THE PROCUREMENT OF BLANKS OF IDENTITY DOCUMENTS OF THE NATIONAL PASSPORT SYSTEM, DRIVING LICENSES AND REGISTRATION CERTIFICATES FOR THE PERIOD 2024 – 2029

REPUBLIC OF MOLDOVA

Agentia Servicii Publice (ASP)
Public Service Agency (PSA)

_____

Lot n°2:

Cards on polycarbonate base support with / without embedded chip (ID-1 format)

APPENDIX LOT N°2 TECHNICAL OFFER

Paris, the 29 July 2024

SELP

Contents

INTRODUCTION

To: **Public Service Agency (PSA),**

Paris, 29th of July 2024

Procurement object: The procurement of blanks of identity documents of the national passport system, driving licenses and registration certificates for the period 2024 – 2029

Dear Madams, dear Sirs,

SELP is known among the world's leading secure document designers and manufacturers with cards and datapage issued for millions of citizens all around the world.

We are trusted by customers whose businesses rely on security, quality, timely delivery, cost effectiveness and flexibility to change. Our solutions and services allow us to provide complete end-to-end solutions to our customers.

SELP takes pleasure in submitting our proposal for the production and delivery of electronic Polycarbonate smart cards. We believe that our final proposal represents an excellent match with your requirements.

We hereby, submit our bid electronically.

We hope this offer will meet your expectations and we are looking forward to continue our cooperation.

We remain also at your disposal for any further information required on our proposal.
Regards,

Bastien BLANC, CEO of Roland Holding SAS, President of SELP SAS

Signature numérique de Bastien BLANC
DN : c=FR, o=ROLAND HOLDING, ou=ROLAND HOLDING, ou=0002 98354971800028, ou=Direction, 2.5.4.97=NTRFR-98354971800028, l=PARIS, sn=BLANC, givenName=Bastien, cn=Bastien BLANC, title=Directeur Général, serialNumber=0100
Date : 2024.07.25 16:09:05 +02'00'

1 SELP PRESENTATION

SELP is a high-tech company with more than 60 years' experience in smart-cards production with high secure production facility for the production of Identity Document located in France.

Human in scale, flexible and client oriented, SELP is the right partner for smart-cards projects.

1.1.1 KEY FIGURES

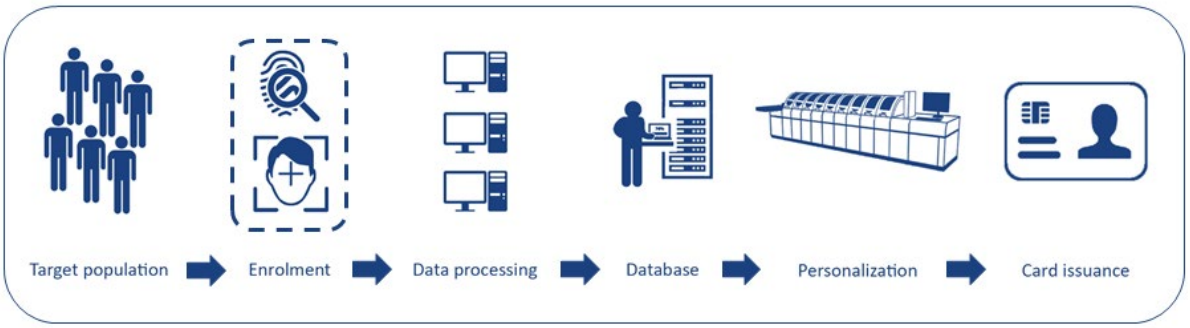
1.1.2 CERTIFICATIONS

SELP is a high security printer, certified by Intergraf and the ISO 14298 standard. This certification qualifies a highly secured environment, and allows the manufacturing of valuable documents.

SELP is also certified ISO 9001 (Angoulême, Mareuil, Puy Guillaume, New Delhi and Mumbai sites) for its quality management, ISO 14001 (Angoulême plant) for its environmental management, and ISO 27001 (Angoulême plant) for the management of data and security.

1.1.3 GLOBAL SOLUTION PROVIDER

SELP is capable of supply a global solution for its smartcards issuers clients. We have the industrial and technological assets to implement any kind of project.



Our expertise is built on five types of services:

- **Design & production:** our capacity to conceive anti-counterfeiting documents, to produce cards on different materials, to respect international standards and to work in optimal quality and security environment.

- **Electronic components & applications:** our capacity to advise our clients on the right technology and the right form-factor (card, inlay, eStickers, eCovers), to supply a certified operating and to develop specific applications.

- **Systems & solutions:** our capacity to supply enrolment solutions, to integrate biometry, to secure our clients' data, to supply perfect personalization service and to build tailor-made Credential Management system (CMS).

- **Service supply:** our capacity to offer storage facilities (own SELP facilities our dedicated platforms), to develop web-services between our system and the one of our clients, to provide fulfillment services and even full outsourcing of the cards management.

- **Dematerialization:** our capacity to conceive innovating solutions to dematerialize cards applications or even cards themselves, to create personalized solutions for our clients and to provide in-house developments thanks to our talented R&D team.

2 LOT 2 : BLANK ID CARDS

2.1 MOLDOVA eID AND eRC DUAL PC CARD

1.1.1 KEY CHARACTERISTICS

Model	One model is proposed for: – Moldova eID DUAL PC card (ID) - EA – Moldova eRC DUAL PC card (RC) - RC
Material	Polycarbonate (PC) card with multi-layer structure
Format	The card format complies with the international norms - ISO/IEC 7810 standard, i.e. 85.6 x 53.98 mm (ID1 format). - ISO/IEC 7501-1 - ISO/IEC 7501-3 - ISO/IEC 10373-1/3/6: 2006 - ISO/IEC 7816 - ISO/IEC 18745-1/2
Design	The Design projects of the cards, provided by PSA, will include the final design of the document's background (high-quality vector and raster graphics) with the document name and data field names, requirements for the positioning and shape of security features, as well as a description of the inks used and their characteristics (e.g., color transition in iris print). The files will be presented in PDF and/or CGT (Corvina) format, for each separate layers and colors.
Interface	The card includes a contact and contactless electronic component (DUAL Interface), which complies with the international norms - ISO/IEC 14443 parts 1- 4.
ICAO Compliance	The proposed card fully complies with the ICAO recommendations specified in the latest version of Doc 9303 and its supplements. It is therefore machine-readable.
European Regulations	Regulation (EU) 2019/1157 of the European Parliament and of the Council of 20 June 2019 on strengthening the security of identity cards of Union citizens and of residence documents issued to Union citizens and their family members exercising their right of free movement or latest amendments thereof.
Durability	The card will have a lifespan of at least 10 years in normal operation. To guarantee this durability, SELP subjects all its security components to the most stringent resistance tests.

