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

O.R.D.A. 467073BV

de înregistrare în
REGISTRUL NAŢIONAL AL
PROGRAMELOR PENTRU CALCULATOR
Seria 467073BV Nr. 13343 din 02.09.2025

SC CERTSIGN SA cu sediul/domiciliul în BUCURESTI, Str. SOSEAUA OLTENITEI, Nr. 107A, Bl. CORP C1, Et. 1, Apt. CAMERA 16, Judet/Sector SECTOR4, cod fiscal 18288250, a fost înregistrată urmare a cererii nr. 3511 din data de 28.08.2025 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.

Andrei-Simion IJAC
DIRECTOR GENERAL

S.C. CERTSIGN S.A. certSIGN 2/3 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 467073BV Nr. 13343 din 02.09.2025 RNPC*

Programele înscrise în Registrul Naţional al Programelor pentru Calculator de

SC CERTSIGN SA

Programe producţie proprie

Nr. Crt.	Denumire program	Tip program
1	BSA	Aplicatie utilitara
2	Canal securizat intre dispozitivele I/O si unitatea de procesare pentru extinderea securitatii software (SABOTORE)	Aplicatie utilitara
3	certSAFE	Aplicatie utilitara
4	certSAFE CA	Aplicatie utilitara
5	certSAFE OCSP	Aplicatie utilitara
6	certSAFE RA	Aplicatie utilitara
7	certSAFE TS	Aplicatie utilitara
8	certSAFE versiunea 3	Aplicatie utilitara
9	certSAFE(RootCA, RA/LRA, KRM, CMS, LDAP, CA, OCSP, RA, TS)	Aplicatie utilitara
10	certSIGN EIDAS Node Client	Aplicatie utilitara
11	Certsign Remote QSCD (PAPERLESS)	Aplicatie utilitara
12	CISRES	Aplicatie utilitara
13	c-itsSAFE	Aplicatie utilitara
14	clickSIGN pdf (exceptie Art. 30, Ref. 1, alin. 1)	Aplicatie utilitara
15	clickSIGN PDF Ultimate	Aplicatie utilitara
16	emailerSAFE SE	Aplicatie utilitara
17	ERRU Core	Aplicatie utilitara
18	gateSAFE	Aplicatie utilitara
19	MASH	Aplicatie utilitara
20	Paperless Authentication Service	Aplicatie utilitara
21	Paperless Authenticator	Aplicatie utilitara
22	Paperless flowSIGN	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 467073BV Nr. 13343 din 02.09.2025 RNPC*

Programele înscrise în Registrul Naţional al Programelor pentru Calculator de

SC CERTSIGN SA

23	Paperless Mobile	Aplicatie utilitara
24	Paperless QVSA	Aplicatie utilitara
25	Paperless SMS-Gateway	Aplicatie utilitara
26	Paperless vToken	Aplicatie utilitara
27	Paperless vToken for MacOS	Aplicatie utilitara
28	Paperless vToken for Windows	Aplicatie utilitara
29	Paperless webSIGN	Aplicatie utilitara
30	persoSAFE	Aplicatie utilitara
31	persoSAFE G2	Aplicatie utilitara
32	persoSAFE-PT	Aplicatie utilitara
33	RSS (Paperless)	Aplicatie utilitara
34	Servicii de atestare a identitatii in medii descentralizate bazate pe tehnologii de tip blockchain (IDBC)	Aplicatie utilitara
35	SERVICIU DE POSTA ELECTRONICA SECURIZATA NEREPUDIABILA CU VALOARE LEGALA - SPENS	Aplicatie utilitara
36	shellSAFE	Aplicatie utilitara
37	Signing Service Application (SSA)	Aplicatie utilitara
38	SISTEM DE SEMNARE LA DISTANTA	Aplicatie utilitara
39	Sistem LTPS	Aplicatie utilitara
40	Sistem software de colectare si garantare de continut web	Aplicatie utilitara
41	SRSPIRIM	Aplicatie utilitara
42	tachoSAFE BDA	Aplicatie utilitara
43	tachoSAFE BG-CIA v2	Aplicatie utilitara
44	tachoSAFE CA G1	Aplicatie utilitara
45	tachoSAFE-CA Gen 2	Aplicatie utilitara
46	tachoSAFE (exceptie Art. 30, Ref. 1, alin. 1)	Aplicatie utilitara

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 467073BV Nr. 13343 din 02.09.2025 RNPC*

Programele înscrise în Registrul Naţional al Programelor pentru Calculator de

SC CERTSIGN SA

47	tachoSAFE-CA Gen 2 Revocation Functionality	Aplicatie utilitara
48	tachoSAFE CSR v1	Aplicatie utilitara
49	tachoSAFE CY-CIA v2	Aplicatie utilitara
50	tachoSAFE MD-CIA v2	Aplicatie utilitara
51	tachoSAFE RO-ADR	Aplicatie utilitara
52	tachoSAFE RO-CIA v2	Aplicatie utilitara
53	tachoSAFE RO-CPP	Aplicatie utilitara
54	tachoSAFE SRB-CIA v2	Aplicatie utilitara
55	TachoSAFE TACHOnet v3	Aplicatie utilitara
56	tachoSAFE TJ-CIA v2	Aplicatie utilitara
57	tachoSAFE UA-CIA v2	Aplicatie utilitara
58	tachoSAFE UZ-CIA v2	Aplicatie utilitara
59	Trust4Mobile Enterprise	Aplicatie utilitara
60	Trust4Mobile Enterprise Bridge	Aplicatie utilitara
61	Trust4Mobile Enterprise Edition	Aplicatie utilitara
62	Trust4Mobile Enterprise Windows client	Aplicatie utilitara
63	Verifying Service Application (VSA)	Aplicatie utilitara
64	WebSigner	Aplicatie utilitara

Programe distribuite / comercializate

Nr. Crt.	Denumire program	Producator	Tip program
1	BSA	SC CERTSIGN SA	Aplicatie utilitara
2	Canal securizat intre dispozitivele I/O si unitatea de procesare pentru extinderea securitatii software (SABOTORE)	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 467073BV Nr. 13343 din 02.09.2025 RNPC*

