-10-26 until 2010-10-27

Description of test: Delamination Control Card

Standard of test method:	ISO/IEC 10373-1 (2006)
Standard of requirements:	ISO/IEC 7810 (2003)

Complies with requirements:

- [X] yes
- [ ] no

Appendix: DEL I06

Order No. (Fogra): 24509

Issued: 2010-10-29

Client: Trüb AG

Test results and evaluation of each sample:

Sample no.	Type of sample	Test Section	Peel strength in N/cm	Evaluation
D 1	Control Card	1 FS	> 3,5 *	X ok
		3 BS	> 3,5 *	☐ fault
D 2	Control Card	2 FS	> 3,5 *	X ok
		4 BS	> 3,5 *	☐ fault
D 3	Control Card	3 FS	> 3,5 *	X ok
		1 BS	> 3,5 *	☐ fault
D 4	Control Card	4 FS	> 3,5 *	X ok
		2 BS	> 3,5 *	☐ fault

Remarks:

* No delamination possible without destruction of the cards.

FS = front side of the card
BS = back side of the card (contact chip)

Card D 1 shows delaminations in the area of the flag (front side of the card, left upper corner) during the preparation for the measurement. These delaminations are not measurable according to ISO/IEC 10373-1.

DAP-PL-

Appendix: LIE K06

Order No. (Fogra):	24509
Issued:	2010-10-29
Client:	Trüb AG
Type of sample:	PCS-C-ID1-01A/MDA_eTG/TP97172
Date of testing:	2010-10-26 until 2010-10-29

Description of test: Light fastness Driver Card

Standard of test method: PRfGHIC*

Standard of requirements: PRfGHIC*

Complies with requirements: [X] yes

[ ] no

* PRfGHIC: Physical requirements for the German health insurance card

Appendix: LIE K06

Order No. (Fogra): 24509

Issued: 2010-10-29

Client: Trüb AG

Test results and evaluation of each card:

Card no.	Type of card	Inspection of the printed area after exposion to xenon arc light till grade 4 of the blue wool scale.	Evaluation
		front / back	
A 5	Driver Card	[X] / [ ]	[X] ok [ ] fault
A 6	Driver Card	[X] / [ ]	[X] ok [ ] fault
A 7	Driver Card	[ ] / [X]	[X] ok [ ] fault
A 8	Driver Card	[ ] / [X]	[X] ok [ ] fault
A 9	Driver Card	Card has not been exposed to xenon arc light; Card was used as sample for comparison.	

Remarks:

Exposure till grade 3 of BWS:
No visible change of the printing inks.
Barely visible decrease of the brightness of the UV-active elements.

Exposure till grade 4 of BWS:
No visible change of the printing inks.
Further slight decrease of the brightness of the UV-active elements.

S.C. CERTSIGN S.A. certSIGN 2/8

DAP-PL-

fogra

Appendix: LIE K06

Order No. (Fogra):	24509
Issued:	2010-10-29
Client:	Trüb AG
Type of sample:	PCS-C-ID1-01A/MDA_eTG/TP97172
Date of testing:	2010-10-26 until 2010-10-29

Description of test: Light fastness Company Card

Standard of test method: PRfGHIC*

Standard of requirements: PRfGHIC*

Complies with requirements: [X] yes

[ ] no

* PRfGHIC: Physical requirements for the German health insurance card

Appendix: LIE K06

Order No. (Fogra): 24509

Issued: 2010-10-29

Client: Trüb AG

Test results and evaluation of each card:

Card no.	Type of card	Inspection of the printed area after exposion to xenon arc light till grade 4 of the blue wool scale.	Evaluation
B 5	Company Card	front [X] back [ ]	[X] ok [ ] fault
B 6	Company Card	front [X] back [ ]	[X] ok [ ] fault
B 7	Company Card	front [ ] back [X]	[X] ok [ ] fault
B 8	Company Card	front [ ] back [X]	[X] ok [ ] fault
B 9	Company Card	Card has not been exposed to xenon arc light; Card was used as sample for comparison.	

