IDPrime PIV v3.0 Applet on IDCore 3130 Platform
FIPS 140-2 Cryptographic Module
Non-Proprietary Security Policy

Table of Contents

Table of Tables

Table of Figures

References

Acronym	Full Specification Name
[FIPS140-2]	NIST, *Security Requirements for Cryptographic Modules*, May 25, 2001
[GlobalPlatform]	*GlobalPlatform Consortium: GlobalPlatform Card Specification 2.2.1,* January 2011, http://www.globalplatform.org
[ISO 7816]	ISO/IEC 7816-1:1998 *Identification cards -- Integrated circuit(s) cards with contacts -- Part 1: Physical characteristics* ISO/IEC 7816-2:2007 *Identification cards -- Integrated circuit cards -- Part 2: Cards with contacts -- Dimensions and location of the contacts* ISO/IEC 7816-3:2006 *Identification cards -- Integrated circuit cards -- Part 3: Cards with contacts -- Electrical interface and transmission protocols* ISO/IEC 7816-4:2005 *Identification cards -- Integrated circuit cards -- Part 4: Organization, security and commands for interchange*
[ISO 14443]	*Identification cards – Contactless integrated circuit cards – Proximity cards* ISO/IEC 14443-1:2008 Part 1*: Physical characteristics* ISO/IEC 14443-2:2010 Part 2: *Radio frequency power and signal interface* ISO/IEC 14443-3:2011 Part 3: *Initialization and anticollision* ISO/IEC 14443-4:2008 Part 4: *Transmission protocol*
[JavaCard]	*Java Card 3.0.5 Runtime Environment (JCRE) Specification* *Java Card 3.0.5 Virtual Machine (JCVM) Specification* *Java Card 3.0.5 Application Programming Interface* Published by Sun Microsystems, October 2015.
[SP800-131A Rev. 2]	NIST Special Publication 800-131A revision 1, *Transitions: Recommendation for Transitioning the Use of Cryptographic Algorithms and Key Lengths*, March 2019
[SP 800-133]	NIST Special Publication 800-133, *Recommendation for Cryptographic Key Generation*, December 2012
[SP 800-38B]	NIST Special Publication 800-38B, *Recommendation for Block Cipher Modes of Operation: the CMAC Mode for Authentication*, May 2005
[SP 800-90A]	NIST Special Publication 800-90A revision 1, *Recommendation for the Random Number Generation Using Deterministic Random Bit Generators (Revised)*, June 2015
[SP 800-67 Rev. 2]	NIST Special Publication 800-67 revision 2, *Recommendation for the Triple Data Encryption Algorithm (Triple-DES) Block Cipher*, November 2017
[FIPS113]	NIST, *Computer Data Authentication*, FIPS Publication 113, 30 May 1985.
[FIPS 197]	NIST, *Advanced Encryption Standard (AES)*, FIPS Publication 197, November 26, 2001.
[PKCS#1]	*PKCS #1 v2.1: RSA Cryptography Standard*, RSA Laboratories, June 14, 2002
[FIPS 186-4]	NIST, Digital Signature Standard (DSS), FIPS Publication 186-4, July, 2013
[SP 800-56A Rev. 3]	NIST Special Publication 800-56A Revision 3, *Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography*, April 2018
[SP 800-56B]	NIST Special Publication 800-56B revision 1, *Recommendation for Pair-Wise Key-Establishment Schemes Using Integer Factorization Cryptography*, September 2014
[FIPS 180-4]	NIST, *Secure Hash Standard*, FIPS Publication 180-4, August 2015

Acronym	Full Specification Name
[SP 800-38F]	NIST Special Publication 800-38F, *Recommendation for Block Cipher Modes of Operation: Methods for Key Wrapping*, December 2012
[IG]	NIST, *Implementation Guidance for FIPS PUB 140-2 and the Cryptographic Module Validation Program,* last updated February 2019.
[SP800-73-4]	NIST Special Publication 800-73-4, *Interfaces for Personal Identity Verification – Part 1: PIV Card Application Namespace, Data Model and Representation,* May 2015.
[SP800-78-4]	NIST Special Publication 800-78-4, *Cryptographic Algorithms and Key Sizes for Personal Identity Verification,* May 2015
[SP800-76-2]	NIST Special Publication 800-76-2, *Biometric Specifications for Personal Identity Verification,* July 2013.
[FIPS201-2]	NIST, *Federal Information Processing Standard 201-2, Personal Identity Verification (PIV) of Federal Employees and Contractors,* August 2013.

Table 1 – References

Acronyms and Definitions

Acronym	Definition
API	Application Programming Interface
CM	Cryptographic Module
CSP	Critical Security Parameter
DAP	Data Authentication Pattern, see [GlobalPlatform]
DM	Delegated Management, see [GlobalPlatform]
DPA	Differential Power Analysis
GP	Global Platform
HID	Human Interface Device (Microsoftism)
IC	Integrated Circuit
ISD	Issuer Security Domain, see [GlobalPlatform]
KAT	Known Answer Test
OP	Open Platform (predecessor to Global Platform)
PCT	Pairwise Consistency Test
PKI	Public Key Infrastructure
SCP	Secure Channel Protocol, see [GlobalPlatform]
SSD	Supplementary Security Domain, see [GlobalPlatform]
SPA	Simple Power Analysis

Table 2 – Acronyms and Definitions

1. Introduction

This document defines the Security Policy for the Gemalto IDPrime PIV v3.0 Applet on IDCore 3130 Platform cryptographic module (CM), herein denoted the *Module*. The *Module*, validated to FIPS 140-2 overall Level 2, is a single-chip "dual" module implementing the Global Platform operational environment, with Card Manager, PIV, PIV Admin and MoC Server (Biometric Match-on-Card) Applets.

The *Module* is a limited operational environment under the FIPS 140-2 definitions. The *Module* includes a firmware load function to support necessary updates. New firmware versions within the scope of this validation must be validated through the FIPS 140-2 CMVP. Any other firmware loaded into this module is out of the scope of this validation and requires a separate FIPS 140-2 validation.

