KEY CEREMONY (NON-CLASSIFIED PART)

Key management and transport ceremony between chip supplier and STC Transport key diversification

1 Preamble

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

2 Terminology

Daughter transport key (TK_{ICC})	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 (TK_M)	Collective transport key for batch of chips
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 chip supplier.

3 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 (TK_M).
- Chip supplier writes in to the chip specific data during initialization. Those data are specifying used mother transport key (TK_M).

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

3.1 ZMK key ceremony

Zone Master Key (ZMK) is generated by chip 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)

3.2 TK_M key ceremony

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

3.3 Key exchange technical description

Used cryptographic terminology is summarized in following table:

Term	Definition
ZMK	
TK_M	
TK_M'	
$TK_{ICC/TYPE}$	
$E_{KEY}(DATA)$	
$D_{KEY}(DATA)$	
(+)	
||	
AES256	
RND(COUNT)	
ZERO(COUNT)	
?=?	
=	
KCV	
$DIV_{KEY}(I,DATA)$	
CMAC(K, M)	
||	
$FIRST_N(DATA)$	
$LAST_N(DATA)$	
NN_h	

Tab. 1 Transport key distribution terminology

3.3.1 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.

3.3.2 Generation and distribution of TK_M 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.

3.3.3 Diversification and storing of TK_{ICC} 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.

1 Appendixes

3.4 AES 256 key diversification data coding example

This chapter shows proposed algorithm implementation for [redacted] 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