Remarks:

Exposure till grade 3 of BWS:
No visible change of the printing inks.
Barely visible decrease of the brightness of the UV-active elements.

Exposure till grade 4 of BWS:
No visible change of the printing inks.
Further slight decrease of the brightness of the UV-active elements.

DAP-PL-

fogra

Appendix: LIE K06

Order No. (Fogra):	24509
Issued:	2010-10-29
Client:	Trüb AG
Type of sample:	PCS-C-ID1-01A/MDA_eTG/TP97172
Date of testing:	2010-10-26 until 2010-10-29

Description of test: Light fastness Workshop Card

Standard of test method: PRfGHIC*

Standard of requirements: PRfGHIC*

Complies with requirements: [X] yes

[ ] no

* PRfGHIC: Physical requirements for the German health insurance card

S.C. CERTSIGN S.A.

Appendix: LIE K06

Order No. (Fogra): 24509

Issued: 2010-10-29

Client: Trüb AG

Test results and evaluation of each card:

Card no.	Type of card	Inspection of the printed area after exposion to xenon arc light till grade 4 of the blue wool scale. front / back	Evaluation
C 5	Workshop Card		[X] ok [ ] fault
C 6	Workshop Card		[X] ok [ ] fault
C 7	Workshop Card		[X] ok [ ] fault
C 8	Workshop Card		[X] ok [ ] fault
C 9	Workshop Card	Card has not been exposed to xenon arc light; Card was used as sample for comparison.	

Remarks:

Exposure till grade 3 of BWS:
No visible change of the printing inks.
Barely visible decrease of the brightness of the UV-active elements.

Exposure till grade 4 of BWS:
No visible change of the printing inks.
Further slight decrease of the brightness of the UV-active elements.

DAP-PL-

Appendix: LIE K06

Order No. (Fogra):	24509
Issued:	2010-10-29
Client:	Trüb AG
Type of sample:	PCS-C-ID1-01A/MDA_eTG/TP97172
Date of testing:	2010-10-26 until 2010-10-29

Description of test: Light fastness Control Card

Standard of test method: PRfGHIC*

Standard of requirements: PRfGHIC*

Complies with requirements: ☒ yes

☐ no

* PRfGHIC: Physical requirements for the German health insurance card

DAP-PL-

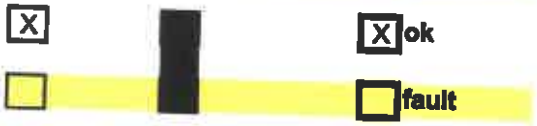
Appendix: LIE K06

Order No. (Fogra): 24509

Issued: 2010-10-29

Client: Trüb AG

Test results and evaluation of each card:

Card no.	Type of card	Inspection of the printed area after exposion to xenon arc light till grade 4 of the blue wool scale.	Evaluation
		front / back	
D 5	Control Card		[X] ok [ ] fault
D 6	Control Card		[X] ok [ ] fault
D 7	Control Card		[X] ok [ ] fault
D 8	Control Card		[X] ok [ ] fault
D 9	Control Card	Card has not been exposed to xenon arc light; Card was used as sample for comparison.	

Remarks:

Exposure till grade 3 of BWS:
No visible change of the printing inks.
Barely visible decrease of the brightness of the UV-active elements.

Exposure till grade 4 of BWS:
No visible change of the printing inks.
Further slight decrease of the brightness of the UV-active elements.

Operator economic
CERTSIGN S.A.

DECLARAŢIE PRIVIND MOSTRELE DE CARDURI

Subsemnatul, **Armand-Dragos ROPOT**, reprezentant împuternicit al **CERTSIGN S.A.**, în calitate de **ofertant**, la procedura de **Licitatie deschisa** pentru atribuirea contractului de achiziţie publică având ca obiect **„Cartele tahografice personalizate"**, Codul CPV 30162000-2, la data de **08.01.2021**, organizată de **Autoritatea Administrativă "Agenţia Naţională Transport Auto"**, declar pe propria răspundere că **ofertantul CERTSIGN S.A.** este în măsură să prezinte mostrele de carduri personalizate funcţionale, în cazul în care autoritatea contractantă le va solicita.