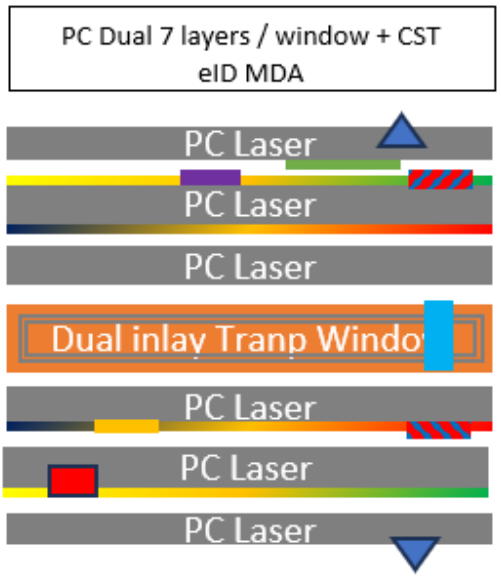
2.1.1 CARD STRUCTURE

The identity card we offer is a polycarbonate card with a secure construction that allows a personalisation at the heart of the card, protected by printing and DOVID.

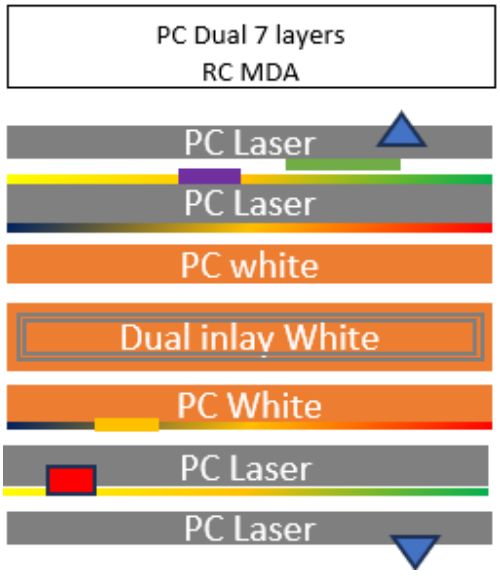
Polycarbonate is a plastic material with excellent mechanical properties and high thermal resistance. It has a lifespan of around 10 years (without any degradation). It has high mechanical and thermal resistance, and can be used to personalize data at the heart of the card, as well as incorporating security features to combat counterfeiting and falsification.

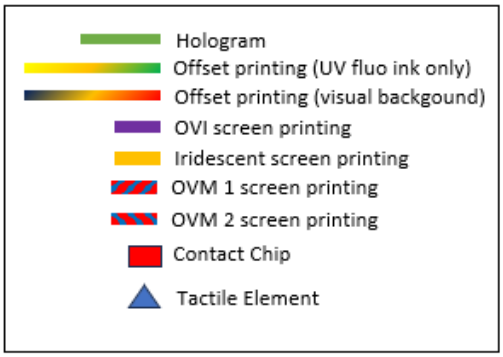
The proposed identity card is made of **seven layers of Polycarbonate** material.

eID card structure



eRC card structure



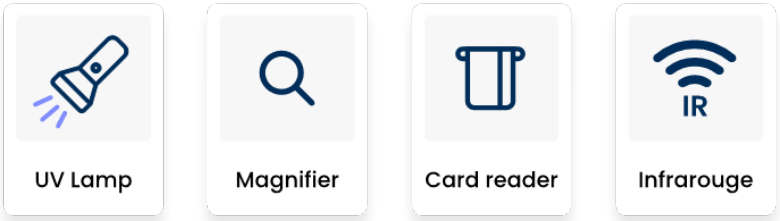


2.1.2 SECURITY FEATURES

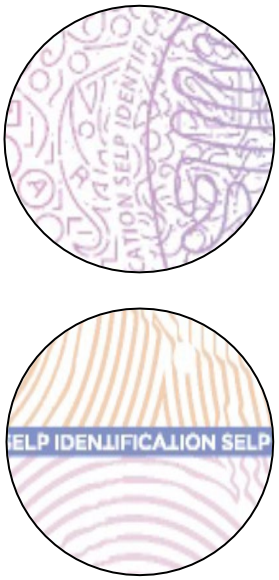
Additional securities are described in this offer with the following pictograms:

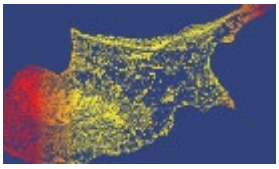
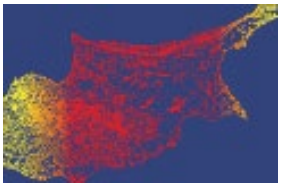
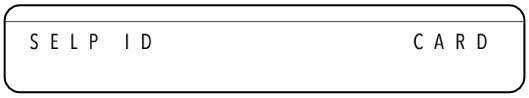
The first level (overt) relates to security features that the public can easily check, without special aids.

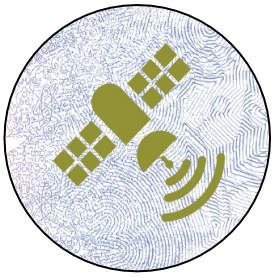
Second-level (covert) relates to security features that can be checked with simple tools.

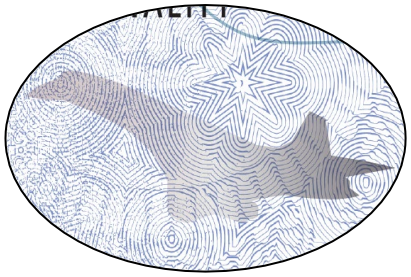
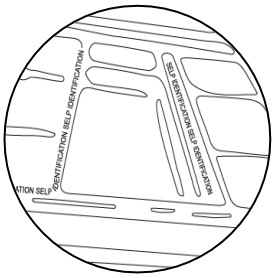


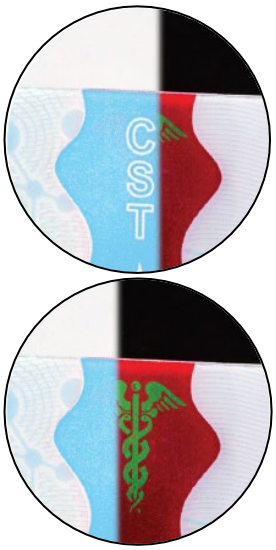
Third-level (forensic) security features are for qualified forensic laboratories and other sophisticated laboratory equipment.

Specifications for card body		
UV Dull polycarbonate	A UV dull substrate is a substrate with no bleaching agents in its composition and therefore which has **no fluorescence under UV light**. This characteristic enables the use of fluorescent inks under UV. This will make evident such attacks as adding a laminate which would react under UV light and be easily detected.	
Guilloches	Guilloches background is made up of fine lines arranged in random, geometric patterns. The patterns, unique to each project, are effective against attempts at falsification by abrasion. They are generated using software accessible only to high-security printers and are very difficult to reproduce by standard means, limiting the risk of counterfeiting.	
Anti-scanning Anti-copy	One anti-copy method is based on changing line thickness and distance, but still keeping the ink coverage constant. The idea with this approach is that the counterfeiter's process would not be so accurate and different color shades would be visible due to variation in line width and distance in between single lines.	
Invisible micro-lettering (positive and negative)	Micro-lettering is the micro printing of a word or a sentence which is not visible to the naked eye and is easily mistaken for a simple line. This element can be integrated into the background of the document or used to highlight an element.	