The FIPS 140-2 security levels for the *Module* are as follows:

Security Requirement	Security Level
Cryptographic Module Specification	2
Cryptographic Module Ports and Interfaces	2
Roles, Services, and Authentication	3
Finite State Model	2
Physical Security	3
Operational Environment	N/A
Cryptographic Key Management	2
EMI/EMC	3
Self-Tests	2
Design Assurance	3
Mitigation of Other Attacks	2

Table 3 – Security Level of Security Requirements

The Module implementation is compliant with:

- [ISO 7816] Parts 1-4
- [JavaCard]
- [GlobalPlatform]

2. Cryptographic Module Ports and Interfaces

2.1 Hardware and Physical Cryptographic Boundary

The *Module* is designed to be embedded into a plastic card body, passport, USB key, secure element etc., with a contact plate connection and/or RF antenna. The physical form of the *Module* is depicted in Figure 1 (to scale). The cryptographic boundary is defined as the surfaces and edges of the packages as shown in Table 4 and figure 1. The *Module* relies on [ISO 7816] and/or [ISO 14443] card readers as input/output devices.

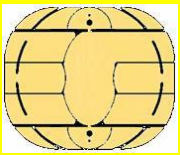
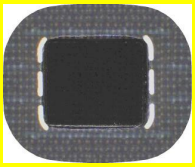
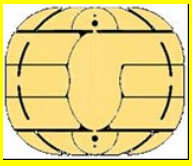
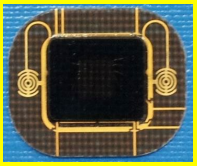
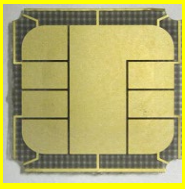
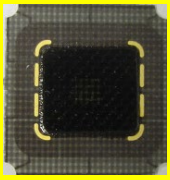
WORLD RLT Module (A1977038)	
 Oblong punching **Top View – Contact Plate**	 **Bottom View – Black Epoxy with RLT Technology**
WORLD Combi RLT Module (A1714221)	
 Oblong punching **Top View – Combi Plate**	 **Bottom View – Black Epoxy with RLT Technology**
G8 G286 Module (A2410334)	
 **Top View – Contact Plate**	 **Bottom View – Black Epoxy with RLT Technology**

Figure 1 – Physical form and Cryptographic Boundary

2.2 PIN assignments - Contact & Combi modules:

Contact No.	Description	Logical interface type
VCC	Supply voltage	Power
RST	Reset signal	Control in
CLK	Clock signal	Control in
GND	Ground	Power
I/O	Input/output	Data in, data out, control in, status out
LA	Antenna coil connection (combi only)	Power, Data in, Data out, Control in, Status out
LB	Antenna coil connection (combi only)	Power, Data in, Data out, Control in, Status out

Table 4 – Module Physical Ports and Corresponding Logical Interfaces

For contact interface operation, the *Module* conforms to [ISO 7816] part 1 and part 2. The electrical signals and transmission protocols follow the [ISO 7816] part 3. The conditions of use are the following:

Conditions	Range
Voltage	1.8V, 3 V and 5.5 V
Frequency	1MHz to 10MHz

Table 5 – Voltage and Frequency Ranges

For contactless interface operation, the *Module* conforms to [ISO 14443] part 1 for physical connections, and to [ISO 14443] parts 2, 3 and 4 for radio frequencies and transmission protocols.

The conditions of use are the following:

Conditions	Range
Supported bit rate	106 Kbits/s, 212 Kbits/s, 424 Kbits/s, 848 Kbits/s
Operating field	Between 1.5 A/m and 7.5 A/m rms
Frequency	13.56 MHz +- 7kHz

Table 6 – Contactless Voltage and Frequency Ranges

3. Cryptographic Module Specification

3.1 Firmware and Logical Cryptographic Boundary

Figure 2 depicts the Module operational environment and applets.