Ataşăm prezentei declaraţii, imaginile cu mostrele de carduri personalizate funcţionale, scrisorile însoţitoare ale cardurilor precum şi scrisoarea de PIN aferentă cardului de atelier.

Înţeleg ca în cazul în care această declaraţie nu este conformă cu realitatea sunt pasibil de încălcarea prevederilor legislaţiei penale privind falsul în declaraţii.

Data completării: 30.12.2020

Operator economic,

CERTSIGN S.A.
Semnat: _____ L.Ş.
Nume: Armand-Dragos ROPOT
În calitate de: Reprezentant împuternicit

CARTELA CONDUCĂTORULUI AUTO
DRIVER CARD
REPUBLICA MOLDOVA

MD

1. Popescu
2. Ilie
3. 23.04.1971
4a. 20.12.2020 4b. 19.12.2025
4c. ANTA
5a. 123456789
5b. 0001010000LFF000
6.
7.
8. MD,Bender,49 Let Pobedi,65,Ap.1

CARTELA DE ATELIER
WORKSHOP CARD
REPUBLICA MOLDOVA

MD

1. East-Test SRL
2. Popescu
3. Ilie
4a. 20.12.2020 4b. 19.12.2021
4c. ANTA
5b. 0002020[illegible]
7.
8. MD,Chisinau,Chisinau,3

CARTELA DE CONTROL
CONTROL CARD
REPUBLICA MOLDOVA

MD

1. ANTA
2. Popescu
3. Ilie
4a. 20.12.2020 4b. 19.12.2022
4c. ANTA
5b. 0003030000C1WO[illegible]
6.
7.
8. MD,Chisinau,Aleea Garii,6

CARTELA OPERATORULUI DE TRANSPORT
COMPANY CARD
REPUBLICA MOLDOVA

MD

1. ILIE TRANS S.R.L
2. Popescu
3. Ilie
4a. 20.12.2020 4b. 19.12.2025
4c. ANTA
5b. 0000404000G1Y100
7.
8. MD,Chisinau,N. Zelinski,6/1,Ap.3


e1
232
CARTELA CONDUCĂTORULUI AUTO
DRIVER CARD
1. Nume / Surname
2. Prenume / First name(s)
3. Data naşterii / Birth date
4a. Data eliberării / Date of start of validity of card
4b. Data expirării / Administrative end of validity date of card
4c. Autoritatea emitentă / Issuing authority
5a. Numărul permisului conducătorului / Driving licence number
5b. Numărul cartelei / Card number
6. Fotografie / Photograph
7. Semnătura / Signature
8. Adresa / Address
SPECIMEN
Please return to:
Ministerul Transporturilor şi Infrastructurii Drumurilor, Agenţia Naţională Transport Auto
Address: Republica Moldova, Chişinău, MD2001, St. Alexei Ciorl, Nr. 8


e1
209
CARTELA DE ATELIER
WORKSHOP CARD
1. Denumirea atelierului / Workshop Name
(2.) Name / Surname
(3.) Prenume / First name(s)
4a. Data eliberării / Date of issue
4b. Data expirării / Date of expiry
4c. Autoritatea emitentă / Issuing authority
5b. Numărul cartelei / Card Number
(7.) Semnătura / Signature
8. Adresa / Address
SPECIMEN
Please return to:
Ministerul Transporturilor şi Infrastructurii Drumurilor, Agenţia Naţională Transport Auto
Address: Republica Moldova, Chişinău, MD2068, St. Alexei Russo, Nr. 1


e1
209
CARTELA DE CONTROL
CONTROL CARD
1. Autoritatea de control / Control Body
(2.) Nume / Surname
(3.) Prenume / First name(s)
4a. Data eliberării / Date of issue
4b. Data expirării / Date of expiry
4c. Autoritatea emitentă / Issuing authority
5b. Numărul cartelei / Card number
(6.) Fotografie / Photograph
(7.) Semnătura / Signature
8. Adresa / Address
SPECIMEN
Please return to:
Ministerul Transporturilor şi Infrastructurii Drumurilor, Agenţia Naţională Transport Auto
Address: Republica Moldova, Chişinău, MD2068, St. Alexei Russo, Nr. 1