Delibarate error	A specific design will be created with deliberate error.	
Rainbow printing	Rainbow printing is achieved using specially adapted offset machines. It's generated by blending two colours in a controlled manner, to create a subtle color transition. Its control is made all the easier by the fact that its integration into the design is optimized by the know-how of our designers.	
Invisible and fluorecent under UV-A and UV-B rainbow printing	Rainbow printing is achieved using specially adapted offset machines. It's generated by blending two colours in a controlled manner, to create a subtle color transition. Its control is made all the easier by the fact that its integration into the design is optimized by the know-how of our designers. The ink used for this features is invisible under normal light and appear fluorescent under UV-A & UV-B.	 
Metameric ink pair	Infrared (IR) abs / trans inks look the same under normal light. They are both visible for the human eye. When looking with a special IR light source, only IR abs inks are visible. These inks provide additional copy protection. The verification requires IR light source which are not so common.	 

Optically Variable Ink (OVI) with UV	Optically Variable Ink is an optical security feature characterized by a unique and striking color-shift that is visible to the naked eye simply by titling the document. OVI distinguishes itself by its high chromaticity and a long color travel. Two OVI are proposed in new electronic identity card, one integrated into the front side	 
Semi-transparent DOVID	The polycarbonate card will be protected with a Semi-transparent DOVID (Diffractive Optical Variable Identification Device) embedded in the core of the card at lamination stage. The DOVID, is mainly a level 1 security feature, controllable with the naked eye by titling the card. It also embeds level 2 and level 3 security features. DOVID will display the following feature: - maintained in the same plane and angle of light reflection, the two distinct reflective colors of the DOVID will interchange at any 90° rotation. - by tilting "DOVID" up and clown, part or the entire surface of the two colored reflective areas will simultaneously display animations in opposite directions. - a part of one of the two colored reflective areas forms an object that renders a positive 3D relief effect on the "DOVID" surface. Area size: minimum 31mm x 31mm. The same Dovid will be used for all type of cards.	

Iridescent Ink	Thanks to iridescent inks and their unique property of reflecting incident light, we can observe effects of brilliance and invisibility depending on the angle of observation. This feature makes it an interesting choice for protecting an ID card, as it makes it more difficult to scan or copy the document using traditional equipment.	
Relief embossing	A relief embossing is created during the card lamination stage. Extreme pressure fuses the polycarbonate layers together and creates a relief. The relief features created by the lamination process are effective against counterfeiting and data tampering. Several features can be included: guilloches, micro-lettering, matte effect, super tactile effect, etc. Combining them adds complexity to the design in order to avoid counterfeiting and falsification (by overlaping a lamina), and must be worked on in conjunction with the design of the cards. Relief embossing will be the same for all type of cards.	 
CLI/MLI	Changeable or multiple laser image (CLI / MLI) consists of personalization of typically two data through a lens on the ID document surface. The two sets of data are alternately visible when tilting the document. CLI/MLI will be on the backside of the card	

Specifications for eID card body ONLY		
Transparent window with CST ink	Transparent window with color change (the transparent area will change its color according to the color of the background on which it is viewed, using technology with which the material used will have the effect of optical change): - on light background: the window will have a primary color (blue); - on dark background: the window will change its hue to a second color (red), and an image will appear as a third color (yellow-green) as an embedded image; - the embedded image will also be reactive to UV light (yellow-green fluorescence). Area size: 10 mm x 12 mm. The transparent window will accept laser engraving at the personalization stage.	

2.1.3 PRE-PERSONALIZATION

The purpose of an Identity document is to store personal information that enables a person to be identified with certainty. The certainty with which another person can be identified derives not only from the security of the card itself, but also from the way in which the data is securely stored on the card.

Specifications for the card personalization		
Unique sequencial card number	At the manufacturing stage, in order to secure the management of cards movement, each card shall be assigned with a sequential number, applied in a 1D barcode, placed on the backside of the card and will ensure the consecutive numbering of the cards.	

2.1.4 THE DUAL INTERFACE CHIP

Req No.	Position in chip	Requirements	Comments
1.	**Field of use of the Chip**	National eID card	Compliant
2.	**Operating system security**	Operating System must be certified according to EAL6+	Compliant
3.	**Interface**	Chip shall support the following interfaces: a) Contact interface, according to ISO/IEC 7816 b) Contactless interface (RF), according to ISO/IEC 14443, 1-4 c) NFC support, according to ISO/IEC 18092 Type A interface for data rates up to 848 kbit/s, symmetric and asymmetric data rate configurations.	Compliant
4.	**Chip service lifetime**	Minimum 10 years	Compliant
5.	**Memory**	Minimum available memory for user data shall be 120 kB, where: 85 kB shall be reserved for the personalization of the applications described in (16) 35 kB shall be reserved for future use and storage of personal data.	Compliant
6.	**Cryptography: Symmetric cryptographie algorithms**	Minimum set of supported algorithms: DES, 56 bit key length 2-DES, 112 bit key length 3-DES, 168 bit key length AES, 128, 192 and 256 bit key length	Compliant

7.	**Cryptography: Asymmetric cryptographie algorithms**	Minimum set of supported algorithms : Rivest-Shamir-Adleman (RSA), up to 2048 bits key length Elliptic-curve cryptography (ECC), including 256or 384 bits key length	Compliant
8.	**Cryptography: Hash functions**	Minimum set of supported hash functions : SHA-224, SHA-256, SHA-384 and SHA-512	Compliant
9.	**Random number generator**	The chip shall have a built-in hardware random number generator	Compliant
10.	**Hardware accelerators for Computing cryptographie functions**	The chip shall have a built-in hardware Accelerators for computing the above-mentioned cryptography functions	Compliant
11.	**Containers for user secret keys and certificates**	The chip shall have at least three (3) independent containers to securely store the user's private keys and certificates. The chip is expected to contain keys and secret certificates for the following purposes: (a) qualified certificate for electronic signature; (b) user identification; (c) secure email.	Compliant
12.	**Containers for user secret keys and certificates. Safety requirements**	Containers for storing user private keys and certificates shall comply with the information security requirements for storing qualified certificate for electronic signature as defined in point 23 of Article 3 of Regulation (EU) No 910/2014 [1] Appendix A, and one of the following standards: EN 419211, parts 1-6; FIPS 140-2 (Security Requirements For Cryptographie Modules), levels 3 or 4; EN ISO/IEC 15408, parts 1-5;	Compliant
13.	**PIN &PUK**	The chip shall support separate secure access mechanisms to each of the containers (1, 2, 3) using PIN (Personal Identification Number): PIN1, PIN2, PIN3 - for containers 1, 2, 3 respectively. The chip shall support PIN management using the PUK (Personal Unblocking Key).	Compliant
14.	**Qualified electronic Signature Creation Devices (QSigCDs)**	The Chip shall be certified as Qualified electronic Signature Creation Devices (QSigCDs) as defined in point 23 of Article 3 of Regulation (EU) No 910/2014 [1], Appendix A.	Compliant
15.	**Supported Standards**	ICAO Doc 9303, v. 12: BAC, PACE/ SAC, AA BSI-TR03110 [2] Appendix A	Compliant