Programele înscrise în Registrul Naţional al Programelor pentru Calculator de

SC CERTSIGN SA

3	certSAFE	SC CERTSIGN SA	Aplicatie utilitara
4	certSAFE CA	SC CERTSIGN SA	Aplicatie utilitara
5	certSAFE OCSP	SC CERTSIGN SA	Aplicatie utilitara
6	certSAFE RA	SC CERTSIGN SA	Aplicatie utilitara
7	certSAFE TS	SC CERTSIGN SA	Aplicatie utilitara
8	certSAFE versiunea 3	SC CERTSIGN SA	Aplicatie utilitara
9	certSAFE(RootCA, RA/LRA, KRM, CMS, LDAP, CA, OCSP, RA, TS)	SC CERTSIGN SA	Aplicatie utilitara
10	certSIGN EIDAS Node Client	SC CERTSIGN SA	Aplicatie utilitara
11	Certsign Remote QSCD (PAPERLESS)	SC CERTSIGN SA	Aplicatie utilitara
12	CISRES	SC CERTSIGN SA	Aplicatie utilitara
13	c-itsSAFE	SC CERTSIGN SA	Aplicatie utilitara
14	clickSIGN pdf (exceptie Art. 30, Ref. 1, alin. 1)	SC CERTSIGN SA	Aplicatie utilitara
15	clickSIGN PDF Ultimate	SC CERTSIGN SA	Aplicatie utilitara
16	emailerSAFE SE	SC CERTSIGN SA	Aplicatie utilitara
17	ERRU Core	SC CERTSIGN SA	Aplicatie utilitara
18	gateSAFE	SC CERTSIGN SA	Aplicatie utilitara
19	MASH	SC CERTSIGN SA	Aplicatie utilitara
20	Paperless Authentication Service	SC CERTSIGN SA	Aplicatie utilitara
21	Paperless Authenticator	SC CERTSIGN SA	Aplicatie utilitara
22	Paperless flowSIGN	SC CERTSIGN SA	Aplicatie utilitara
23	Paperless Mobile	SC CERTSIGN SA	Aplicatie utilitara
24	Paperless QVSA	SC CERTSIGN SA	Aplicatie utilitara
25	Paperless SMS-Gateway	SC CERTSIGN SA	Aplicatie utilitara
26	Paperless vToken	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 467073BV Nr. 13343 din 02.09.2025 RNPC*

Programele înscrise în Registrul Naţional al Programelor pentru Calculator de

SC CERTSIGN SA

27	Paperless vToken for MacOS	SC CERTSIGN SA	Aplicatie utilitara
28	Paperless vToken for Windows	SC CERTSIGN SA	Aplicatie utilitara
29	Paperless webSIGN	SC CERTSIGN SA	Aplicatie utilitara
30	persoSAFE	SC CERTSIGN SA	Aplicatie utilitara
31	persoSAFE G2	SC CERTSIGN SA	Aplicatie utilitara
32	persoSAFE-PT	SC CERTSIGN SA	Aplicatie utilitara
33	RSS (Paperless)	SC CERTSIGN SA	Aplicatie utilitara
34	Servicii de atestare a identitatii in medii descentralizate bazate pe tehnologii de tip blockchain (IDBC)	SC CERTSIGN SA	Aplicatie utilitara
35	SERVICIU DE POSTA ELECTRONICA SECURIZATA NEREPUDIABILA CU VALOARE LEGALA - SPENS	SC CERTSIGN SA	Aplicatie utilitara
36	shellSAFE	SC CERTSIGN SA	Aplicatie utilitara
37	Signing Service Application (SSA)	SC CERTSIGN SA	Aplicatie utilitara
38	SISTEM DE SEMNARE LA DISTANTA	SC CERTSIGN SA	Aplicatie utilitara
39	Sistem LTPS	SC CERTSIGN SA	Aplicatie utilitara
40	Sistem software de colectare si garantare de continut web	SC CERTSIGN SA	Aplicatie utilitara
41	SRSPIRIM	SC CERTSIGN SA	Aplicatie utilitara
42	tachoSAFE BDA	SC CERTSIGN SA	Aplicatie utilitara
43	tachoSAFE BG-CIA v2	SC CERTSIGN SA	Aplicatie utilitara
44	tachoSAFE CA G1	SC CERTSIGN SA	Aplicatie utilitara
45	tachoSAFE-CA Gen 2	SC CERTSIGN SA	Aplicatie utilitara
46	tachoSAFE (exceptie Art. 30, Ref. 1, alin. 1)	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 467073BV Nr. 13343 din 02.09.2025 RNPC*

Programele înscrise în Registrul Naţional al Programelor pentru Calculator de

SC CERTSIGN SA

47	tachoSAFE-CA Gen 2 Revocation Functionality	SC CERTSIGN SA	Aplicatie utilitara
48	tachoSAFE CSR v1	SC CERTSIGN SA	Aplicatie utilitara
49	tachoSAFE CY-CIA v2	SC CERTSIGN SA	Aplicatie utilitara
50	tachoSAFE MD-CIA v2	SC CERTSIGN SA	Aplicatie utilitara
51	tachoSAFE RO-ADR	SC CERTSIGN SA	Aplicatie utilitara
52	tachoSAFE RO-CIA v2	SC CERTSIGN SA	Aplicatie utilitara
53	tachoSAFE RO-CPP	SC CERTSIGN SA	Aplicatie utilitara
54	tachoSAFE SRB-CIA v2	SC CERTSIGN SA	Aplicatie utilitara
55	TachoSAFE TACHOnet v3	SC CERTSIGN SA	Aplicatie utilitara
56	tachoSAFE TJ-CIA v2	SC CERTSIGN SA	Aplicatie utilitara
57	tachoSAFE UA-CIA v2	SC CERTSIGN SA	Aplicatie utilitara
58	tachoSAFE UZ-CIA v2	SC CERTSIGN SA	Aplicatie utilitara
59	Trust4Mobile Enterprise	SC CERTSIGN SA	Aplicatie utilitara
60	Trust4Mobile Enterprise Bridge	SC CERTSIGN SA	Aplicatie utilitara
61	Trust4Mobile Enterprise Edition	SC CERTSIGN SA	Aplicatie utilitara
62	Trust4Mobile Enterprise Windows client	SC CERTSIGN SA	Aplicatie utilitara
63	Verifying Service Application (VSA)	SC CERTSIGN SA	Aplicatie utilitara
64	WebSigner	SC CERTSIGN SA	Aplicatie utilitara

Andrei-Simion IJAC
DIRECTOR GENERAL

Darius MARIN
DIRECTOR D.G.C.E.C.

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 II

a Certificatului Seria 467073BV Nr. 13343 din 02.09.2025 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	SOS. OLTENITEI	107A	CORP C1	CAM. 16	SECTOR4
2	BUCURESTI	BD. TUDOR VLADIMIRESCU	29A			SECTOR5

Andrei-Simion IJAC
DIRECTOR GENERAL

Darius MARIN
DIRECTOR D.G.C.E.C.