e1
209
CARTELA OPERATORULUI DE TRANSPORT
COMPANY CARD
1. Denumirea operatorului de transport / Company name
(2.) Nume / Surname
(3.) Prenume / First name(s)
4a. Data eliberării / Date of issue
4b. Data expirării / Date of expiry
4c. Autoritatea emitentă / Issuing authority
5a. Numărul cartelei / Card number
(7.) Semnătura / Signature
8. Adresa / Address
SPECIMEN
Please return to:
Ministerul Transporturilor şi Infrastructurii Drumurilor, Agenţia Naţională Transport Auto
Address: Republica Moldova, Chişinău, MD2068, St. Alexei Russo, Nr. 1


S.C. CERTSIGN S.A.
2/8

Republica Moldova
Ministerul Transporturilor şi Infrastructurii Drumurilor
Agenţia Naţională Transport Auto

certSIGN.

Data	**2020-12-21**
Expeditor	ANTA
Telefon	(+373 22) 32-09-60
Fax	(+373 22) 49-88-10
e-mail	tahodigital@gmail.com

Ilie Popescu
Ceucari 65, Bl.4, Ap.57

Chisinau
Raion , Republica Moldova

Prezenta scrisoare conţine PIN-ul pentru cartela dumneavoastră de atelier.
Acest cod este valid doar cu cartela corespunzătoare de atelier.

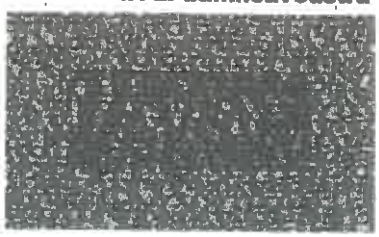
Pentru a preveni orice fel de abuz al PIN-ului, vă recomandăm să distrugeţi această scrisoare.
Codul trebuie scris şi păstrat într-un loc sigur şi separat de cartelă (de exemplu într-un seif).
Nu scrieţi niciodată codul pe cartela de atelier!

Acest număr PIN trebuie folosit numai cu cartela de atelier primită anterior.

Solicitant:	Ilie Popescu Chisinau Raion , Republica Moldova
Număr Cartelă:	00020200004YS201
Informaţii de contact:	Ministerul Transporturilor si Infrastructurii Drumurilor al Republicii Moldova, Agentia Nationala Transport Auto
Adresa:	Republica Moldova, Chisinau, MD2001, Str. Aleea Garii, Nr. 6
Telefon:	(+373 22) 32-09-60
Fax:	(+373 22) 49-88-10
e-mail:	tahodigital@gmail.com

AGENŢIA NAŢIONALĂ TRANSPORT AUTO împreună cu partenerul său, compania CERTSIGN din România, vă mulţumesc pentru încrederea acordată.

Numărul PIN al dumneavoastră



S.C. CERTSIGN S.A. BUCUREŞTI - R

certSIGN.

ANTA

Republica Moldova
Ministerul Transporturilor şi Infrastructurii Drumurilor
Agenţia Naţională Transport Auto

H_TMD002/1
WSC_0002/1

Data **2020-12-20**
Expeditor ANTA
Telefon (+373 22) 32-09-60
Fax (+373 22) 49-88-10
e-mail tachodigital@gmail.com

Ilie Popescu
Aleea Gării 6
MD2001 Chişinău
Republica Moldova

Număr cartelă: 00020200004YS201

Avem plăcerea de a vă înmâna cartela solicitată de dumneavoastră.

Ghidul de utilizare al acestei cartele se poate accesa pe internet la adresa http://cartelatahograf.arr.ro/ în cadrul secţiunii "Ghid Utilizare".