16.	**Applications**	Manufacturer (Supplier) shall provide to Customer the following applications for working with the chip: lCAO BAC Application (MRTD), ICAO SAC/EAC (PACEv2) Application, EID Application, QDS Application (Secure Signature Creation Device).	Compliant
17.	**ICAO MRTD Application**	ICAO Application shall comply with the requirements set up in ICAO Doc 9303, Part 10, 11, 12. The list of DGs used and their formats shall be approved by the Supplier and the Customer at the stage of drafting the technical specifications	Compliant
18.	**MRZ/CAN**	Chip software shall support access control mechanisms based on MRZ and CAN.	Compliant
19.	**EAC Application**	EAC Application shall comply with the requirements of BSI-TR 03110 [2] Appendix A	Compliant
20.	**EID Application**	The EID application shall offer the possibility to work with additional user related data (p. 21), intended to further identify the owner, to provide contact information, etc.	Compliant
21.	**Additional user related data with separately defined access rights**	The chip shall have additional memory for storing additional user related data with separately defined access rights. Minimum available memory 35 kB. The content and formats of additional user related data shall be agreed between the Manufacturer (Supplier) and the Customer at the stage of drafting the technical specifications. Manufacturer (Supplier) shall provide to Customer with publicly available links to several examples (best practices) of the use of additional memory to store additional user related data.	Compliant See below the examples and links.
22.	**QDS Application**	QDS Application shall ensure chip operation as Qualified electronic Signature Creation Devices (QSigCDs)-Regulation (EU) No 910/2014, Article 3, point 23 [1], Appendix A. The same application shall be able to work with containers 2 and 3, which store the keys and certificates for holder authentication and secure email respectively.	Compliant

<table>
<tr><td>23.</td><td>Middleware</td><td>Middleware for the exploitation of the containers describes in (11) above, and the management of the PIN and PUK (13).
Middleware shall be delivered for all versions of Windows supported by Microsoft in 32 and 64 bits.
Middleware SDK shall be delivered for all Android and iOS versions supported.
Middleware shall support both contact and contactless interfaces with the card.
Middleware shall support the chip and application offered by the Manufacturer (Supplier).
Middleware shall be supported for the duration of the contract, with Maintenance services.</td><td>Compliant see §2.1.5</td></tr>
<tr><td>24.</td><td>SDK</td><td>Manufacturer (Supplier) shall provide to Customer an SDK for working with the chip, consisting in the complete documentation set for personalization,
200 test cards, sample personalization scripts as per personalization profile that will be defined by PSA.</td><td>Compliant</td></tr>
<tr><td rowspan="2">25.</td><td rowspan="2">Tests - key generation, digital signature execution, digital signature verification.</td><td>Chip Manufacturer (Supplier) shall provide to Customer the results of the following tests performed for the most popular algorithms, in the technical conditions satisfying the QSCD certification -
RSA 2048 bits, ECC 256 bits, ECC 384 bits:
Keys generating time (sample of at least 1000 tests);
Electronic signature execution time (sample of at least 100 tests);
Electronic signature verifying time (sample of at least 100 tests).</td><td>Compliant
See the table below.</td></tr>
<tr><td colspan="2">
<table>
<tr><th></th><th></th><th>Timing in seconds</th></tr>
<tr><td rowspan="2">RSA 2048 bits</td><td>Key generation</td><td>5</td></tr>
<tr><td>Signature</td><td>0,3</td></tr>
<tr><td rowspan="2">EC DSA 256 bits</td><td>Key generation</td><td>0,12</td></tr>
<tr><td>Signature</td><td>0,1</td></tr>
<tr><td rowspan="2">EC DSA 384 bits</td><td>Key generation</td><td>0,2</td></tr>
<tr><td>Signature</td><td>0,18</td></tr>
</table>
Electronic signature verifying time is not applicable.
Those are the timing from the card perspective (excluding computer process from the application or middleware) and is related to the card key generation or signature operation (hash operation are outside the process).
</td></tr>
</table>

26	**Security update on the field**	In case where a security vulnerability would be confirmed on the supplied product, the chip shall allow a way to update embedded software in a secure way. It shall be possible to apply the update the embedded software of the chip while the document has been already personalized and issued to the citizen. The update shall not alter the certifications of the products, nor reduce the available memory. Manufacturer (Supplier) shall bear all the direct costs related to the development and implementation of the update of the embedded software. Indirect costs related to the operational part of such update on the field (staff, eventual software deployment on IT infrastructure, communication) will be supported by the PSA.	Compliant

Use cases

The chip and OS proposed by SELP can serve for several use cases which create advantages for both the government and citizen.

Nationality proof 	The first purpose of a card is to allow a citizen to claim his citizenship wherever he is in the world. ICAO specifications allow governments to include technical mechanisms that enables police forces to authenticate the issuing State of the controlled card. This mechanism is called Passive Authentication.
Identity Control 	Reading the data stored in the chip allows anyone who is equipped with relevant technical means to make a correlation between the chip data and that printed on the card. The data included in the chip cannot be modified because it is sealed by the issuing State thanks to the Passive Authentication mechanism, which aims at digitally signing the holder data with a private key robust enough to guarantee their integrity.

The memory space may be used after eID issuance for different use case such as:

Health Records Integration: integration of medical prescription or partial history of medicine deliveries. Some vital information might also be stored (allergies, person to inform,….) and the eID may be a mean of access to dedicated web portal. For example, Estonian citizen can access their data by means of authentication with their eID cards.
Estonian e-Health Records (e-estonia.com)

Driving License Information: it might be possible to create a link between the driving license and the national eID card. The eID card would carry the driving licenses information and be able to be used for card rental or contracting insurance . This would allow citizen to only carry its eID card.
Everything You Need To Know About Digital Driver's Licenses [2024] (upgradedpoints.com)

Digital Voting: In countries where digital voting is allowed, citizens can use their eID cards to cast votes securely. The card's cryptographic features ensure the integrity and privacy of the voting process. For instance, in Belgium, citizens can vote online using their eID cards during elections.
Electronic voting by country - Wikipedia

Library Services: Citizens can use their eID cards to borrow books from libraries, access digital resources, and manage their accounts. The card acts as a library card, streamlining the borrowing process.

SELP

ID-One Cosmo X

Fulfilling the demand for flexibility and security from conception to post-issuance

ID-One Cosmo X is IDEMIA's leading modular Java Card Operating System (OS) that can store and update multiple applications with the highest level of certification, CC EAL5+ and EAL6+. This versatile platform can be used for a variety of solutions such as Government eID, eServices, health cards, voting, logical and physical access.