INSTITUTUL NAŢIONAL DE CERCETARE, DEZVOLTARE
ŞI ÎNCERCĂRI PENTRU ELECTROTEHNICĂ
I C M E T CRAIOVA
DIVIZIA ÎNALTĂ TENSIUNE

accredited for TESTING
SR EN ISO/CEI 17025:2005
ACCREDITATION CERTIFICATE
LI 1036

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 Vladimiresu, 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 8 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

AVERTISMENTE:

a. *Rezultatele încercărilor se referă numai la produsul încercat.*
b. *Publicarea sau reproducerea conţinutului acestui raport în orice altă formă, exceptând fotocopierea completă, nu este permisă fără aprobarea Diviziei din care face parte laboratorul.*
c. *Toate semnăturile din prezentul raport sunt în original*

certSIGN 2/8

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 București

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 BUCUREŞTI - ROMÂNIA

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 vărf
Timpul de măsurare / frecvenţă:	1 sec
Lărgimea de bandă:	9 kHz
Zona verificată:	Uşa camerei ecranate

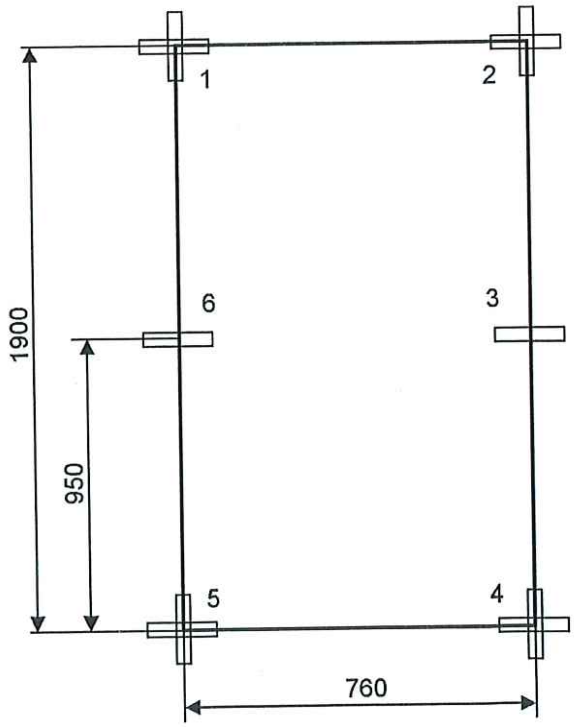

Fig. 1 – Punctele de verificare a eficienţei ecranării în jurul uşii

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 aceiaşi 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)

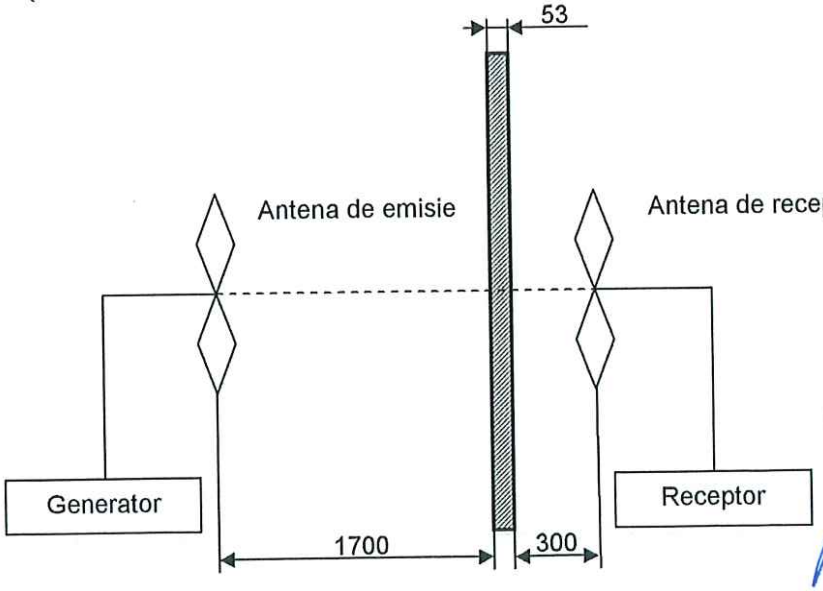

Fig. 2 – Amplasamentul de măsurare a eficienţei ecranării pe peretele cu uşa

S-a realizat o măsurare a nivelului de referinţă cu antenele amplasate faţă în faţă, apoi cu 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 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

RDW

Division Vehicle Regulation & Admission

THE NETHERLANDS

APPROVAL CERTIFICATE
FOR PRODUCTS IN ACCORDANCE WITH APPENDIX 1B

Name of competent administration : RDW

Communication concerning [1]:

- ☒ Approval
- ☐ Withdrawal of an approval

- ☐ Of a control device model
- ☐ Of a control device component [2]
- ☒ Of a driver card
- ☒ Of a workshop card
- ☒ Of a company card
- ☒ Of a inspector's card

with regard to the European agreement concerning the work of crews of vehicles engaged in international road transport (AETR) of 1 July 1970, consolidated version ECE-TRANS-SC1-2010 and that meets the requirements set out in Annex IA/IB to Council Regulation (EEC) No. 3821/85 of 20 December 1985.

Approval number : **e4*AETR*3821/85*0005*00**

1.	Manufacturing or commercial mark	: Tachograph G1 v1.6 cards for Moldova
2.	Name of model	: Tachograph G1 cards for Moldova Thales Digital Tachograph G1 v1.6 [Version 2.2.1.N]
3.	Name of manufacturer	: Thales DIS Finland OY
4.	Address of manufacturer	: Myllynkivenkuja 4 01620 Vantaa Finland
5.	Submitted for approval on	: 08 November 2024
6.	Test laboratory or laboratories	:
6.1	Test laboratory for functional certification	: UL TS B.V.
6.2	Test laboratory for security certification	: ANSSI
6.3	Test laboratory for interoperability certification	: DTLab
7.	Date and number of report	:

Type-approval Department

P.O. Box 777
2700 AT Zoetermeer
The Netherlands

Tel. + 31 79 345 83 02
E-mail typeapproval@rdw.nl
www.rdw.nl

Approval number: e4*AETR*3821/85*0005*00

7.1	Date and number of functional certificate	: 07 November 2024, RDW-AETR-0121197
7.2	Date and number of security certificate	: 16 August 2022, ANSSI-CC-2022138 15 December 2022, ANSSI-CC-2022/38-M01
7.3	Date and number of interoperability certificate	: 26 May 2023, JRC DTLab/A3-156/2023
8.	Date of approval	:
9.	Date of withdrawal of approval	: N/A
10.	Model(s) of component(s) of control device with which the component is intended to be used	: Not specified, any type approved Vehicle Unit compliant with Commision Regulation (EC) 1360/2002 and 2016/799
11.	Place	: Zoetermeer
12.	Date	: 03 December 2024
13.	Descriptive documents annexed	: TR_e4-AETR-382185-0005-01.pdf IF_e4-AETR-382185-0005-01.pdf
14.	Remarks ((including the affixing of seals if required)	: Item 6.1 and 7.1, certificate issued by RDW Item 6.2 and 7.2, certificate issued by ANSSI Item 6.3 and 7.3, certificate issued by JRC Interoperability tests with specific Tachograph G1 v1.6 are not performed by JRC. Instead interoperability certificate for Tachograph G2V2 is applied to demonstrate Tachograph G1 cards interoperability testing. The results are obtained during G2V2 interoperability tests, when the G2V2 cards have been inserted in G1 Vehicles Units and all required G1 functionality has been fully tested and certified by JRC. Further detail are provided by the issuer in: IF_e4-AETR-382185-0005-01.pdf, Tachograph G1 v1.6, Information, Moldova
	Signature	:

RDW

R. R. van der Spek

S.C. CERTSIGN S.A. CertSIGN 2/8 BUCURESTI - ROMANIA

(1) Tick the relevant boxes.
(2) Specify the component dealt with in the notification.