Reguli generale de folosire:
- utilizarea acestei cartele se va face conform normelor legale în vigoare;
- cartela este netransmisibilă; ea se va prezenta la solicitarea organelor de control abilitate conform normelor legale în vigoare;
- cartela este destinată exclusiv pentru autentificarea la dispozitivul tahograf digital;
- cartela se poate utiliza doar în perioada de valabilitate precizată pe aceasta; la sfârşitul perioadei de valabilitate se poate solicita o nouă cartelă la una din agenţiile ANTA;
- în cazul în care cartela se pierde, este furată sau se deteriorează, vă rugăm să vă prezentaţi la o agenţie ANTA pentru a anunţa incidentul şi pentru a solicita o nouă cartelă;

Dacă aveţi întrebări şi probleme legate de utilizarea cartelei vă rugăm să solicitaţi sprijinul personalului agenţiei ANTA de unde aţi primit cartela sau să scrieţi la adresa de mail: tachodigital@gmail.com

Agenţia Naţională Transport Auto împreună cu partenerul său, compania CERTSIGN din România, vă mulţumesc pentru încrederea acordată.

Informaţii de contact:
Ministerul Transporturilor şi Infrastructurii Drumurilor al Republicii Moldova,
Agenţia Naţională Transport Auto
Adresa: Republica Moldova, Chisinau, MD2001, Strada Aleea Garii, Nr. 6
Tel: (+373 22) 32-09-60, fax (+373 22) 49-88-10, e-mail: tachodigital@gmail.com

certSIGN.

ANTA

Republica Moldova
Ministerul Transporturilor şi Infrastructurii Drumurilor
Agenţia Naţională Transport Auto

H_TMD001/1
DRV_0001/1

Data **2020-12-20**
Expeditor ANTA
Telefon (+373 22) 32-09-60
Fax (+373 22) 49-88-10
e-mail tachodigital@gmail.com

Ilie Popescu
Aleea Gării 6
MD2001 Chişinău
Republica Moldova

Număr carteiă: 0001010000LFF000

Avem plăcerea de a vă înmâna cartela solicitată de dumneavoastră.

Ghidul de utilizare al acestei cartele se poate accesa pe internet la adresa http://cartelatahograf.arr.ro/ în cadrul secţiunii "Ghid Utilizare".

Reguli generale de folosire:
- utilizarea acestei cartele se va face conform normelor legale în vigoare;
- cartela este netransmisibilă; ea se va prezenta la solicitarea organelor de control abilitate conform normelor legale în vigoare;
- cartela este destinată exclusiv pentru autentificarea la dispozitivul tahograf digital;
- cartela se poate utiliza doar în perioada de valabilitate precizată pe aceasta; la sfârşitul perioadei de valabilitate se poate solicita o nouă carteiă la una din agenţiile ANTA;
- în cazul în care cartela se pierde, este furată sau se deteriorează, vă rugăm să vă prezentaţi la o agenţie ANTA pentru a anunţa incidentul şi pentru a solicita o nouă carteiă;

Dacă aveţi întrebări şi probleme legate de utilizarea cartelei vă rugăm să solicitaţi sprijinul personalului agenţiei ANTA de unde aţi primit cartela sau să scrieţi la adresa de mail: tachodigital@gmail.com

Agenţia Naţională Transport Auto împreună cu partenerul său, compania CERTSIGN din România, vă mulţumesc pentru încrederea acordată.

Informaţii de contact:
Ministerul Transporturilor şi Infrastructurii Drumurilor al Republicii Moldova,
Agenţia Naţională Transport Auto
Adresa: Republica Moldova, Chisinau, MD2001, Strada Aleea Garii, Nr. 6
Tel: (+373 22) 32-09-60, fax (+373 22) 49-88-10, e-mail: tachodigital@gmail.com

CERTSIGN S.A.
certSIGN

certSIGN.

ANTA

Republica Moldova
Ministerul Transporturilor şi Infrastructurii Drumurilor
Agenţia Naţională Transport Auto

H_TMD003/1
CTR_0003/1

Data **2020-12-20**
Expeditor ANTA
Telefon (+373 22) 32-09-60
Fax (+373 22) 49-88-10
e-mail tachodigital@gmail.com

Ilie Popescu
Aleea Gării 6
MD2001 Chişinău
Republica Moldova

Număr cartelă: 0003030000C1W000

Avem plăcerea de a vă înmâna cartela solicitată de dumneavoastră.