Compliant with the latest standards

Specifically designed for the demands and challenging requirements of the identity and multi-application government programs, ID-One Cosmo X is the most advanced Java Card (3.1 CE) and Global Platform (2.3) OS on the market. It provides guaranteed interoperability and security as required by governments.

Adapting to an evolving market

From conception to post-issuance, ID-One Cosmo X adapts to our clients needs:

- A tailor-made solution with Flexicode architecture
- IDEMIA's multi Match-on-card
- Various IDEMIA applets are supported
- Ready to host third- party Java Card applets

Effective and long-lasting security

The high level of security of ID-One Cosmo X is guaranteed thank to its Common Criteria Security Certification at the highest level, EAL5+ and EAL6+, state-of-the-art cryptography and cutting-edge security mechanism.

Additionally, thanks to JPatch, ID-One Cosmo X and IDEMIA's applets can remain secure throughout the lifetime of a document thanks to IDEMIA's exclusive and innovative solution.

The JPatch solution is a unique and innovative way to remotely upgrade IDEMIA's embedded software anytime, anywhere, even after the issuance of the ID document. This allows potential security or functional updates in the field.

Why IDEMIA?

As a technology innovator, IDEMIA is actively involved in industry standardization committees and security evaluations.
As a result, IDEMIA's products provide the latest security features within highly secure operating systems.

With over 135 active government IDEMIA is the global leader in civil identity solutions.
Our long-standing partnerships with governments are proof of the reliability and accuracy of our technology

Benefits

Interoperability

- Ability to load third part applications
- Open standardized services

Flexibility

- New applications can be loaded after card issuance to provide a dynamic response to citizen's changing needs during the smart card lifecycle
- Multiple applets can be loaded on a single card

Innovative

ID-One Cosmo X is IDEMIA's versatile solution with:

- CC EAL5+ and EAL6+ security certification as an open platform
- Biometrics (face, fingerprint and iris)
- JPatch to ensure long-lasting security
- JBox to provide flexibility at cryptography level
- Flexicode for modularity at conception level

ID-One Cosmo X

Corporate cards | Travel documents | eID cards (national residence permits) | Health cards | Driver's licenses

Communication Interface and protocol

- Dual interface
- Contact: ISO/IEC 7816-3
- Contactless: ISO/IEC 14443
- Type A and B up to 848Kb/s (3.4Mbps in option)
- Extended APDU
- Secure messaging

Chip

- Infineon SLC37GDx512
- Certified CC EAL6+

User memory

- From 180K to 235K

Standards

- Java Card 3.1 CE
- Global Platform 2.3
- ISO/IEC 7816,14443
- ICAO 9303 Edition 8
- ISO/IEC 18013
- ISO/IEC TR 19446
- Minex II

Security

- DES/3DES
- AES up to 256bits
- RSA up to 4096 bits
- ECC up to 521 bits
- SHA-1, SHA-2, SHA-3 Family
- Advanced accelerator Java Card API for PACE GM and IM
- SCP02, SCP03

Security services

- PIN/PUK verification
- Electronic signature (QSCD)
- Data Decryption/Encryption
- Multi Match-on-Card
- RSA/ECC On Board Key Generation
- JPatch
- JBox

Security mechanisms

- Active Authentication
- Passive Authentication
- Chip/Terminal Authentication
- Basic Access Control
- PACE GM, IM
- PACE CAM (in option)
- EAC V1

Supported IDEMIA applets

- CombICAO
- ID-A
- TnD
- PIV
- TachoDrive v4

Security certifications

Open Platform certified **EAL5+ and EAL6+** according to the following protection profile: Java Card protection profile – Open Configuration – Version 3.0.5

SELP

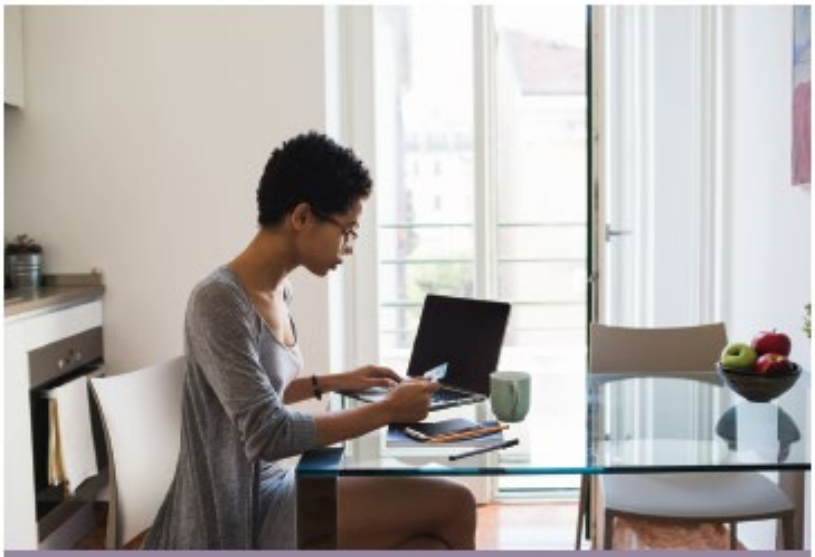
JPatch

Ensuring long-lasting security in embedded software

Passports, identity cards and residence permits are expected to have a substantial lifespan, usually ten years. Due to this length of time, security erosion of embedded OS is a growing concern, as hacking and fraud capabilities are progressing. The longer the lifespan of an eDocument, the higher the possibility of security erosion of the embedded software. How to reconcile these two trends?

JPatch is an advanced technology developed by IDEMIA to enable remote upgrades of the JavaCard embedded software without altering the user's data in the eID document.

Thanks to JPatch, a high level of security can be maintained over the lifetime of an identity document.



Why IDEMIA?

With over 3 billion identity documents issued worldwide, IDEMIA fully understands the market's needs for identity documents that are trustworthy and reliable.

IDEMIA is actively involved in industry standardization committees and security evaluations. Our products provide the latest security features within highly secure operating systems (over 190 CC certified products on ANSSI website).

By having an OS that is natively designed to be upgraded in the field, IDEMIA demonstrates its commitment to maintaining the highest level of security.

Convenience

Upgrades on JavaCard embedded software can be done anytime, anywhere, in a seamless manner, through IDEMIA's CMS.

High level of data protection and privacy

There is no need to safeguard the data outside the embedded document, and no need to restore the binding between issuing authority, document holder and ID document.

Cost and time efficiency

With JPatch, when a card needs to be updated there is no need to apply for a new one. The current card can be upgraded, thereby avoiding unnecessary cost and time spent on a replacement.

Effective and long-lasting memory management

JPatch has a negligible impact on IDEMIA's initial user data memory provision.

JPatch, an exclusive technology to upgrade embedded software in the field

Jpatch is an innovative and unique solution to remotely update OS and applets in the field. It allows security and/or functional issues to be corrected and upgraded directly on the embedded software. Upgrades can be done even after the issuance of the ID document.