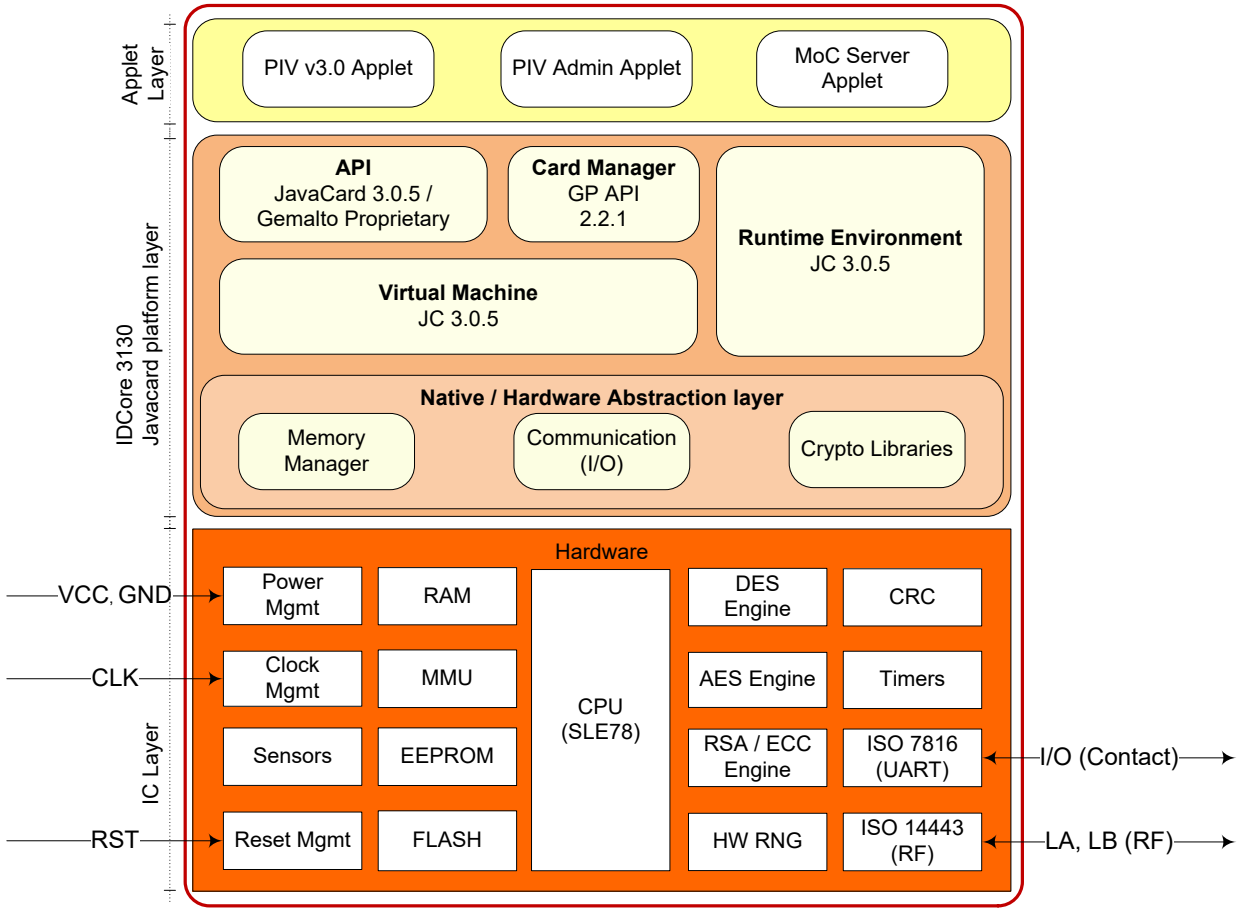


Figure 2 – Module Block Diagram

The *Module* supports [ISO7816] T=0, T=1 and T=CL communication protocols.

The *Module* provides an execution sandbox for Applets, performing the requested services as described in this security policy. Applets access module functionality via internal API entry points that are not exposed to external entities. External devices have access to *Module* services by sending APDU commands.

The *Module* inhibits all data output via the data output interface while the *Module* is in error state and during self-tests.

The *JavaCard API (JCAPI)* is an internal interface, available to applets. Only applet services are available at the card edge (the interfaces that cross the cryptographic boundary).

The *Javacard Runtime Environment (JCRE)* implements the dispatcher, registry, loader, and logical channel functionalities.

The *Virtual Machine (VM)* implements the byte code interpreter, firewall, exception management and byte code optimizer functionalities.

The *Card Manager* is the card administration entity, allowing authorized users to manage the card content, keys, and life cycle states. The Card Manager behaves similarly to an applet but is properly represented as a constituent of the platform. In case of delegated management (DM), the Supplementary Security Domain (SSD) behaves similarly to the Card Manager in term of card content, keys and life cycle states.

The *Memory Manager* implements functions such as memory access, allocation, deletion and garbage collection.

The *Communication* handler implements the ISO 7816 and ISO 14443 communications protocols in contactless mode and dual mode.

The *Cryptography Libraries* implement the algorithms listed in Section 3.3.

Applets, such as PIVv3.0, PIV Admin and MoC Server, access module functionalities via internal API entry points that are not exposed to external entities. External devices have access to *Module* services by sending APDU commands.

Section 5 describes applet functionality in greater detail.

3.2 Versions and Mode of Operation

Hardware:

Infineon SLE78CLFX400VPH with packaging A1714221
Infineon SLE78CFX400VPH with packaging options A1977038 or A2410334

Firmware:

IDCore 3130 (Build09C) with Applets [PIV v3.0 (Build08), PIV Admin v3.0 (Build 08), MoC Server (version 1.1)]

This Module is available in one of the three possible packaging options:

HW Versions	Packaging Options
SLE78CLFX400VPH	World Combi RLT; P/N: A1714221 (Combi)
SLE78CFX400VPH	World RLT P/N: A1977038 (Contact only) G8 G286 P/N: A2410334 (Contact only)

Table 7 – Hardware Versions with Packaging Options

3.3 The Module supports a FIPS Approved mode of operation and a non-FIPS Approved mode of operation. Only the approved and allowed cryptographic functions listed in Table 8 and Table 9 are to be used, along with the guidance detailed in Section 13 of this Security Policy. Any use of Table 10 non-approved cryptographic functions transitions the Module to the non-Approved mode of operation.

Cryptographic Functionality

The *Module* implements the *FIPS Approved* cryptographic functions listed in the table below:

Algorithm	Description	Cert #
AES	[FIPS 197] Advanced Encryption Standard algorithm. The Module supports 128-, 192- and 256-bit key lengths with ECB and CBC encrypt/ decrypt modes.	5243
AES CMAC	[SP 800-38B] The Module supports 128-, 192- and 256-bit key lengths.	5243
CKG	[SP 800-133] Section 6.1, Section 7.1: The Module generates symmetric keys and seeds to be used in asymmetric key generation directly from unmodified DRBG output.	Vendor Affirmed
CVL (RSADP)	[SP 800-56B] RSA key decryption primitive using 2048-bit keys (same RSA implementation validated below).	1715 1716
CVL (RSASP1)	[FIPS 186-4] [PKCS#1 v2.1] RSA signature generation primitive using 2048-bit keys (same RSA implementation validated below).	1714 1717
DRBG	[SP 800-90A] Deterministic Random Bits Generator (256-bit security strength CTR-DRBG based on AES).	2005
ECDSA	[FIPS 186-4] Elliptic Curve Digital Signature Algorithm using the NIST defined curves. – Key pair generation: P-256 and P-384 curves. – Signature generation: P-224, P-256 and P-384 curves with SHA-2. – Signature verification: P-224, P-256 and P-384 curves (approved SHA sizes of the *Module*). *Note: ECDSA P-192 and P-521 were tested but are not utilized. ECDSA P-224 key pair generation was tested but is not utilized.	1365
KBKDF	[SP 800-108] The Module supports AES CMAC 128-, 192- and 256-bit key lengths.	177
KTS	[SP 800-38F] Use of approved AES encryption method with the combination of approved Authentication method AES CMAC, in accordance with SP 800-38F. The Module supports 128-, 192- and 256-bit key lengths.	5243
KTS	[SP 800-56B] The Module supports Key Transport Method using RSA-OAEP 2048-bit keys. Key establishment methodology provides 112 bits of encryption strength.	Vendor Affirmed
RSA	[FIPS 186-4] [PKCS#1 v1.5 and PSS] RSA algorithms. – Key pair generation using 2048-bit keys. – Signature generation using 2048-bit keys with SHA-2. – Signature verification using 2048-bit keys (approved SHA sizes of the *Module*). *Note: RSA 1024-bit signature verification was tested but is not utilized	2802
RSA CRT	[FIPS 186-4] [PKCS#1 v1.5 and PSS] RSA CRT algorithm. – Key pair generation using 2048--bit keys; – Signature generation using 2048-bit keys with SHA-2; – Signature verification using 2048-bit keys (approved SHA sizes of the CM). *Note: RSA CRT 1024-bit signature verification was tested but is not utilized	2803
SHA-1 SHA-2	[FIPS 180-4] Secure Hash Standard compliant one-way (hash) algorithms. The Module supports the SHA-1 (160 bits), SHA-2 (224- bit, 256-bit, 384-bit, 512-bit) variants.	4221
Triple-DES	[SP 800-67 Rev 2] Triple Data Encryption Algorithm. The Module supports the 3-Key options; CBC and ECB encrypt/ decrypt modes. The module enforces a limit of 2^{16} encryptions with the same Triple-DES key by maintaining a counter. *Note: The Triple-DES 2-key decryption option was tested but is not utilized.	2651