Bundesamt
für Sicherheit in der
Informationstechnik

Deutsches IT-Sicherheitszertifikat

erteilt vom Bundesamt für Sicherheit in der Informationstechnik

BSI-DSZ-CC-1107-V5-2024 (*)

IFX_CCI_00002Dh, 000039h, 00003Ah, 000044h, 000045h, 000046h, 000047h, 000048h, 000049h, 00004Ah, 00004Bh, 00004Ch, 00004Dh, 00004Eh design step T11 with firmware 80.306.16.0, 80.306.16.1 or 80.312.02.0, optional NRG™ SW 05.03.4097, optional HSL v3.52.9708, UMSLC lib v01.30.0564, optional SCL v2.15.000 or v2.11.003, optional ACL v3.35.001, v3.34.000, v3.33.003 or v3.02.000, optional RCL v1.10.007, optional HCL v1.13.002 and user guidance

SOGIS Recognition Agreement

from	Infineon Technologies AG
PP Conformance:	Security IC Platform Protection Profile with Augmentation Packages Version 1.0, 13 January 2014, BSI-CC-PP-0084-2014
Functionality:	PP conformant plus product specific extensions Common Criteria Part 2 extended
Assurance:	Common Criteria Part 3 conformant EAL 6 augmented by ALC_FLR.1
valid until:	4 December 2028

The IT Product identified in this certificate has been evaluated at an approved evaluation facility using the Common Methodology for IT Security Evaluation (CEM), Version 3.1 extended by Scheme Interpretations by advice of the Certification Body for components beyond EAL 5 and CC Supporting Documents as listed in the Certification Report for conformance to the Common Criteria for IT Security Evaluation (CC), Version 3.1. CC and CEM are also published as ISO/IEC 15408 and ISO/IEC 18045.

(*) 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 and Notification. For details on the validity see Certification Report part A chapter 5.

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.

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.

Common Criteria Recognition Arrangement recognition for components up to EAL 2 and ALC_FLR only

Bonn, 4 September 2024
For the Federal Office for Information Security

Sandro Amendola
Director-General

L.S.

DAkkS Deutsche Akkreditierungsstelle D-ZE-19615-01-00

Bundesamt für Sicherheit in der Informationstechnik
Godesberger Allee 185-189 - D-53175 Bonn - Postfach 20 03 63 - D-53133 Bonn
Phone +49 (0)228 99 9582-0 - Fax +49 (0)228 9582-5477 - Infoline +49 (0)228 99 9582-111

RDW

Division Vehicle Regulation & Admission

THE NETHERLANDS

FUNCTIONAL CERTIFICATE FOR SMART TACHOGRAPHS

Notification concerning [1]:

- ☐ recording equipment model
- ☐ recording equipment component [2]
- ☒ a driver's card
- ☒ a workshop card
- ☒ a company card
- ☒ a controller's card

Notification concerning smart tachographs with regard to

the European agreement concerning the work of crews of vehicles engaged in international road transport (AETR) of 1 July 1970, consolidated version ECE-TRANS-SC1-2010, in accordance with the requirements set out in Annex IA/IB[3] to Council Regulation (EEC) No. 3821/85 of 20 December 1985.

Functional certificate number		: **RDW-AETR-0121197**
1.	Name of manufacturer	: Thales DIS Finland Oy
2.	Name of ~~model/component~~/card [3]	: Tachograph G1 v1.6 cards for Moldova
3.	Number of model	: Thales Digital Tachograph G1 v1.6
4.	Chip hardware	: IFX_CCI_000039H (SLC37GDA512) Infineon
5.	Chip software	: Smart Tachograph application G1 v2.2.1.N on IFX_CCI_000039H
6.	Card identification	: Tachograph cards for Moldova
7.	Test laboratory for functional certification	: UL TS B.V. De Heyderweg 2 2314 XZ Leiden

General : The ~~recording equipement model/recording equipment component~~/driver card/workshop card/company card/controller card [3] does/~~does not~~ [3] comply with the requirements laid down in Annex IA/IB[3] to the above mentioned Regulation.

Tests : The tests are carried out in accordance with:
- Annex IA/IB[3] to above-mentioned Regulation.

See Appendix A to this functional certificate.

Type-approval Department

P.O. Box 777
2700 AT Zoetermeer
The Netherlands

Tel. + 31 79 345 83 02
E-mail typeapproval@rdw.nl
www.rdw.nl

Functional certificate number: RDW-AETR-0121197

Conclusion	:	The ~~recording equipement model/recording equipment component~~/driver card/workshop card/company card/controller card [3]complies with the requirements and there ~~are~~/are no [3] objections to granting the functional certificate under the above-mentioned Regulation.
Issued by	:	RDW Europaweg 205 2711 ER Zoetermeer The Netherlands
Place, date	:	Zoetermeer, ...
Signature	:	07 November 2024

R. R. van der Spek

Remarks :

: Appendix A: - Test Report for Digital Tachograph Type Approval Functional Certification PV24090501

Reference documentation of appendix A:
- TR_FC_RDW-AETR-0121197
- FIME_TACHO_FP24062801_1a
- FIME_Results_FP24062801_Dr_01_Intake_1a.pdf
- FIME_Results_FP24062801_Dr_01_T0_1a.pdf
- FIME_Results_FP24062801_Dr_01_T1_1a.pdf
- FIME_Results_FP24062801_Dr_02_T0_1a.pdf
- FIME_Results_FP24062801_Dr_02_T1_1a.pdf
- FIME_Results_FP24062801_Ws_07_Intake_1a.pdf
- FIME_Results_FP24062801_Ws_07_T0_1a.pdf
- FIME_Results_FP24062801_Ws_07_T1_1a.pdf
- FIME_Results_FP24062801_Ws_08_T0_1a.pdf
- FIME_Results_FP24062801_Ws_08_T1_1a.pdf
- FIME_Results_FP24062801_Ws_09_DestrG1_1a.pdf
- FIME_Results_FP24062801_Ws_10_DestrG1_1a.pdf
- FIME_Results_FP24062801_Ct_13_T0_1a.pdf
- FIME_Results_FP24062801_Ct_13_T1_1a.pdf
- FIME_Results_FP24062801_Ct_14_T0_1a.pdf
- FIME_Results_FP24062801_Ct_14_T1_1a.pdf
- FIME_Results_FP24062801_Cp_19_T0_1a.pdf
- FIME_Results_FP24062801_Cp_19_T1_1a.pdf
- FIME_Results_FP24062801_Cp_20_T0_1a.pdf
- FIME_Results_FP24062801_Cp_20_T1_1a.pdf
- RDW-2016_799-0121405 Corr.02 (certificate only)
- RDW-2016-799-0121406 (certificate only)
- UL_TestReport_PV23020201_G2V2_1a
- 2.2.1.M_anssi-cc-2022_38_SecurityCertificate_engTranslation
- 2.2.1.M_ANSSI-CC-2022-38_SecurityCertificate_Scan
- 2.2.1.N_anssi-cc-2022_38-m01_SecurityMaintenanceReport
- 2.2.1.N_anssi-cc-2022_38-m01_SecurityMaintenanceReport_engTranslatior
- Interoperability Certification - THALES- A3h - 156 Ares(2023)3660335
- FIME_OptValRes_PV24090501_1a
- FIME_TestResults_PV24090501_Dr_MD_1a
- FIME_TestResults_PV24090501_Ws_MD_1a
- FIME_TestResults_PV24090501_Ct_MD_1a
- FIME_TestResults_PV24090501_Cp_MD_1a
- TachographG1_CardBody_Specification_Moldova_V2.0
- TachographG1_Information_Moldova_V2.0

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

(1) Tick the relevant boxes.
(2) Specify the component dealt with in the notification.
(3) Strike out what does not apply.