- By ensuring the embedded software always remains protected against attacks, JPatch guarantees the highest level of security over the lifetime of an identity document.
- Furthermore, this solution maintains the confidentiality and privacy of the user data stored on the document.

Technical specifications

Long lasting security

Thanks to JPatch, the highest level of protection is guaranteed for embedded software.

As soon as a security risk is detected on a smart card in circulation, IDEMIA is able to remove the threat by securely updating the operating system remotely.

These remote updates allow corrections of functional and/or security issues.

A high level of data protection and privacy

JPatch technology does not erase, modify, or put at risk the user's data that is stored in the embedded software.

In particular, the following data is maintained:

- Personal data is unaffected during the upgrade, Therefore it is not necessary to safeguard it outside the embedded software. This approach guarantees the confidentiality and privacy of the data.
- Technical data (certificates, private keys, PIN etc.) also remains on the card, so it is not necessary to generate and import it after the upgrade.

The association between the card, the holder and the issuer is maintained.

Effective and long-lasting memory management

JPatch preserves the memory size dedicated to users' data. Using JPatch to update documents does not reduce the amount of memory that is available for user data throughout the lifetime of the document.

Updates are implemented in a precise, targeted manner, and only overwrite the code in question.

Certifications and standards

Common Criteria Certified

Compliant with security standards

- SOG IS application note for code loading in use phase
- ANSSI CC Note 6

2.1.5 THE MIDDLEWARE

The middleware is the licensed software enabling interfacing the PKI applet to most commons IT systems (like Windows log on, Microsoft Outlook to sign emails, etc…). It is compatible with a wide range of environment (Windows, Linux, MacOS, Android, iOS.) and use cases (PKI, Strong Authentication, Smartcard Log On, Network Access, VPN Access, Remote Access and Biometry).

The proposed middleware is Universal Middleware for Cryptographic devices including SW libraries.

The proposed Universal Middleware is PKCS#11 with support to Microsoft CSP-NG, Apple TokenD/CryptoTokenKit, Android OS, Apple iOS and most relevant Linux distributions.
It is designed to be agnostic of the very specific security IC and it supports wide range of IC's.

The Middleware is fully compliant to the requirements as requested:

- Middleware for the exploitation of the containers describes in (Req. n°11) above, and the management of the PIN and PUK (Req. n°13).
- Middleware shall be delivered for all versions of Windows supported by Microsoft in 32 and 64 bits.
- Middleware SDK shall be delivered for all Android and iOS versions supported.
- Middleware shall support both contact and contactless interfaces with the card.
- Middleware shall support the chip and application offered.
- Middleware shall be supported for the duration of the contract, with Maintenance services (5 Years warranty of the middleware)
    - Bug fixing - Adaptive/Corrective

2.2 MOLDOVA CHIPLESS PC CARD (DL AND VP)

1.1.2 KEY CHARACTERISTICS

Model	One model is proposed for: – Moldova chipless DL PC card (DL) - DL – Moldova chipless VP PC card (VP) - VP
Material	Polycarbonate (PC) card with multi-layer structure
Format	The card format complies with the international norms - ISO/IEC 7810 standard, i.e. 85.6 x 53.98 mm (ID1 format). - ISO/IEC 7501-1 - ISO/IEC 7501-3 - ISO/IEC 10373-1/3/6: 2006 - ISO/IEC 7816 - ISO/IEC 18013-4 **(DL only)**
Design	The Design projects of the cards, provided by PSA, will include the final design of the document's background (high-quality vector and raster graphics) with the document name and data field names, requirements for the positioning and shape of security features, as well as a description of the inks used and their characteristics (e.g., color transition in iris print). The files will be presented in PDF and/or CGT (Corvina) format, for each separate layers and colors.
Interface	The card is chipless.
ICAO Compliance	The proposed card fully complies with the ICAO recommendations specified in the latest version of Doc 9303 and its supplements. It is therefore machine-readable.
European Regulations	Directive 20061126/CE of the European Parliament and of the Council of 20 December 2006 on driving licences; Council Directive 1999/37 ICE of 29 April 1999 on the registration documents for vehicles;
Durability	The card will have a lifespan of at least 10 years in normal operation. To guarantee this durability, SELP subjects all its security components to the most stringent resistance tests.

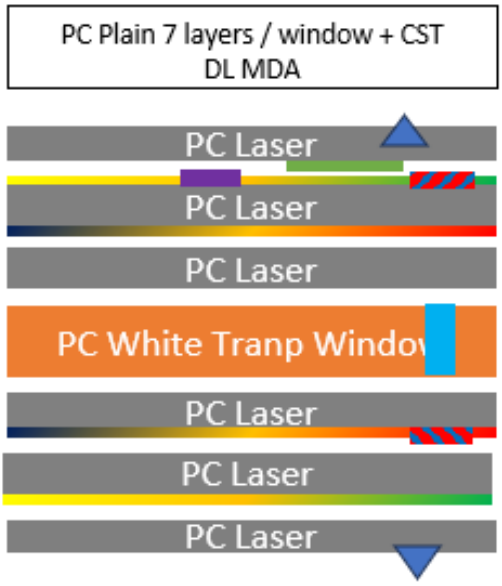
2.2.1 CARD STRUCTURE

The identity card we offer is a polycarbonate card with a secure construction that allows a personalisation at the heart of the card, protected by printing and DOVID.

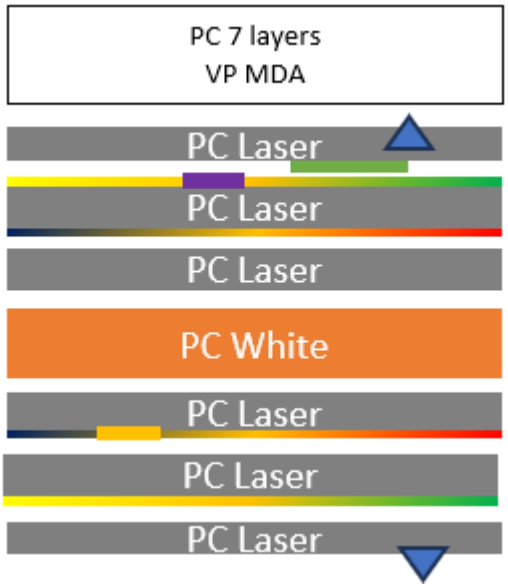
Polycarbonate is a plastic material with excellent mechanical properties and high thermal resistance. It has a lifespan of around 10 years (without any degradation). It has high mechanical and thermal resistance, and can be used to personalize data at the heart of the card, as well as incorporating security features to combat counterfeiting and falsification.

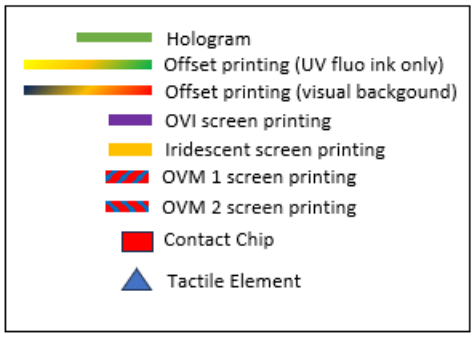
The proposed identity card is made of **seven layers of Polycarbonate** material.