Table 8 – FIPS Approved Cryptographic Functions

The *Module* also implements the *FIPS Non-Approved but Allowed* cryptographic functions listed in the table below:

Algorithm	Description
NDRNG	True Random Number Generator

Table 9 – FIPS Non-Approved but Allowed Cryptographic Functions

Due to Algorithm Transitions, the *Module* implements the *FIPS Non-Approved* cryptographic functions listed in the table below:

Algorithm	Description
CVL (ECC CDH SP 800-56A Rev. 3 non-compliant)	ECC CDH Primitive using the NIST defined curves: P-224, P-256, P-384 and P-521. (Cert, #1713)
KAS (Diffie-Hellman SP 800-56A non-compliant)	OnePassDH P-256 with SHA-256 for OPACITY secure Messaging (CS2).
KAS (EC Diffie-Hellman SP 800-56A Rev. 3 non-compliant)	OnePassDH P-384 with SHA-384 for OPACITY secure Messaging (CS7).

Table 10 – FIPS Non-Approved Cryptographic Functions

4. Module Critical Security Parameters

All CSPs used by the Module are described in this section. All usage of these CSPs by the Module are described in the services detailed in Section 5.

CSPs defined in an Approved mode of operation are not to be accessed or shared while in a non-Approved mode of operation. CSPs shall not be generated while in a non-Approved mode.

4.1 Platform Critical Security Parameters

CSP	Description / Usage
OS-DRBG-EI	272-bit random drawn by the NDRNG HW chip during startup and used as entropy input for the [SP800-90A] DRBG implementation. Provides at least 256 bits of entropy.
OS-DRBG-STATE	16-byte AES state V and 32-byte AES key used in the [SP800-90A] CTR DRBG implementation.
OS-GLOBALPIN	4 to 16-byte Global PIN value managed by the ISD. Character space is not restricted by the module.
OS-MKDK	AES-128 (SCP03) key used to encrypt OS-GLOBALPIN value.
SD-KENC	AES-128/192/256 (SCP03) encryption master key used to derive SD-SENC.
SD-KMAC	AES-128/192/256 (SCP03) Security Domain MAC master key, used by the CO to derive SD-SMAC.

SD-KDEK	AES-128/192/256 (SCP03) Sensitive data decryption key used by the User role to decrypt CSPs.
SD-SENC	AES-128/192/256 (SCP03) Session encryption key used by the Module role to encrypt / decrypt secure channel data.
SD-SMAC	AES-128/192/256 (SCP03) Security Domain Session MAC key, used to verify secure channel message integrity.
DAP-SYM	AES-128 (DAP) key optionally loaded in the field and used to verify the MAC signature of packages loaded into the Module.
DM-TOKEN-SYM	AES-128 Delegate Management Token Symmetric key.
DM-RECEIPT-SYM	AES-128 Delegate Management Receipt Symmetric key.

Table 11 – Platform Critical Security Parameters

4.2 PIV Applet Critical Security Parameters

All CSPs used by the PIV applet are described in this section. All usage of these CSPs by the *Module* are described in the services detailed in Section 5. In the table below, the PIV prefix denotes PIV applet. All keys listed below correspond to those specified in NIST SP 800-73-4.

CSP	Description / Usage
PIV-AUTH-TDES	PIV Card Application Administration Key (9B): Symmetric 3-Key TDES encryption / decryption key used by the PIV Applet. External authenticate using this key grants CAA rights. (application security status indicator)
PIV-AUTH-AES	PIV Card Application Administration Key (9B): Symmetric AES-128/192/256 encryption / decryption key used by the PIV Applet. External authenticate using this key grants CAA rights. (application security status indicator)
PIV-AUTH_CH-TDES	PIV Card Authentication Key (9E): Symmetric 3-Key TDES encryption / decryption key used by the PIV Applet. Internal authenticate using to authenticate the card holder (physical access rights)
PIV-AUTH_CH-AES	PIV Card Authentication Key (9E): Symmetric AES-128/192/256 encryption / decryption key used by the PIV Applet. Internal authenticate using to authenticate the card holder (physical access rights)
PIV-AUTH-RSA	PIV authentication Key (9A): 2048-bit private part of the RSA key pair used for Authentication.
PIV-AUTH-ECC	PIV authentication Key (9A): P-256 or P-384 Private part of ECC key pair used for Authentication.
PIV-AS-RSA	PIV Digital Signature Key (9C): 2048-bit private part of the RSA key pair used for Asymmetric signature (Asymmetric key protected by PIN Always used for signature).
PIV-AS-ECC	PIV Digital Signature Key (9C): P-256 or P-384 Private part of ECC key pair used for Asymmetric signature (Asymmetric key protected by PIN Always used for signature).
PIV-AKM-RSA	PIV Key Management Key (9D): 2048-bit private part of the RSA key pair used for Key Management.
PIV-AKM-ECC	PIV Key Management Key (9D): P-256 or P-384 Private part of ECC key pair used for Key Management.
PIV-AUTH_CH-RSA	PIV Card Authentication Key (9E):