EUROPEAN COMMISSION
JOINT RESEARCH CENTRE
Dir. T – Digital Transformation and Data
Cybersecurity and Digital Technologies Unit

Ref. Ares(2025)9056604 - 23/10/2025

DT Lab

Ispra, Ares reg. date

Council Regulation (EC) 1360/2002 (Annex 1B)

Interoperability Certification N°. JRC_DTLab/A3-183/2025

Manufacturer	**THALES DIS FRANCE SAS** 6 rue de la Verrerie 92190 Meudon **FRANCE**
Specimen under Test	Thales Digital Tachograph G1 v1 6
Functional certificate	Rijksdienst Voor Het Wegverkeer n° RDW-AETR-0121197 – 07/11/2024
Security certificate	ANSSI-CC-2022/38 – 16/08/2022 ANSSI-CC-2022/38-M01 – 15/12/2022
Test Specifications:	Interoperability Test Specification v2.3 (JRC S&T Reports: JRC75155 - 2012) Interoperability of this tachograph card has been demonstrated with all type of tachograph cards and recording equipment listed on the next page.

Validity of this certificate:	6 months after registration date	requirements 449 and 453 of (EU) 2016/799
Public web site:	https://dtc.jrc.ec.europa.eu	requirement 454 of (EU) 2016/799
Remarks :	Personalised for Moldova.	

Technical Responsible
M. Gemo
Marica Gemo

Head of Unit (acting)
I. Nai Fovino
Nai Fovino

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

Interoperability has been demonstrated with the following components		
According to regulation (EU) 2016/799 amended by regulation (EU) 2021/1228 (Annex 1Cv2)	*Type Approval number*	*Result*
Smart tachograph Cards		
Thales - Digital Tachograph G2V2 / G2V2 V2.2.1.N on IFX CCI_000039H	e4-0024-00	☑
STMicroelectronics – SmartTacho V. 4.0 - J-TACHOG2V2 v.1.0.2	e3-1004	☑
Idemia – TachoDrive v4 on Cosmo X	e4-0039-00	☑
Idemia – TachoDrive v4 on Cosmo X - SAAAAR code OS 09 33 64 and SAAAAR jPatch codes: 099441 and 099E21	e4-0040-00	☑
Vehicle Units		
Continental Automotive GmbH - DTCO 1381 - Release 4.1	e1-84-08	☑
Stoneridge Electronics AB - SE5000 – 8.1 Revision A	JRC_DTLab/A2-162/2023[1]	☑
Continental Automotive GmbH - DTCO 1381 - Release 4.1a	JRC_DTLab/A1-177/2025[2]	☑
Stoneridge Electronics AB - SE5000-8.1 Revision F	JRC_DTLab/A2-175/2025[3]	☑
According to regulation (EU) 2016/799 (Annex 1C)		
Smart tachograph Cards		
Gemalto – Smart Tachograph G2 on MultiApp V4.01	e4-0001-00	☑
Idemia - Smart Tachograph G2 - IDeal Drive DT V3.0 Applet code v. 416304	e13-0001-00	☑
STMicroelectronics - Smart Tachograph v3.0 – OS J-Tacho vl.2.6	e3-1003	☑
STMicroelectronics – SmartTacho V3.1 – OS J-Tacho vl.3.1	e3-1003-1	☑
Vehicle Units		
Continental Automotive GmbH - DTCO 1381 - Release 4.0e	e1-84-04	☑
Stoneridge Electronics AB - SE5000 - 8 Revision G	e5-0002-06	☑
Intellic GmbH – EFAS-4.10 – v5.00	e1-222-00	☑
Other Components		
Motion Sensor: VDO 2185	e1-0002-00	☑
Motion Sensor: Lesikar TACH3 - HW v02 / SW v03	e5-0100-v02	☑
According to regulation (EC) 1360/2002 (Annex 1B)		
Tachograph Cards		
Gemalto - MultiApp ID Tachograph 36K	e13-28-01	☑
Gemalto - MultiApp ID Tachograph 36K	e2-32	☑
Gemalto - MultiApp ID Tachograph V1.3	e11-1002-01	☑
Giesecke & Devrient - STARCOS 3.4 ID Tachograph C1	e1-216	☑
Giesecke & Devrient - STARCOS 3.6 ID Tachograph P1	e1-238	☑
Idemia – IDeal Drive DT V3.0 Applet code version 416304	e1-242-00	☑
Idemia - TachoDrive v4 on ID-One Cosmo X	e68-001	☑
Morpho - ORGA Tachograh N Micardo v1.0	e1-191	☑
Morpho - MICARDO Tachograph V3.6	e1-212	☑
Morpho - Morpho Haarlem Tachograph V1.0	e1-237	☑
Thales – MultiApp V4.0.1	e4-0001-00	☑
Trueb - TCOS v1.0 Release 2	e1-182-04	☑
Trueb - Tru/cos tacho v1.1	e1-232	☑

[1] Interoperability certificate number granted to Revision A, type-approval granted to Revisions B (e5-0002-08), D (e5-0002-10) and E (e5-0002-11).
[2] Interoperability certificate number granted to SW release 04.01.36, type-approval granted to SW Release 04.01.40 (e1-84-09).
[3] Interoperability certificate number granted to Revision F SW release 2322, type-approval granted to Revision G SW release 2424 (e5-0002-13).

