**Key management and transport ceremony between chip supplier and STC**

**Transport key diversification**

# Preamble

This document describes transport key ceremony required between STC and chip 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 |
| Chip supplier (IS) | 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 chips |
| ED | Electronic Document |
| ED issuer (MOT) | Issuer of ED is Ministry of Transport. |
| 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 chip supplier. |
|  |  |

# Key ceremony description

Key ceremony description is based on following basis:

* ZMK is generated by chip supplier.
* Mother transport key is generated by chip supplier.
* Chip supplier initializes the chips using daughter transport keys that are derived from collective mother transport key (TKM).
* Chip supplier writes in to the chip specific data during initialization. Those data are specifying used mother transport key (TKM).

ZMK and Keys between chip supplier and ED producer are exchanged using Key Ceremony.

## ZMK key ceremony

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

* Partial key ZMK 1 is sent to the key custodian 1, in a tamper proofed sealed envelope (Courier A)
* Partial key ZMK 2 is sent to the key custodian 2, in a tamper proofed sealed envelope (Courier B)
* Partial key ZMK 3 is sent 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 chip 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 0. |
| 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

Obsah obrázku text, diagram, Plán, mapa

Obsah vygenerovaný umělou inteligencí může být nesprávný.

Figure 1 Key ceremony process