	2048-bit private part of the RSA key pair used for Internal authenticate using to authenticate the card holder (physical access rights).
PIV-AUTH_CH-ECC	PIV Card Authentication Key (9E): P-256 or P-384 Private part of ECC key pair used for Internal authenticate using to authenticate the card holder (physical access rights).
PIV-KS-RSA	Retired Key Management (82 up to 95): 2048-bit private part of the RSA key pair used for Key Storage, managed by PIV Card application Crypto Officer to store keys history.
PIV-KS-ECC	Retired Key Management (82 up to 95): P-256 or P-384 Private part of ECC key pair used for Key Storage, managed by PIV Card application Crypto Officer to store keys history.
PIV-Local PIN	PIV Card Application PIN (Local PIN 80): Between 6 and 8 byte-long, in numerical format. (application security status indicator)
PIV-Global PIN	PIV Card Holder Global PIN (00): Between 6 and 8 byte-long, in numerical format. (global security status indicator)
PIV-PUK	PIV card PUK (81): 8 byte-long, in hexadecimal format (all characters allowed) (application security status indicator)
PIV-PC	PIV card Pairing Code: 8 byte-long, used for Virtual Contact Interface (VCI), in numerical format. (application security status indicator)

Table 12 – PIV Applet Critical Security Parameters

4.3 Platform Public Keys

Key	Description / Usage
DAP-ASYM	2048-bit RSA Data Authentication Pattern Asymmetric key, used to verify package loading process.
DM-TOKEN-ASYM	2048-bit RSA Delegate Management Token Asymmetric key.

Table 13 – Platform Public Keys

4.4 PIV Applet Public Keys

Key	Description / Usage
PIV-AUTH-RSA-PUB	PIV authentication Key (9A): 2048-bit public part of the RSA key pair used for Authentication.

PIV-AUTH-ECC-PUB	PIV authentication Key (9A): P-256 or P-384 public part of ECC key pair used for Authentication.
PIV-AS-RSA-PUB	PIV Digital Signature Key (9C): 2048-bit public part of the RSA key pair used for Asymmetric signature (Asymmetric key protected by PIN Always used for signature).
PIV-AS-ECC-PUB	PIV Digital Signature Key (9C): P-256 or P-384 public part of ECC key pair used for Asymmetric signature (Asymmetric key protected by PIN Always used for signature).
PIV-AKM-RSA-PUB	PIV Key Management Key (9D): 2048-bit public part of the RSA key pair used for Key Management.
PIV-AKM-ECC-PUB	PIV Key Management Key (9D): P-256 or P-384 public part of ECC key pair used for Key Management.
PIV-AUTH_CH-RSA-PUB	PIV Card Authentication Key (9E): 2048-bit public part of the RSA key pair used for Internal authenticate using to authenticate the card holder (physical access rights).
PIV-AUTH_CH-ECC-PUB	PIV Card Authentication Key (9E): P-256 or P-384 public part of ECC key pair used for Internal authenticate using to authenticate the card holder (physical access rights).
PIV-KS-RSA-PUB	Retired Key Management (82 up to 95): 2048-bit public part of the RSA key pair used for Key Storage, managed by PIV Card application Crypto Officer to store keys history.
PIV-KS-ECC-PUB	Retired Key Management (82 up to 95): P-256 or P-384 public part of ECC key pair used for Key Storage, managed by PIV Card application Crypto Officer to store keys history.

Table 14 – PIV Applet Public Keys

5. Roles, Authentication and Services

The *Module*:

- Does not support a maintenance role.
- Clears previous authentications on power cycle.
- Supports Global Platform SCP logical channels, allowing concurrent operators in a limited fashion.

Authentication of each operator and their access to roles and services is as described below, independent of logical channel usage. Only one operator at a time is permitted on a channel.

Applet deselection (including Card Manager), card reset, or power down terminates the current authentication; re-authentication is required after any of these events for access to authenticated services.

Authentication data is encrypted during entry (by SD-KDEK), is stored in plaintext and is only accessible by authenticated services.

Table 15 lists all operator roles supported by the Module.

Role ID	Role Type	Role Description
CO	Crypto-Officer	Cryptographic Officer - Role that manages Module content and configuration, including issuance and management of Module data via the ISD or SSD authenticated as described in *Secure Channel Protocol Authentication* below.
CAA	Other	The PIV Card Application Administrator (CAA) role represents an external application requesting the services offered by the PIV Applet. An applet authenticates the Application Operator role by verifying possession of the Application External Authenticate TRIPLE-DES or AES key
CH	User	The PIV Card Holder (CH) role is responsible for ensuring the ownership of his *Module*, and for not communicating his PIN to other parties. The PIV Applet authenticates the Card Holder by verifying the PIN value.
CHII	User	The PIV Card Holder II (CHII) role is responsible for unblocking and/or changing the Card Holder PIN. The PIV authenticates the Card Holder II by verifying the PUK value.
CHPC	User	The PIV Card Holder Pairing Code (CHPC) role is responsible for ensuring the ownership of his *Module*, and for not communicating his Pairing Code to other parties. The PIV Applet authenticates the Card Holder by verifying the Pairing Code value.
CHOCC	Other	The Card Holder On Card Comparison role is responsible for ensuring the ownership of his *Module*. The PIV Applet authenticates the CHOCC role by verifying the biometric fingerprint through the MoC Server Applet. Treated as an unauthenticated role.
UA	Other	Unauthenticated role

Table 15 – Roles Supported by the Module

5.1 Secure Channel Protocol Authentication Method (CO)

The Secure Channel Protocol authentication method is provided by the *Secure Channel* service. The SD-KENC and SD-KMAC keys are used to derive the SD-SENC and SD-SMAC keys, respectively. The SD-SENC key is used to create a cryptogram; the external entity participating in the mutual authentication also creates this cryptogram. Each participant compares the received cryptogram to the calculated cryptogram and if this succeeds, the two participants are mutually authenticated (the external entity is authenticated to the *Module* in the CO role).

The probability that a random attempt will succeed using this authentication method is:

- 1/2^128 = 2.9E-39 (for any of AES-128/192/256 SD-KENC/SD-SENC, assuming a 128-bit block)

The Module enforces a maximum of 255 failed SCP authentication attempts. The probability that a random attempt will succeed over a one-minute interval is:

- 255/2^128 = 7.5E-37 (for any of AES-128/192/256 SD-KENC/SD-SENC, assuming a 128-bit block)

5.2 PIV Application Administrator Authentication (CAA)

a) **The 3-Key Triple-DES** authentication provides 112 bits of security strength. The *Module* uses the PIV-AUTH-TDES to authenticate the CAA role.