Vehicle Units		
Actia - SMARTACH STDII - version 6.11	e2-25	☑
Continental Automotive GmbH - DTCO 1381 - Release 2.2	e1-84-20	☑
Continental Automotive GmbH - DTCO 1381 - Release 3.0	e1-84-24	☑
Intellic GmbH – EFAS-4.8 - v03.50	e1-222	☑
Stoneridge Electronics AB - SE5000 - Revision 7.6	e5-0002	☑
Pars Ar-Ge Ltd - DTC 101 - Version 1.1	e37-0004	☑
ASELSAN - STC 8250- Version 1.1	e37-0007	☑
ASELSAN - STC 8255- Version 1.0	e37-0008	☑
Other Components		
Motion Sensor: Actia IS2000 LR5-R1.2	e2-26	☑
Motion Sensor: VDO KITAS 2171	e1-175-06	☑
Motion Sensor: VDO KITAS 2171	e1-175-07	☑
Motion Sensor: Lesikar TACH2 HW version 04 and SW version 02	e5-0101	☑
Motion Sensor: BogArt DTMS V01	e20-1	☑

S.C. CERTSIGN S.A. certSIGN 2 BUCUREȘTI ROMÂNIA

PREMIER MINISTRE

Liberté
Égalité
Fraternité

Schéma français d'évaluation et de certification de la sécurité des technologies de l'information

CERTIFICAT ANSSI-CC-2022/38-R01

Ce certificat est associé au rapport de certification ANSSI-CC-2022/38-R01

Tachograph G1, G2V1, G2V2 on IFX_CCI_000039h

version 2.2.1.N

Développeur : THALES DIS
Commanditaire : THALES DIS
Centre d'évaluation : CEA Leti

Critères Communs version 3.1, révision 5

EAL4 Augmenté
(ALC_DVS.2, ATE_DPT.2, AVA_VAN.5)

conforme aux profils de protection :

Digital Tachograph – Smart Card (Tachograph Card) version 1.02, 15 novembre 2011, référence BSI-CC-PP-0070-2011
Digital Tachograph – Tachograph Card (TC PP), version 1.0, 9 May 2017., référence BSI-CC-PP-0091-2017

Date de validité : date de signature + 5 ans.

Paris, le 17/3/2025 | 09:30 CET

Vincent Strubel

Timothy BAILLIE
Expert Traducteur
près la Cour d'Appel de Besançon
ANGLAIS, FRANÇAIS, ESPAGNOL, PORTUGAIS
N° ne varietur S/285227 Date 21 MARS 2025

SÉCURITÉ DES TECHNOLOGIES DE L'INFORMATION — SOGIS

Dans le cadre du CCRA, ce certificat est reconnu au niveau EAL2

Ce certificat est émis conformément au décret 2002-535 du 18 avril 2002 modifié relatif à l'évaluation et à la certification de la sécurité offerte par les produits et systèmes des technologies de l'information.

Secrétariat général de la défense et de la sécurité nationale, Agence nationale de la sécurité des systèmes d'information
51, boulevard de La Tour-Maubourg, 75700 PARIS 07 SP

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

Le produit, objet de cette certification, a été évalué par le CEA - LETI sis en France en appliquant la *Common Methodology for Information Technology Security Evaluation*, version 3.1, révision 5, conforme aux Critères communs, version 3.1, révision 5.

Ce certificat s'applique uniquement à cette version spécifique de produit dans sa configuration évaluée. Il ne peut être dissocié de son rapport de certification complet. L'évaluation a été menée conformément aux dispositions du SOG-IS, du CCRA et du schéma français. Les conclusions du centre d'évaluation, formulées dans le rapport technique d'évaluation, sont cohérentes avec les preuves fournies.

Ce certificat ne constitue pas en soi une recommandation du produit par l'Agence nationale de la sécurité des systèmes d'information et ne garantit pas que le produit certifié soit totalement exempt de vulnérabilités exploitables.

[Logo: PRIME MINISTER
Liberty
Equality
Fraternity]

French assessment scheme for the evaluation and certification of the security of information technologies

CERTIFICATE ANSSI-CC-2022/38-R01

This certificate is associated with the ANSSI-CC-2022/38-R01 certification report

Tachograph G1, G2V1, G2V2 on IFX_CCI_000039h

version 2.2.1.N

Developer: THALES DIS
Sponsor: THALES DIS
Assessment centre: CEA Leti

Version 3.1, revision 5 Common Criteria

EAL4 Augmented

(ALC_DVS.2, ATE_DPT.2, AVA_VAN.5)

conforming to the protection profiles:
Digital Tachograph – Smart Card (Tachograph Card) version 1.02, 15 November 2011, reference BSI-CC-PP-0070-2011
Digital Tachograph – Tachograph Card (TC PP), version 1.0, 9 May 2017., reference BSI-CC-PP-0091-2017

Date of validity: date of signature + 5 years.

Paris, the 17/03/2025 | 09:30 Central European Time

[Signature]

Timothy BAILLIE
Expert Traducteur
près la Cour d'Appel de Besançon
ANGLAIS, FRANÇAIS, ESPAGNOL, PORTUGAIS
N° ne varietur S/2803227 Date 21 MARS 2025

[Logo] [Logo] [Logo]
Under the terms of the CCRA, this certificate is recognised at level EAL2.

This certificate is issued in accordance with Decree 2002-535 of 18 April 2002, as amended, relating to the evaluation and certification of the security offered by information technology products and systems.
Secretariat-General for National Defense and Security (France), French Cybersecurity Agency (ANSSI)
51, boulevard de La Tour-Maubourg, 75700 PARIS 07 SP

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

The product subject to this certification was evaluated by the CEA - LETI located in France by applying the *Common Methodology for Information Technology Security Evaluation*, version 3.1, revision 5, conforms to the Common Criteria, version 3.1, revision 5.

This certificate applies only to this specific product version in its evaluated configuration. It cannot be separated from its full certification report. The assessment was carried out in accordance with the provisions of the SOG-IS, the CCRA and the French scheme. The conclusions of the assessment centre, as set out in the technical assessment report, are consistent with the evidence provided.

This certificate does not in itself constitute a recommendation of the product by the French National Agency for the Security of Information Systems and does not guarantee that the certified product is completely free of exploitable vulnerabilities.

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 an inspector's card

Bauartgenehmigung Nr. / Approval No.: e1*232*02

1. Hersteller- oder Handelsmarke:
Manufacturing or commercial mark:
Gemalto AG

S.C. CERTSIGN S.A. certSign 2/6 BUCUREȘTI - ROMÂNIA

Nummer der Genehmigung: e1*232*02
Approval No.:

2. Modellbezeichnung:
Name of model:
tru/cos tacho V1.1-AETR

3. Name des Herstellers:
Name of manufacturer:
Gemalto AG

4. Anschrift des Herstellers:
Address of manufacturer:
CH-5000 Aarau

5. Vorgelegt zur Bauartgenehmigung am:
Submitted for approval on:
10.08.2017

6. Prüfstelle(n):
Test laboratory or laboratories:
TÜV Nord Mobilität GmbH & Co. KG Institut für Fahrzeugtechnik und Mobilität
DE-45307 Essen

7. Datum und Nummer des Prüfberichts:
Date and number of reports:
09.08.2017 8114937660

8. Datum der Bauartgenehmigung:
Date of approval:
30.07.2015

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

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

Nummer der Genehmigung: e1*232*02
Approval No.:

11. Ort: **DE-24944 Flensburg**
Place:

12. Datum: **21.08.2017**
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	**"CH", "UA", "MD"**
driver card	
Werkstattkarte	**"CH", "MD"**
workshop card	
Unternehmenskarte	**"CH", "MD"**
company card	
Kontrollkarte	**"CH", "MD"**
inspector's card	

Fahrerkarte, Werkstattkarte, Unternehmenskarte und Kontrollkarte in der Ländervariante Moldavien "MD" kommen hinzu
driver card, workshop card, company card and inspector's card in the country variant Moldova "MD" are added

Unterschrift: **Im Auftrag**
Signature:

(Jörg Burgkhardt)

KRAFTFAHRT-BUNDESAMT 527

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

Kraftfahrt-Bundesamt

DE-24932 Flensburg

Nr. der Genehmigung: e1*232*02
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**.