Ghidul de utilizare al acestei cartele se poate accesa pe internet la adresa http://cartelatahograf.arr.ro/ în cadrul secţiunii "Ghid Utilizare".

Reguli generale de folosire:
- utilizarea acestei cartele se va face conform normelor legale în vigoare;
- cartela este netransmisibilă; ea se va prezenta la solicitarea organelor de control abilitate conform normelor legale în vigoare;
- cartela este destinată exclusiv pentru autentificarea la dispozitivul tahograf digital;
- cartela se poate utiliza doar în perioada de valabilitate precizată pe aceasta; la sfârşitul perioadei de valabilitate se poate solicita o nouă cartelă la una din agenţiile ANTA;
- în cazul în care cartela se pierde, este furată sau se deteriorează, vă rugăm să vă prezentaţi la o agenţie ANTA pentru a anunţa incidentul şi pentru a solicita o nouă cartelă;

Dacă aveţi întrebări şi probleme legate de utilizarea cartelei vă rugăm să solicitaţi sprijinul personalului agenţiei ANTA de unde aţi primit cartela sau să scrieţi la adresa de mail: tachodigital@gmail.com

Agenţia Naţională Transport Auto împreună cu partenerul său, compania CERTSIGN din România, vă mulţumesc pentru încrederea acordată.

Informaţii de contact:
Ministerul Transporturilor şi Infrastructurii Drumurilor al Republicii Moldova,
Agenţia Naţională Transport Auto
Adresa: Republica Moldova, Chisinau, MD2001, Strada Aleea Garii, Nr. 6
Tel: (+373 22) 32-09-60, fax (+373 22) 49-88-10, e-mail: tachodigital@gmail.com

S.C. CERTSIGN S.A.
certSIGN
2/8

certSIGN.

ANTA

Republica Moldova
Ministerul Transporturilor şi Infrastructurii Drumurilor
Agenţia Naţională Transport Auto

H_TMD004/1
ENT_0004/1

Data 2020-12-20
Expeditor ANTA
Telefon (+373 22) 32-09-60
Fax (+373 22) 49-88-10
e-mail tachodigital@gmail.com

Ilie Popescu
Aleea Gării 6
MD2001 Chişinău
Republica Moldova

Număr cartelă: 0000404000G1Y100

Avem plăcerea de a vă înmâna cartela solicitată de dumneavoastră.

Ghidul de utilizare al acestei cartele se poate accesa pe internet la adresa http://cartelatahograf.arr.ro/ în cadrul secţiunii "Ghid Utilizare".

Reguli generale de folosire:
- utilizarea acestei cartele se va face conform normelor legale în vigoare;
- cartela este netransmisibilă; ea se va prezenta la solicitarea organelor de control abilitate conform normelor legale în vigoare;
- cartela este destinată exclusiv pentru autentificarea la dispozitivul tahograf digital;
- cartela se poate utiliza doar în perioada de valabilitate precizată pe aceasta; la sfârşitul perioadei de valabilitate se poate solicita o nouă cartelă la una din agenţiile ANTA;
- în cazul în care cartela se pierde, este furată sau se deteriorează, vă rugăm să vă prezentaţi la o agenţie ANTA pentru a anunţa incidentul şi pentru a solicita o nouă cartelă;

Dacă aveţi întrebări şi probleme legate de utilizarea cartelei vă rugăm să solicitaţi sprijinul personalului agenţiei ANTA de unde aţi primit cartela sau să scrieţi la adresa de mail: tachodigital@gmail.com

Agenţia Naţională Transport Auto împreună cu partenerul său, compania CERTSIGN din România, vă mulţumesc pentru încrederea acordată.