- The probability that a random attempt at authentication will succeed is 1/2^64, assuming a 64-bit block length
- The Module enforces a maximum of 10 failed CAA authentication attempts. Based on the maximum count value of the failed authentication blocking mechanism (ratification counter), the probability that a random attempt will succeed over a one-minute period is 10/2^64

b) **The AES** authentication provides 128/192/256 bits of security strength. The *Module* uses the PIV-AUTH-AES to authenticate the CAA role.

- The probability that a random attempt at authentication will succeed is 1/2^128 (for 128-bit length)
- The *Module* enforces a maximum of 10 failed CAA authentication attempts. Based on the maximum count value of the failed authentication blocking mechanism (ratification counter), the probability that a random attempt will succeed over a one-minute period is 10/2^128

5.3 PIV Card Holders (CH, CHII, CHPC)

a) **PIN Verification (CH):** this authentication method compares a PIN value sent to the *Module* to the stored PIN (or Global PIN) values. If the two values are equal, the Card Holder is authenticated. This method is used in the PIV Applet services to authenticate the CH role.

The *Module* enforces string length of 6 bytes minimum (8 bytes maximum). The format supported is numerical (i.e., 0-9) for the 1st six bytes and for the last 2 characters “FF” is also possible. So that the strength of this authentication method is as follows:

- The probability that a random attempt at authentication will succeed is 1/(10^6*11^2)
- Based on a maximum count of 15 for consecutive failed service authentication attempts, the probability that a random attempt will succeed over a one minute period is lower than 15/(10^6*11^2)

b) **PUK Verification (CHII)**: this authentication method compares a PUK value sent to the *Module* to the stored PUK value if the two values are equal, the Card Holder II is authenticated. This method is used in the PIV Applet services to authenticate the CHII role and allows CHII to unblock and/or change the Card Holder PIN.

   The *Module* enforces string length of 8 bytes. The format supported is hexadecimal, meaning that all byte value from 00h to FFh are supported. Then the strength of this authentication method is as follows:

   - The probability that a random attempt at authentication will succeed is lower than1/256^8
   - Based on a maximum count of 15 for consecutive failed service authentication attempts, the probability that a random attempt will succeed over a one-minute period is lower than 15/256^8

c) **Pairing Code Verification (CHPC):** this authentication method compares a Pairing Code value sent to the *Module* to the stored Pairing Code value. If the two values are equal, the Card Holder is authenticated. This method is used in the PIV Applet services to authenticate the CHPC role.

   It is procedurally enforced that the string length is 8 bytes. The format supported is numerical (i.e., 0-9).

   In case of a bad verification of the Pairing code, a slowdown mechanism is implemented to prevent brute force attack, so that no more than 97 attempts are possible in a one-minute period.

   The strength of this authentication method is as follows:

   - The probability that a random attempt at authentication will succeed is 1/10^8
   - The probability that a random attempt will succeed over a one-minute period is 97/10^8

5.4 Card Holder On-Card Comparison (CHOCC)

Biometric Verification (CHOCC): this authentication method runs a biometric person authentication aka On-Card-Comparison (OCC) of a candidate fingerprint template as defined by [FIPS 201-2].

The **CHOCC** role is used to access the Printed information and Pairing Code reference Data container. It allows to access to general Authenticate operations with PIV authentication Key (9A), PIV Digital Signature Key (9C) and PIV Key Management Key.

As defined in [SP800-76-2], the threshold of the Biometric algorithm is set to ensure the FNMR (False Non-Match Rate) to be less than or equal to 0.02 when the FMR (False Match Rate) is at or below 0.0001.

As a consequence, the On-Card Comparison (OCC) is not considered as a valid authentication method and will be classified as an unauthenticated service.

5.5 Platform Services

All services implemented by the Module are listed in the tables below.

Service	Description
Context	Select an applet or manage logical channels.
Module Info (Unauth)	Read unprivileged data objects, e.g., module configuration or status information.
Module Reset	Power cycle or reset the Module. Includes Power-On Self-Test if self-test flag is set.
Run Cryptographic KATs	Resets a flag so that cryptographic KATs may be performed on demand via Module Reset.

Table 16 – Unauthenticated Platform Services

Service	Description	CO
Lifecycle	Modify the card or applet life cycle status.	X
Manage Content	Load and install application packages and associated keys and data.	X
Module Info (Auth)	Read module configuration or status information (privileged data objects).	X
Secure Channel	Establish and use a secure communications channel.	X

Table 17 – Authenticated Platform Services

5.6 PIV Services

All services implemented by the PIV applet are listed in the table below.

Service	Description	CAA	CH	CHII	CHPC	CHOCC	UA
SELECT	Selects a DF or an EF by its file ID, path or name (in the case of DFs).	X	X	X	X	X	X
GENERAL AUTHENTICATE	Performs INTERNAL AUTHENTICATE, EXTERNAL AUTHENTICATE, MUTUAL AUTHENTICATE.	X					
CHANGE REFERENCE DATA	Changes the value of a PIN, Global PIN, PUK or Pairing Code depending on which VERIFY service is called. (Note : User Auth is always done within the command itself by providing previous PIN) Secure Messaging is enforced for this command.		X	X	X		
RESET RETRY COUNTER	Unblocks and changes the value of a PIN or Biometric Template (aka Finger Print). Secure Messaging is enforced for this command.	X		X			

Service	Description	CAA	CH	CHII	CHPC	CHOCC	UA
PUT DATA	Creates, updates or deletes an object value in the data model.	X				X	
GET DATA	Retrieves the data content of the single data object whose tag is given in the data field.	X	X	X	X	X	X
GENERATE ASYMMETRIC KEY PAIR	Generates an RSA or ECDSA Asymmetric Key Pair	X					
VERIFY (PIN)	Authenticates the user (CH) to the card by presenting the User PIN. The User Authenticated status is granted with a successful PIN verification.		X				
VERIFY (BIOMETRY)	Authenticates the user (CHOCC) to the card by presenting the Biometric template (aka Finger Print or Minutiae). The User Authenticated status is granted with a successful On Card Comparison.					X	
VERIFY (PAIRING CODE)	Authenticates the user pairing code (CHPC) to the card by presenting the Pairing code. The User Authenticated status is granted with a successful Pairing Code verification.				X		

Table 18 – PIV Applet Services by Role

The PIV applet enforces the restrictions of algorithms, modes, and key sizes per NIST SP 800-131A Revision 1.