DL card structure



VP card structure



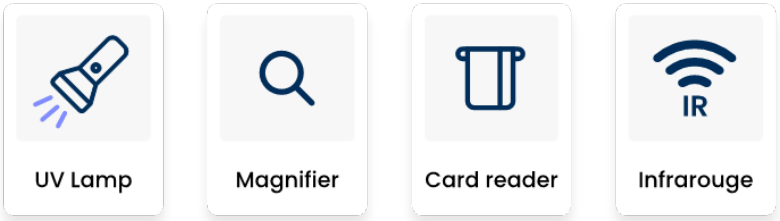


2.2.2 SECURITY FEATURES

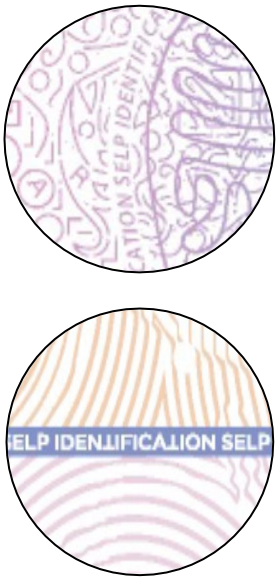
Additional securities are described in this offer with the following pictograms:

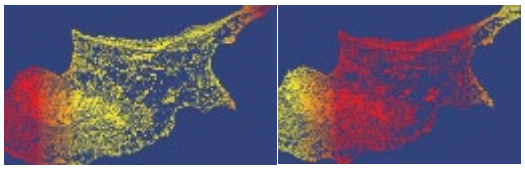
The first level (overt) relates to security features that the public can easily check, without special aids.

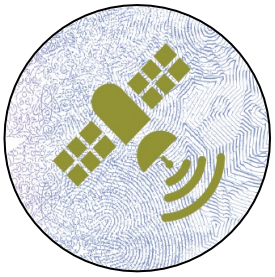
Second-level (covert) relates to security features that can be checked with simple tools.

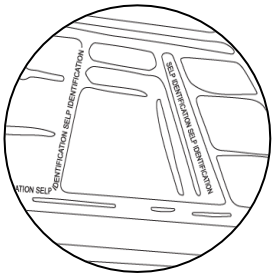


Third-level (forensic) security features are for qualified forensic laboratories and other sophisticated laboratory equipment.

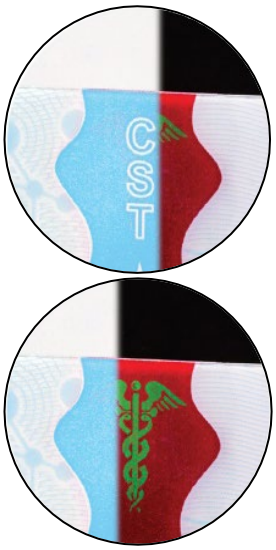
Specifications for card body		
UV Dull polycarbonate	A UV dull substrate is a substrate with no bleaching agents in its composition and therefore which has **no fluorescence under UV light**. This characteristic enables the use of fluorescent inks under UV. This will make evident such attacks as adding a laminate which would react under UV light and be easily detected.	
Guilloches	Guilloches background is made up of fine lines arranged in random, geometric patterns. The patterns, unique to each project, are effective against attempts at falsification by abrasion. They are generated using software accessible only to high-security printers and are very difficult to reproduce by standard means, limiting the risk of counterfeiting.	
Anti-scanning Anti-copy	One anti-copy method is based on changing line thickness and distance, but still keeping the ink coverage constant. The idea with this approach is that the counterfeiter's process would not be so accurate and different color shades would be visible due to variation in line width and distance in between single lines.	
Invisible micro-lettering (positive and negative)	Micro-lettering is the micro printing of a word or a sentence which is not visible to the naked eye and is easily mistaken for a simple line. This element can be integrated into the background of the document or used to highlight an element.	

Delibarate error	A specific design will be created with deliberate error.	
Rainbow printing	Rainbow printing is achieved using specially adapted offset machines. It's generated by blending two colours in a controlled manner, to create a subtle color transition. Its control is made all the easier by the fact that its integration into the design is optimized by the know-how of our designers.	
Invisible and fluorecent under UV-A and UV-B rainbow printing	Rainbow printing is achieved using specially adapted offset machines. It's generated by blending two colours in a controlled manner, to create a subtle color transition. Its control is made all the easier by the fact that its integration into the design is optimized by the know-how of our designers. The ink used for this features is invisible under normal light and appear fluorescent under UV-A & UV B.	
Metameric ink pair **IR**	Infrared (IR) abs / trans inks look the same under normal light. They are both visible for the human eye. When looking with a special IR light source, only IR abs inks are visible. These inks provide additional copy protection. The verification requires IR light source which are not so common.	

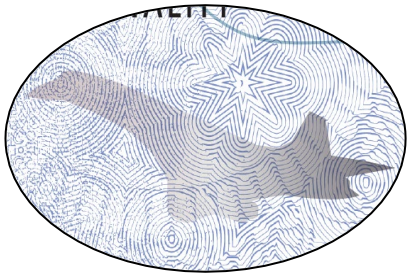
Optically Variable Ink (OVI) with UV	Optically Variable Ink is an optical security feature characterized by a unique and striking color-shift that is visible to the naked eye simply by titling the document. OVI distinguishes itself by its high chromaticity and a long color travel. Two OVI are proposed in new electronic identity card, one integrated into the front side	 
Semi-transparent DOVID	The polycarbonate card will be protected with a Semi-transparent DOVID (Diffractive Optical Variable Identification Device) embedded in the core of the card at lamination stage. The DOVID, is mainly a level 1 security feature, controllable with the naked eye by titling the card. It also embeds level 2 and level 3 security features. DOVID will display the following feature: - maintained in the same plane and angle of light reflection, the two distinct reflective colors of the DOVID will interchange at any 90° rotation. - by tilting "DOVID" up and clown, part or the entire surface of the two colored reflective areas will simultaneously display animations in opposite directions. - a part of one of the two colored reflective areas forms an object that renders a positive 3D relief effect on the "DOVID" surface. Area size: minimum 31mm x 31mm. The same Dovid will be used for all type of cards.	

Relief embossing	A relief embossing is created during the card lamination stage. Extreme pressure fuses the polycarbonate layers together and creates a relief. The relief features created by the lamination process are effective against counterfeiting and data tampering. Several features can be included: guilloches, micro-lettering, matte effect, super tactile effect, etc. Combining them adds complexity to the design in order to avoid counterfeiting and falsification (by overlaping a lamina), and must be worked on in conjunction with the design of the cards. Relief embossing will be the same for all the type of cards.	 
CLI/MLI	Changeable or multiple laser image (CLI / MLI) consists of personalization of typically two data through a lens on the ID document surface. The two sets of data are alternately visible when tilting the document. CLI/MLI will be on the backside of the card	

Specifications for Driving License (DL) card body ONLY

Transparent window with CST ink	Transparent window with color change (the transparent area will change its color according to the color of the background on which it is viewed, using technology with which the material used will have the effect of optical change): - on light background: the window will have a primary color (blue); - on dark background: the window will change its hue to a second color (red), and an image will appear as a third color (yellow-green) as an embedded image; - the embedded image will also be reactive to UV light (yellow-green fluorescence). Area size: 10 mm x 12 mm. The transparent window will accept laser engraving at the personalization stage.	