Informaţii de contact:
Ministerul Transporturilor şi Infrastructurii Drumurilor al Republicii Moldova,
Agenţia Naţională Transport Auto
Adresa: Republica Moldova, Chisinau, MD2001, Strada Aleea Garii, Nr. 6
Tel: (+373 22) 32-09-60, fax (+373 22) 49-88-10, e-mail: tachodigital@gmail.com

H_TMD004/1
ENT_0004/1

Ilie Popescu
Aleea Gării 6
MD2001 Chişinău
Republica Moldova

Număr cartelă: 0000404000G1Y100

AUTORITATEA ADMINISTRATIVĂ
Agenţia Naţională Transport Auto
Strada Aleea Gării, nr. 6
MD2001, Chişinău, Republica Moldova
Telefon: (+373 22) 73-35-75
Fax: (+373 22) 49-88-10
e-mail: secretariat@anta.gov.md
web: www.anta.gov.md

certSIGN SA
Şos. Olteniţei nr. 107A, sector 4, 041303,.Bucureşti, România
Telefon: (+40) 21 311 99 04
Fax: (+40) 21 311 99 05
e-mail: office@certsign.ro
web: www.certsign.ro

S.C. CERTSIGN S.A. BUCUREŞTI - ROMÂNIA

H_TMD003/1
CTR_0003/1

Ilie Popescu
Aleea Gării 6
MD2001 Chişinău
Republica Moldova

Număr cartelă: 0003030000C1W000

AUTORITATEA ADMINISTRATIVĂ
Agenţia Naţională Transport Auto
Strada Aleea Gării, nr. 6
MD2001, Chişinău, Republica Moldova
Telefon: (+373 22) 73-35-75
Fax: (+373 22) 49-88-10
e-mail: secretariat@anta.gov.md
web: www.anta.gov.md

certSIGN SA
Şos. Olteniţei nr. 107A, sector 4, 041303,.Bucureşti, România
Telefon: (+40) 21 311 99 04
Fax: (+40) 21 311 99 05
e-mail: office@certsign.ro
web: www.certsign.ro

H_TMD001/1
DRV_0001/1

Ilie Popescu
Aleea Gării 6
MD2001 Chişinău
Republica Moldova

Număr cartelă: 0001010000LFF000

AUTORITATEA ADMINISTRATIVĂ
Agenţia Naţională Transport Auto
Strada Aleea Gării, nr. 6
MD2001, Chişinău, Republica Moldova
Telefon: (+373 22) 73-35-75
Fax: (+373 22) 49-88-10
e-mail: secretariat@anta.gov.md
web: www.anta.gov.md

certSIGN SA
Şos. Olteniţei nr. 107A, sector 4, 041303,.Bucureşti, România
Telefon: (+40) 21 311 99 04
Fax: (+40) 21 311 99 05
e-mail: office@certsign.ro
web: www.certsign.ro

H_TMD002/1
WSC_0002/1

Ilie Popescu
Aleea Gării 6
MD2001 Chişinău
Republica Moldova

Număr cartelă: 00020200004YS201

AUTORITATEA ADMINISTRATIVĂ
Agenţia Naţională Transport Auto
Strada Aleea Gării, nr. 6
MD2001, Chişinău, Republica Moldova
Telefon: (+373 22) 73-35-75
Fax: (+373 22) 49-88-10
e-mail: secretariat@anta.gov.md
web: www.anta.gov.md

certSIGN SA
Şos. Olteniţei nr. 107A, sector 4, 041303,.Bucureşti, România
Telefon: (+40) 21 311 99 04
Fax: (+40) 21 311 99 05
e-mail: office@certsign.ro
web: www.certsign.ro

Ilie Popescu
Ceucari 65, Bl.4, Ap.57

Chisinau
Raion , Republica Moldova

AUTORITATEA ADMINISTRATIVĂ
Agenția Națională Transport Auto
Strada Aleea Gării, nr. 6
MD2001, Chișinău, Republica Moldova
Telefon: (+373 22) 73-35-75
Fax: (+373 22) 49-88-10
e-mail: secretariat@anta.gov.md
web: www.anta.gov.md

certSIGN SA
Șos. Olteniței nr. 107A, sector 4, 041303,.București, România
Telefon: (+40) 21 311 99 04
Fax: (+40) 21 311 99 05
e-mail: office@certsign.ro
web: www.certsign.ro