5.7 PIV Admin Services

All services implemented by the PIV Admin applet are listed in the table below.

Service	Description	CO	UA
SELECT	Select an applet.	X	X
GET DATA	Returns the specific info on the following objects: -Data Object Control Parameter (DOCP) of SE, PIN, Key or data object. -Applet personalization data	X	X
CHANGE GLOBAL PIN	Changes the value of the GLOBAL PIN.	X	
DELETE BIOMETRIC TEMPLATE	Zeroize and delete all the biometric templates.	X	

Table 19 – PIV Admin Applet Services by Role

5.8 MoC Services

All services implemented by the MoC Server applet are listed in the table below.

Service	Description	CO	CHOCC	UA
SELECT	Selects a DF or an EF by its file ID, path or name (in the case of DFs).	X	X	X
GET DATA	Returns the cardID, matcherID or BIT stored on card at personalization stage.	X	X	X
GET VERSION (Proprietary)	Returns the application identification data and version.	X	X	X
SET LOCK	Allows temporary unlocking and explicit locking of the access to the administrative interface through the *Shareable Interface* mechanisms.	X		

Table 20 – MoC Server Applet Services by Role

5.9 CSP and Key Access by Service

All services are accessing the CSPs according to the table below:

- G = Generate: The *Module* generates the CSP.
- R = Read: The *Module* reads the CSP (read access to the CSP by an outside entity).
- E = Execute: The *Module* executes using the CSP.
- W = Write: The *Module* writes the CSP. The write access is typically performed after a CSP is imported into the *Module* or when the module overwrites an existing CSP.
- Z = Zeroize: The *Module* zeroizes the CSP. For the Context service, SD session keys are destroyed on applet deselect (channel closure)
- - = Not accessed by the service.

CSPs and Keys														
Service	**OS-DRBG-SEI**	**OS-DRBG-STATE**	**OS-GLOBALPIN**	**OS-MKDK**	**SD-KENC**	**SD-KMAC**	**SD-KDEK**	**SD-SENC**	**SD-SMAC**	**DAP-SYM**	**DAP-ASYM**	**DM-TOKEN-SYM**	**DM-RECEIPT-SYM**	**DM-TOKEN-ASYM**
Context	-	-	-	-	-	-	-	Z	Z	-	-	-	-	-
Module Info (Unauth)	-	-	-	-	-	-	-	E[1]	E[1]	-	-	-	-	-
Module Reset	ZEW	ZEGW	-	-	-	-	-	Z	Z	-	-	-	-	-
Run Cryptographic KATs	E	E	-	-	-	-	-	-	-	-	-	-	-	-
Lifecycle	Z	Z	Z	Z	Z	Z	Z	Z	Z	Z	Z	Z	Z	Z
Manage Content	-	-	W	E	W	WE	WE	E[1]	E[1]	EW	E W	E W	E W	E W
Module Info (Auth)	-	-	-	-	-	-	-	E[1]	E[1]	-	-	-	-	-
Secure Channel	-	EW	-	E	E	E	E	GE[1]	GE[1]	-	-	-	-	-

Table 21 – Platform CSP and Key Access by Service

[1] "E" for Secure Channel keys is included for situations where a Secure Channel has been established and all traffic is received encrypted. The Secure Channel establishment includes authentication to the module.

Service	PIV-Local PIN	PIV-Global PIN	PIV-PUK	PIV-PC	PIV-AUTH-TDES	PIV-AUTH-AES	PIV-AUTH_CH-TDES	PIV-AUTH_CH-AES	PIV-AUTH-RSA	PIV-AUTH-ECC	PIV-AS-RSA	PIV-AS-ECC	PIV-AKM-RSA	PIV-AKM-ECC	PIV-AUTH_CH-RSA	PIV-AUTH_CH-ECC	PIV-KS-RSA	PIV-KS-ECC	PIV-AUTH-RSA-PUB	PIV-AUTH-ECC-PUB	PIV-AS-RSA-PUB	PIV-AS-ECC-PUB	PIV-AKM-RSA-PUB	PIV-AKM-ECC-PUB	PIV-AUTH_CH-RSA-PUB	PIV-AUTH_CH-ECC-PUB	PIV-KS-RSA-PUB	PIV-KS-ECC-PUB
Select	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-
General authenticate	-	-	-	-	E	E	E	E	E	E	E	E	E	E	E	E	E	E	E	E	E	E	E	E	E	E	E	E
Change reference data	E WZ	E WZ	E WZ	E WZ	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-
Reset retry counter	W	W	E	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-
Put data	-	-	-	-	WZ	WZ	WZ	WZ	WZ	WZ	WZ	WZ	WZ	WZ	WZ	WZ	WZ	WZ	WZ	WZ	WZ	WZ	WZ	WZ	WZ	WZ	WZ	WZ
Get data	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-
Generate asym key pair	-	-	-	-	-	-	-	-	G	G	G	G	G	G	G	G	G	G	G	G	G	G	G	G	G	G	G	G
Verify (PIN)	E W	E W	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-
Verify (Biometry Template)	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-
Verify (Pairing Code)	-	-	-	E W	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-

Table 22 – PIV applet CSP and Key Access by Service

Service	PIV-Global PIN
Delete Biometric Template	--
Change global Pin	WZ
Get data	--
Select	--

Table 23 – PIV Admin applet CSP and Key Access by Service

For MoC Server applet, there is no CSP and no Key Access using MoC Server services.

6. Finite State Model

The Module is designed using a finite state machine model that explicitly specifies every operational and error state.

An additional document (Finite State Machine document) identifies and describes all the states of the module including all corresponding state transitions.

7. Physical Security Policy

The *Module* is a single-chip implementation that meets commercial-grade specifications for power, temperature, reliability, and shock/vibrations. The *Module* uses standard passivation techniques. The *Module* has been tested for hardness at nominal (20ºC), high (120ºC) and low (-40ºC) temperatures.

The *Module* is designed to be mounted in a plastic smartcard or similar package; physical inspection of the epoxy side of the Module is not practical after mounting. The *Module* also provides a key to protect the *Module* from tamper during transport and the additional physical protections listed in section 12 Mitigation of Other Attacks Policy below.

