**Technical specification of polycarbonate ID1 prelams with contactless chip modules equipped with ICAO travel application**

# Technical specification of ID1 polycarbonate prelams

## Prelam technical specification:

* 15up format (3x5)
* to made from polycarbonate layers
* polycarbonate layers must be compatible with the Makrofol® ID layers from company Covestro in order to maintain the compatibility of the lamination process with existing layers
  + client requires to know which structure have the polycarbonate layers in prelam
  + in the case of the use of polycarbonate layers other than Makrofol® ID layers, client requires an explicit compatibility guarantee with the Makrofol® ID layers in production process in STC
* the contactless module must be appropriate for long life ID cards and contactless module area must be protected against cracking
* Wired antenna
* maximum thickness of prelam must be 350µm including tolerance
  + client prefers lower thickness than maximum
  + client allows prelam with white overlays
* Sheet layout: 

**Obsah obrázku text, mapa

Popis byl vytvořen automaticky**

## Chip technical specification

* Algorithm support: RSA, ECC, ECDH, ECDSA, 3DES
* Min 80kB of memory available for user data
* Minimum retention time 20 years.
* Minimum read/write endurance – 500.000 cycles

## Chip OS technical specification

* Support of ICAO application according to ICAO DOC9303
* Support of hashing algorithm up to SHA-512
* Preferable cryptographical configuration:
  + RSA for Active Authentication
  + NIST-P256 elliptic curves for both Terminal and Chip Authentication
* Support of BAC
* Support of EAC 1.11
* Support of Passive Authentication
* Support of Active Authentication
* Support of SAC/PACE
* On board key generation for CA and AA
* Chip modules must be initialized and pre-personalized (ICAO LDS structure v 1.7 has to be created) by the Seller according to Buyers requirements.
* Chip modules must be secured by transport keys. The key ceremony has to be established between STC and chip modules provider (OS provider).
* KCV (transport key verifier code) must be stored in chip module for automatic recognition of used transport key.

## Key management and transport ceremony between inlay supplier and STC Transport key diversification

### Preamble

This document describes transport key ceremony required between STC and inlay supplier and the diversification used.

### Terminology

|  |  |
| --- | --- |
| *Daughter transport key (TKICC)* | *Specific card (chip) transport key (diversified using mother transport key and using specific card data (serial chip number for example)* |
| *Key diversification* | *New key is generated using mother transport key and specific card data during this process* |
| *Inlay supplier (IS)* | *Inlay with chip module supplier* |
| *Key Check Value (KCV)* | *Key value verifying code. This code is used for key identification* |
| *Mother transport key (TKM)* | *Collective transport key for batch of inlays* |
| *ED* | *Electronic Document* |
| *ED issuer (MOI)* | *Issuer of ED is Ministry of Interior.* |
| *ED producer (STC)* | *Producer of ED (embedding, security printing, and personalization) is State Printing Works of Securities.* |
| *Zone Master Key (ZMK)* | *This key is securing transport of Mother transport keys between STC and inlay supplier.* |
|  |  |

### Key ceremony description

Key ceremony description is based on following basis:

* ZMK is generated by inlay supplier.
* Mother transport key is generated by inlay supplier.
* Inlay supplier initializes the inlays using daughter transport keys that are derived from collective mother transport key (TKM).
* Inlay supplier writes in to the inlay specific data during initialization. Those data are specifying used mother transport key (TKM).
* ZMK and Keys between inlay supplier and ED producer are exchanged using Key Ceremony.

#### ZMK key ceremony

Zone Master Key (ZMK) is generated by inlay supplier. ZMK is split in to 3 parts that are distributed and shipped in different dates to ERP producer in following way:

* Partial key ZMK 1 is send to the key custodian 1, in a tamper proofed sealed envelope (Courier A)
* Partial key ZMK 2 is send to the key custodian 2, in a tamper proofed sealed envelope (Courier B)
* Partial key ZMK 3 is send to the key custodian 3, in a tamper proofed sealed envelope (Courier C)

#### TKM key ceremony

Mother transport key (TKM) is generated in HSM of inlay supplier. TKM is encrypted using ZMK and transported to ED producer.

#### Key exchange technical description

Used cryptographic terminology is summarized in following table:

|  |  |
| --- | --- |
| *Term* | *Definition* |
| * *ZMK* | * *Zone Master Key* |
| * *TKM* | * *Mother transport key* |
| * *TKM´* | * *Encrypted mother transport key* |
| * *TKICC/TYPE* | * *Card specific daughter transport key* |
| * *EKEY(DATA)* | * *Encrypted DATA using key (AES256 ECB encryption)* |
| * *DKEY(DATA)* | * *DATA decryption using key (AES256 ECB encryption)* |
| * *(+)* | * *XOR (exclusive OR)* |
| * *||* | * *Data concatenation* |
| * *AES256* | * *AES 256 bit symmetric encryption algorithm* |
| * *RND(COUNT)* | * *Buffer containing COUNT random bytes* |
| * *ZERO(COUNT)* | * *Buffer of COUNT zero bytes* |
| * *?=?* | * *Compares left and right operand* |
| * *=* | * *Equals left value to right value* |
| * *KCV* | * *Key Check Value– key value verifying code, is used to verify ZMK and TKM´ using encrypted zero buffer* |
| * *DIVKEY(I,DATA)* | * *Diversification of KEY key using diversification data DATA. Diversification is realized using KDF in counter mode as specified in* ***NIST 800-108****. The PRF used in the KDF shall be CMAC. Parameter I denotes number of iterations.* * *Please see example of data coding in Appendix 1.4.4.1.* |
| * *CMAC(K, M)* | * *Cipher-based Message Authentication Code (as specified in* ***NIST 800-38B****) of message M using key K.* |
| * *||* | * *Data junction* |
| * *FIRSTN(DATA)* | * *First N bytes of DATA buffer* |
| * *LASTN(DATA)* | * *Last N bytes of DATA buffer* |
| * *NNh* | * *Hexadecimal notation of NN number, e.g. 1Fh* |
| * *AA:BB:CC:DD* | * *Octet string of specified number of bytes written in hexadecimal notation, e.g. 12:34:56:AB* |

*Tab. 1 Transport key distribution terminology*

##### Generation and distribution of ZMK key

1st phase of key ceremony is generation and distribution of ZMK key.

***Detailed description is part of classified information. Will be provided as a separate document.***

##### Generation and distribution of TKM key

2nd phase of key ceremony is generation and distribution of ZMK key.

***Detailed description is part of classified information. Will be provided as a separate document.***

##### Diversification and storing of TKICC keys into the chips

3nd phase of key ceremony is generation and distribution of ZMK key.

***Detailed description is part of classified information. Will be provided as a separate document.***

### Appendixes

#### AES 256 key diversification data coding example

This chapter shows proposed algorithm implementation for 256 AES ISK key output.

***Detailed description is part of classified information. Will be provided as a separate document.***

#### Scheme of key ceremony process



*Figure 1 Key ceremony process*

# Documentation

## Certification

Product must be certified according following requirements:

* Common Criteria, minimum EAL 5 for chip.
* Common Criteria, minimum EAL 4+ for operating system and ICAO application.

## Conformity with following standards

* Consolidated text: Council Regulation (EC) No 2252/2004 of 13 December 2004 on standards for security features and biometrics in passports and travel documents issued by Member States amended by Regulation (EC) No 444/2009 of the European Parliament and of the Council of 28 May 2009
* Regulation (EU) 2017/1954 of the European Parliament and of the Council of 25 October 2017 amending Council Regulation (EC) No 1030/2002 laying down a uniform format for residence permits for third-country nationals;
* 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
* ICAO 9303 - Machine Readable Travel Documents, Seventh Edition (2015)
* BSI TR-03110 – Advanced Security Mechanism for Machine Readable Travel Documents, v2.10
* ICAO TR-SAC v1.01
* ISO/IEC 15946
* ISO/IEC 7816-3
* ISO/IEC 14443
* ISO/IEC 10373

## Required documentation to be delivered within the official tender (further details are stated in the Tender Documentation)

* Prelam technical drawing
* Chip module datasheet/documentation
* Operating system datasheet and documentation
* Operating system personalization documentation
* CC Certification reports and protocols (both chip and OS)
* Relevant Security targets
* ICAO (RF protocol and Application Test Standard for E-Passport)/BSI (BSI TR-03105) biometric Conformity testing reports L1-L7
* Official statement or any kind of certificate confirming the product is resistant to both ROCA and MINERVA vulnerabilities in case of using the preferred cryptographical configuration according to 3.1.

# Samples

## Samples to be delivered

Preferable cryptographical configuration of the samples:

* + RSA for Active Authentication
  + NIST-P256 elliptic curves for both Terminal and Chip Authentication
* Set 1:
  + 20pcs of white ID1 testing cards, generic initialization with testing generic transport key, LDS configuration upon request of Client
  + Documentation for personalization:
    - Personalization manual
    - Example of personalization script
  + To be delivered as a part of official tender (further details are stated in the Tender Documentation *(main document)*)
* Set 2:
  + 20pcs of white ID1 testing cards, specific initialization according to requirements of the Buyer, testing diversified transport key, testing key ceremony implemented, LDS configuration upon request of Client
  + Documentation for personalization:
    - Personalization manual
    - Example of personalization script
  + Providing of the samples after the Contract signature
* Set 3:
  + 15 sheets of testing prelams, specific initialization according to requirements of the Buyer, testing diversified transport key, testing key ceremony implemented, LDS configuration upon request of Client
  + Documentation for personalization:
    - Personalization manual
    - Example of personalization script
  + Providing of the samples after the Contract signature