Bundesamt
für Sicherheit in der
Informationstechnik

Deutsches IT-Sicherheitszertifikat

erteilt vom Bundesamt für Sicherheit in der Informationstechnik

BSI-DSZ-CC-0889-2013

Tachograph Card

tru/cos tacho v1.1

from	Trueb AG
PP Conformance:	Protection Profile Digital Tachograph - Smart Card (Tachograph Card), Version 1.02, 15 November 2011, BSI-CC-PP-0070-2011
Functionality:	PP conformant plus product specific extensions Common Criteria Part 2 extended
Assurance:	Common Criteria Part 3 conformant EAL 4 augmented by ATE_DPT.2 and AVA_VAN.5

Common Criteria Recognition Arrangement for components up to EAL 4

Common Criteria

The IT product identified in this certificate has been evaluated at an approved evaluation facility using the Common Methodology for IT Security Evaluation (CEM), Version 3.1 extended by advice of the Certification Body for components beyond EAL 5 and guidance specific for the technology of the product for conformance to the Common Criteria for IT Security Evaluation (CC), Version 3.1 and according to Commission Regulation (EC) No. 1360/2002 Annex 1(B) adapting to Council Regulation (EC) No. 3821/85 amended by Commission Regulation (EC) No. 432/2004 of 5 March 2004, Council Regulation (EC) No. 1791/2006 of 20 November 2006 and Commission Regulation (EC) No. 68/2009 of 23 January 2009, Commission Regulation (EU) No. 1266/2009 of 16 December 2009 on recording equipment in road transport.

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.

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.

Bonn, 28 June 2013
For the Federal Office for Information Security

Bernd Kowalski
Head of Department

SOGIS IT SECURITY CERTIFIED MUTUAL RECOGNITION AGREEMENT

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

Bundesamt für Sicherheit in der Informationstechnik
Godesberger Allee 185-189 - D-53175 Bonn - Postfach 20 03 63 - D-53133 Bonn
Phone +49 (0)228 99 9582-0 - Fax +49 (0)228 9582-5477 - Infoline +49 (0)228 99 9582-111

Kraftfahrt-Bundesamt

DE-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:
   Gemalto AG

2. Modellbezeichnung:
   Name of model:
   tru/cos tacho V1.1-AETR

3. Name des Herstellers:
   Name of manufacturer:
   Gemalto AG

4. Anschrift des Herstellers:
   Address of manufacturer:
   CH-5000 Aarau

S.C. CERTSIGN S.A. certSIGN 2/0 BUCUREȘTI - ROMANIA

5. Prüfstelle(n):
Test laboratory or laboratories:
TÜV Nord Mobilität GmbH & Co. KG Institut für Fahrzeugtechnik und Mobilität DE-45307 Essen

6. Datum und Nummer des Prüfberichts:
Date and number of reports:
09.08.2017 8114937660

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.

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

8. Bemerkungen:
Remarks:
Karten mit folgenden Unterscheidungszeichen:
cards with the following distinguishing signs:

Fahrerkarte **driver card**	**"CH", "UA", "MD"**
Werkstattkarte **workshop card**	**"CH", "MD"**
Unternehmenskarte **company card**	**"CH", "MD"**
Kontrollkarte **inspector's card**	**"CH", "MD"**

Fahrerkarte, Werkstattkarte, Unternehmenskarte und Kontrollkarte in der Ländervariante Moldavien "MD" kommen hinzu
driver card, workshop card, company card and inspector's card in the country variant Moldova "MD" are added

9. Ort: **DE-24944 Flensburg**
Place:

10. Datum: **21.08.2017**
Date:

11. Unterschrift: **Im Auftrag**
Signature:

(Jörg Burgkhardt)

KRAFTFAHRT-BUNDESAMT 527

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

EUROPEAN COMMISSION
JOINT RESEARCH CENTRE

Institute for the Protection and Security of the Citizen (Ispra)
G.07 - Digital Citizen Security

DT Lab

05/08/2013

Council Regulation (EC) 1360/2002
Interoperability Certificate N°. JRC_DTC/AC-081/ 2013

Manufacturer :	**Trüb AG** Hintere Bahnhofstrasse 12 CH-5001 Aarau Switzerland

Specimen under Test	Interoperability Tests on Digital Tachograph Cards **. Tru/cos tacho module 1.1**

Test Specification:	Interoperability Test Specification v2.3 (JRC S&T Reports: JRC75155 - 2012) Interoperability of this Digital Tachograph cards has been demonstrated with the following recording equipment and motion sensors:	
Vehicle Unit		**Security Certificate**
Actia SMARTACH STDII version 6.11		DCSSI 2005/14 and M-2006/10
Continental Automotive GmbH DTCO 1381, Release 2.1		BSI-DSZ-CC-0878-2013
Intellic GmbH – EFAS-4 v02		BSI-DSZ-CC-0726-2012
Stoneridge Electronics AB SE5000 Revision 7.4		BSI-DSZ-ITSEC-0805-2012
Motion Sensors		
Actia IS2000 SMARTACH LXRY	Siemens VDO KITAS 2171	
Validity of this certificate:	04/02/2014	(EC) 1360/2002 requirements 286[1] and 289[2]
Public web site:	http://dtc.jrc.ec.europa.eu	(EC) 1360/2002 requirement 290
Remarks :	Switzerland, Latvia, Estonia and Romania personalization were applied on all type of cards (workshop, driver, company and control cards). Bulgaria personalization was applied only on driver and company cards.	

Technical Responsible
M. Chiaramello

Head of Unit
J-P. Nordvik
P.O. Sjoerd Boldy

[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

S.C. CERTSIGN S.A. certSIGN BUCHAREST, ROMANIA

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

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	**„UA", „MD"**
driver card	
Werkstattkarte	**„UA", „MD"**
workshop card	
Unternehmenskarte	**„UA", „MD"**
company card	
Kontrollkarte	**„UA", „MD"**
inspector's card	

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

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**.

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 responsible 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-menta-tion	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 Pro-cessing	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 Messa-ges	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.

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

DAP-PL-2519.00

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:

[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
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.

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 Company Card

Standard of test method:	ISO/IEC 10373-1 (2006)
Standard of requirements:	ISO/IEC 7810 (2003)

Complies with requirements:

[X] **yes**

[ ] **no**

DAP-PL-2519.00

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.

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 Workshop 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
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.