8. Operational Environment

The Module is designated as a limited operational environment under the FIPS 140-2 definitions. The Module includes a firmware load service to support necessary updates. New firmware versions within the scope of this validation must be validated through the FIPS 140-2 CMVP. Any other firmware loaded into this module is out of the scope of this validation and require a separate FIPS 140-2 validation.

9. Electromagnetic Interference and Compatibility (EMI/EMC)

The *Module* conforms to the EMI/EMC requirements specified by part 47 Code of Federal Regulations, Part 15, Subpart B, Unintentional Radiators, Digital Devices, Class B.

10. Self-Test

10.1 Power-on Self-Test*

On power-on or reset, the *Module* performs self-tests described in Table 24. All KATs must be completed successfully prior to any other use of cryptography by the *Module*. If one of the KATs fails, the *Module* enters the *Card Is Mute* error state or *Card is Killed* error state, depending on number of failures.

Test Target	Description
Firmware Integrity	16-bit CRC performed over all code located in FLASH and EEPROM memory (for OS, Applets).
AES	Performs decrypt KAT using an AES 128 key in ECB mode. AES encrypt is self-tested as an embedded algorithm of AES-CMAC.
DRBG	Performs DRBG SP 800-90A Section 11.3 instantiate and generate health test KAT with fixed inputs (derivation function and no reseeding supported).
ECDSA	Performs separate ECDSA signature and verification KATs using an ECC P-224 key.
KBKDF AES-CMAC	Performs a KDF AES-CMAC KAT using an AES 128 key and 32-byte derivation data. The KAT computes session keys and verifies the result. Note that KDF KAT is identical to an AES-CMAC KAT; the only difference is the size of input data.
RSA	Performs separate RSA PKCS#1.5 signature and verification KATs using an RSA 2048 bit key, and an RSA PKCS#1.5 signature KAT using the RSA CRT

Test Target	Description
	implementation with a 2048 bit key. RSA CRT signature verification is tested as part of the RSA signature verification KAT as described above.
SHA-1, SHA-2	Performs separate KATs for SHA-1, SHA-256 and SHA-512.
Triple-DES	Performs separate encrypt and decrypt KATs using 3-Key TDEA in ECB mode.

Table 24 – Power-On Self-Test

* Separate SHA-224 and SHA-384 self-tests are not required per IG 9.4 because SHA-256 and SHA-512 are already self-tested. Per IG 9.6, ECC CDH, KBKDF and ECDSA meet KAS self-test requirements.

10.2 Conditional Self-Tests

On every call to the [SP 800-90] DRBG, the *Module* performs the FIPS 140-2 Continuous RNG test (CRNGT) to assure that the output is different than the previous value. Note that the DRBG is seeded only once per power cycle and therefore a CRNGT is not required to be performed on the NDRNG per IG 9.8.

When any asymmetric key pair is generated (for RSA or ECC keys) the *Module* performs a pairwise consistency test.

When new firmware is loaded into the *Module* or into a SSD (having the Delegated Management privilege) using the Manage content service, the *Module* (or the SSD) verifies the integrity and authenticity of the new firmware (applet) using the SD-SMAC key for MAC process.

Optionally, the *Module* (or the SSD) may also verify a MAC or a signature of the new firmware (applet) using the DAP-SYM key or DAP-ASYM key respectively. The signature or MAC block in this scenario is generated by an external entity using the key corresponding to the asymmetric key DAP-ASYM or the secret key DAP-SYM.

10.3 Reducing the number of Known Answer Tests

The *Module* implements latest [IG], reducing the number of Known Answer tests (KAT) described at chapter 9.11.

On the 1st reset of the *Module*, it performs “Firmware Integrity” test and all Cryptographic KATs.

On each next reset of the *Module,* it performs only “Firmware Integrity test” as permitted by [IG] document.

The cryptographic KATs are also available on demand and can be played by any operator with the Run Cryptographic KATs service (see Section 5.5).

11. Design Assurance

The *Module* meets the Level 3 Design Assurance section requirements.

11.1 Configuration Management

An additional document (Configuration Management Plan document) defines the methods, mechanisms and tools that allow to identify and place under control all the data and information concerning the specification, design, implementation, generation, test and validation of the card firmware throughout the development and validation cycle.

11.2 Delivery and Operation

Some additional documents ('Delivery and Operation', 'Reference Manual', 'Card Initialization Specification' documents) define and describe the steps necessary to deliver and operate the *Module* securely.

11.3 Guidance Documents

The Guidance document provided with *Module* is intended to be the 'Reference Manual'. This document includes guidance for secure operation of the *Module* by its users as defined in the Roles, Authentication and Services chapter.

11.4 Language Level

The *Module* operational environment is implemented using a high-level language. A limited number of firmware modules have been written in assembly to optimize speed or size.

The Module's Applets are Java applets designed for the Java Card environment.

12. Mitigation of Other Attacks Policy

The *Module* implements defenses against:

- Fault attacks
- Side channel analysis (Timing Analysis, SPA/DPA, Simple/Differential Electromagnetic Analysis)
- Probing attacks
- Card tearing

13. Security Rules and Guidance

The *Module* implementation also enforces the following security rules:

- No additional interface or service is implemented by the *Module* which would provide access to CSPs.
- Data output is inhibited during key generation, self-tests, zeroization, and error states.
- There are no restrictions on which keys or CSPs are zeroized by the zeroization service.
- The *Module* does not support manual key entry, output plaintext CSPs or output intermediate key values.

- Status information does not contain CSPs or sensitive data that if misused could lead to a compromise of the Mo*d*ule.

At the time the card is issued, **the PIV Applet** shall be personalized with the appropriate data in order to be initialized into the Approved mode. Personalization includes PIV keys and PIN values. Personalization may be performed using a secure channel (ciphered) or in plaintext, as required by the operator.

The following rules must be observed for conformance to SP800-73-4, FIPS 201-2 and FIPS 140-2:

- The Pairing Code shall be 8 bytes composed of numeric characters.
- The Key lengths shall be in the approved table (see Section 3.3 - Table 8 – FIPS Approved Cryptographic Functions).
- The 9B Authentication key ratification counter shall be set in the range of [01 – 10].
- The PIN ratification counter shall be set in the range of [01 – 15].
- The PUK ratification counter shall be set in the range of [01 – 15].

END OF DOCUMENT