Specifications for Vehicle Registration (VP) card body ONLY

Iridescent Ink	Thanks to iridescent inks and their unique property of reflecting incident light, we can observe effects of brilliance and invisibility depending on the angle of observation. This feature makes it an interesting choice for protecting an ID card, as it makes it more difficult to scan or copy the document using traditional equipment.	

2.2.1 PRE-PERSONALIZATION

The purpose of an Identity document is to store personal information that enables a person to be identified with certainty. The certainty with which another person can be identified derives not only from the security of the card itself, but also from the way in which the data is securely stored on the card.

Specifications for the card personalization		
Unique sequencial card number	At the manufacturing stage, in order to secure the management of cards movement, each card shall be assigned with a sequential number, applied in a 1D barcode, placed on the backside of the card and will ensure the consecutive numbering of the cards.	

3 CARD PACKAGING

SELP will provide a specific packing of cards as specified by PSA to prevent their damage or deterioration during transit to their final destination. Our packing procedure had been made to comply with PSA requirements and to withstand, without limitation, rough handling and exposure to extreme temperatures, salt and precipitation, and open storage.

Packing case size and weights will be take into consideration as peer as PSA requirements.

Grouping of cards

	Inner box	Outer box	Pallet
Cards	500	2 000	100 000
Inner box		4	200
Outer box			50

3.1 INNER BOXES

Cards are put in sequence on the inner boxes in ascending order.

Capacity of the inner box is 500 cards

Size: 450 x 90 x 40 mm

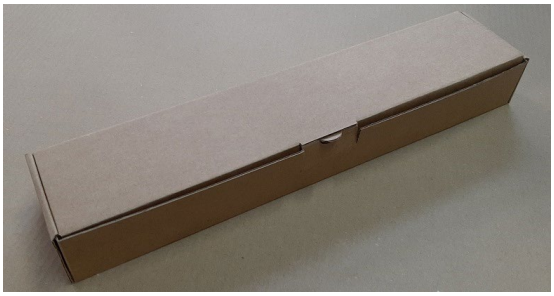


Figure 1 Exterior of the inner box

Last serial number of the inner box

First serial number of the inner box
Front of the micromodule if it's a contact smartcard.

Figure 2 Inner box filled with cards

The inner box will be closed with security tape.

Figure 3 Security sealing (VOID marking)

A logistic label will be applied on the front face of the inner box.

Standard label for box

Information on the label:

- Client's name
- Client's code of the card (if any)
- SELP Manufacturer (name or Logo)
- Designation of the card
- Box number (digits and barcode)
- Quantity of cards in the box
- Range numbers of identity cards contained in the box.

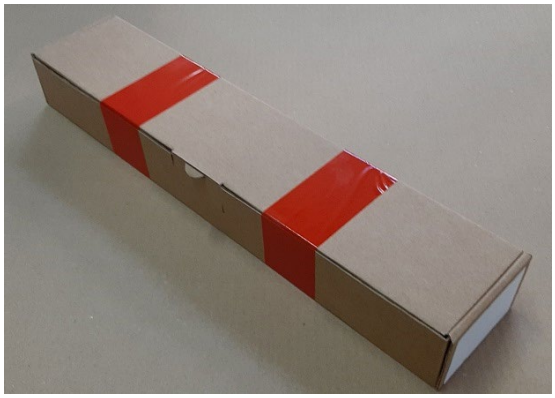


Figure 4 Sealed inner box with label sticked on the front face of the tray.

3.2 CARBOARDS

Format of the carboard: 2000 cards, 4 inner boxes

External size: 464 x 199 x 143 mm

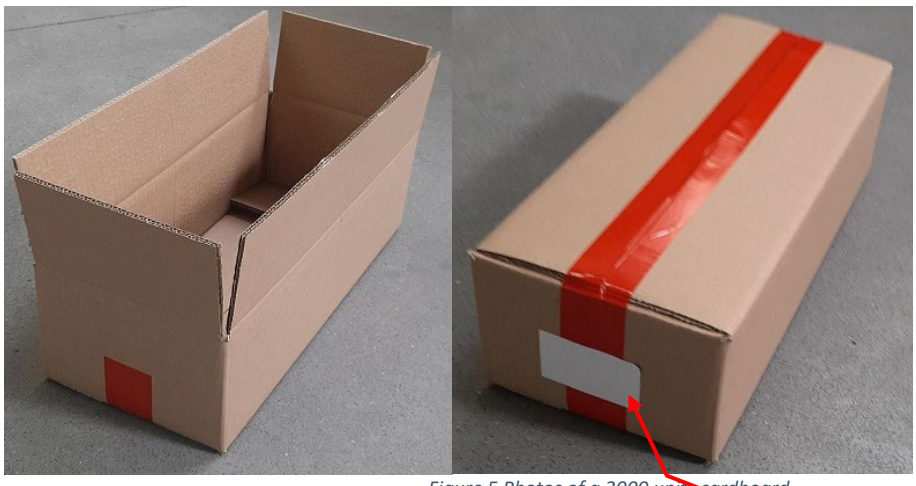
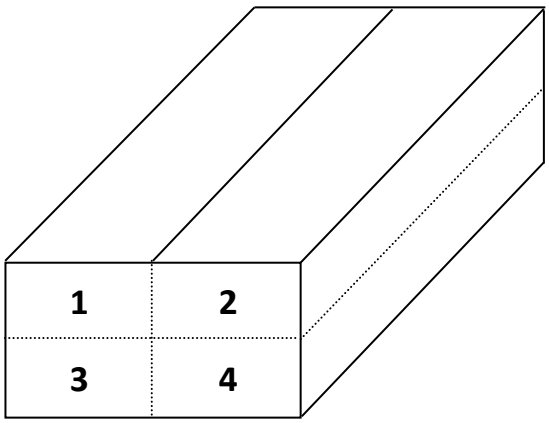


Figure 5 Photos of a 2000 units cardboard

Label sticked on the upper left corner of the small side of the cardboard (same side as the inner box labels)

Storage of the trays in a cardboard :



Notice: if the cardboard is incomplete (before shipment), it will be completed with empty trays without labels.

Standard label for cardboard

Information on the label:

- Client's name
- Delivery address
- Order reference
- Sign shall be displayed on box :
    - "Careful when transporting"
    - "Do not throw"
    - "Store in a dry place"
- Selp Manufacturer (name and address)
- Origin country
- Designation of the card
- Box number (digits and barcode)
- Quantity in each cardboard
- Range numbers of identity cards contained in the box.