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 Control Card

Standard of test method:	ISO/IEC 10373-1 (2006)
Standard of requirements:	ISO/IEC 7810 (2003)

Complies with requirements:

[X] **yes**

[ ] **no**

DAP-PL-2519.00

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

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. front	back	Evaluation
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.

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 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

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	
B 5	Company Card	[X] / [ ]	[X] ok / [ ] fault
B 6	Company Card	[X] / [ ]	[X] ok / [ ] fault
B 7	Company Card	[ ] / [X]	[X] ok / [ ] fault
B 8	Company Card	[ ] / [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-

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

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	
C 5	Workshop Card	[X]		[X] ok
		[ ]		[ ] fault
C 6	Workshop Card	[X]		[X] ok
		[ ]		[ ] fault
C 7	Workshop Card		[X]	[X] ok
			[ ]	[ ] fault
C 8	Workshop Card		[X]	[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: [X] **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		X ok
				fault
D 6	Control Card	X		X ok
				fault
D 7	Control Card		X	X ok
				fault
D 8	Control Card		X	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.

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

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: **DE-24944 Flensburg**
Place:

10. Datum: **02.12.2010**
Date:

11. Unterschrift: **Im Auftrag**

Signature:

Dirk Hansen

KRAFTFAHRT-BUNDESAMT 496

JRC
EUROPEAN COMMISSION

DT Lab

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.

MODALITATEA DE RĂSPUNS LA FACTORII DE EVALUARE

Nr. d/o	Denumirea factorului de evaluare	Ponderea%	Răspuns CERTSIGN S.A.
1.	**Cel mai mic preț al ofertei**	**60**	CERTSIGN S.A. a inclus prețul ofertat în documentul *Anexa nr. 23 – Specificații de preț*, astfel cum s-a solicitat în documentația de atribuire.
2.	**Perioada cea mai scurtă de furnizare a cartelelor tahografice personalizate**	**5**	CERTSIGN S.A. a prevăzut în ofertă o perioadă de furnizare a cartelelor tahografice personalizate de 3 zile lucrătoare (1 zi lucrătoare pentru procesarea comenzii și personalizare carduri și 2 zile lucrătoare pentru livrarea prin curier rapid – DHL).
3.	**Tehnic:**	**35**	
3.1	Suport tehnic de la producător în limba română.	5	CERTSIGN S.A. a inclus în ofertă suport tehnic de la producător în limba română. Producătorul soluției ofertate este CERTSIGN S.A.
3.2	Aplicație software al sistemului pentru înregistrarea de cereri carduri tahograf digital, emitere carduri și gestiune a cardurilor emise de către ANTA, în limba română.	10	Aplicația software a sistemului pentru înregistrarea de cereri carduri tahograf digital, emitere carduri și gestiune a cardurilor emise de către ANTA, ofertată de CERTSIGN S.A., denumită tachoSAFE MD-CIA, este în limba română.
3.3.	Securitatea soluției.	5	CERTSIGN S.A. asigură securitatea completă a soluției propuse, care include: • Securitatea fizică a locațiilor centrelor de date care găzduiesc echipamentele 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 și certificate digitale stocate pe dispozitive criptografice

certSIGN

			hardware, asigurându-se astfel autenticitatea, integritatea și confidențialitatea datelor vehiculate în sistem, • Securitatea de rețea și comunicații, și • Securitate cibernetică a acestor sisteme ținând cont de noile amenințări cibernetice.
3.4.	Mentenanța gratuită și cel mai mic termen de intervenție on-site pentru aplicația software al sistemului pentru înregistrarea de cereri carduri tahograf digital, emitere carduri și gestiune a cardurilor emise de către ANTA.	5	CERTSIGN S.A. a inclus în ofertă mentenanța gratuită, un termen de intervenție remote de 2 ore și un termen de intervenție on-site de 24 de ore pentru aplicația software al sistemului pentru înregistrarea de cereri carduri tahograf digital, emitere carduri și gestiune a cardurilor emise de către ANTA.
3.5.	Dispozitive tehnice gratuite pentru colectarea datelor persoanelor solicitate de cartel tahografice în scopul implementării contractului (Camere foto web, Paduri de semnătură (minim 5 bucăți de fiecare))	5	CERTSIGN S.A. a inclus în ofertă dispozitive tehnice gratuite pentru colectarea datelor persoanelor solicitate de cartele tahografice în scopul implementării contractului, și anume 5 camere foto web și 5 paduri de semnătură.
3.6.	Cel mai mic termen de instalare a aplicației software al sistemului pentru înregistrarea de cereri carduri tahograf digital, emitere carduri și gestiune a cardurilor emise de către ANTA.	5	CERTSIGN S.A. a inclus în ofertă un termen de instalare a aplicației software al sistemului pentru înregistrarea de cereri carduri tahograf digital, emitere carduri și gestiune a cardurilor emise de către ANTA de 0 ore. Aplicația software a sistemului pentru înregistrarea de cereri carduri tahograf digital, emitere carduri și gestiune a cardurilor emise de către ANTA este deja instalată și utilizată în prezent de către ANTA.
TOTAL:		**100**	

Data completării: 31.10.2025

Ofertant,
CERTSIGN S.A.
Reprezentant împuternicit
Armand-Dragoș ROPOT

DECLARAȚIE
privind depunerea în original a mostrelor de cartele

Către:
Autoritatea Administrativă "Agenția Națională Transport Auto"
str. Aleea Gării, 6, mun.Chişinău, Republica Moldova

Stimaţi domni,

Prin prezenta declarăm că am transmis către dumneavostră, până la data limită de depunere a ofertelor, astfel cum ați solicitat la pct. 5 Mostre din Caietul de sarcini, coletul conținând **câte 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,** astfel cum ați solicitat în documentația pentru atribuirea de **Cartele tahografice personalizate, prin procedura de achiziție Acord Cadru pe un termen de 4 ani (2026-2029)** - anunț de participare nr. 21494473 (nr. achiziție comercială conform platformei achizitii.md).
Coletul transmis prin DHL (cod de urmărire colet: 91 9826 1214) a fost recepționat la sediul dumneavoastră în data de 27.10.2025, ora locală 09:12. În acest sens **atașăm** dovada trimiterii preluată de pe site-ul DHL, document ce se poate consulta și online, pe site-ul curierului.

Data completării: 31.10.2025

Ofertant,
CERTSIGN S.A.
Reprezentant împuternicit
Armand-Dragoș ROPOT

27 October 2025

Dear Customer,

This is a proof of delivery / statement of final status for the shipment with waybill number 9198261214.

Thank you for choosing DHL Express.

www.dhl.com

Your shipment 9198261214 was delivered on 27 October 2025 at 09.12

Shipment Status	Delivered	**Destination Service Area**	KISHINEV MOLDOVA, REPUBLIC OF
		Piece ID(s)	JD014600012291119437

Additional Shipment Details

Service	EXPRESS WORLDWIDE doc	**Origin Service Area**	BUCHAREST ROMANIA
Picked Up	23 October 2025 at 14.59	**Shipper Reference**	Mostra Tahox4-pin 9198261214RO20251023110319667