

SECORA™ Connect SLS21 D1 Infineon CCC Digital Key Applet V1.0

Security Target

About this document

Scope and purpose

This document contains the Security Target for the evaluation of the **SECORA™ Connect SLS21 D1 Infineon CCC Digital Key Applet V1.0**.

Intended audience

CCC Digital Key Applet evaluators, CCC certification body. Also, technical personnel, including Device OEMs, Vehicle OEMs, and Secure Element integrators, who are responsible for deploying, configuring, and managing the Digital Key applet on a Secure Element.

Table of contents

Table of contents	2
1 Security Target Introduction (ASE_INT)	4
1.1 ST Reference	4
1.2 TOE Reference	4
1.3 TOE Identification	4
1.4 TOE Overview	5
1.4.1 TOE Definition	5
1.4.2 Non-TOE HW/SW/FW Available to the TOE	7
1.4.3 TOE Operational Usage	8
1.4.4 TOE Major Security Features	8
1.5 TOE Description	9
1.5.1 Component Overview	9
1.5.2 Interfaces of the TOE	10
1.5.3 Package Types	10
1.5.4 Lifecycle and Delivery	10
1.5.5 Forms of delivery	12
2 Conformance Claims (ASE_CCL)	13
2.1 CC Conformance Claim	13
2.2 PP Claim	13
2.3 Package Claim	13
2.4 Conformance Rationale	13
2.5 Statement of Compatibility	14
3 Security Problem Definition (ASE_SPD)	15
4 Security Objectives (ASE_OBJ)	16
4.1 Security Objectives defined in the claimed PPs	16
4.2 Security Objectives defined in this ST	16
4.3 Security Objective Rationale	16
5 Security Requirements (ASE_REQ)	17
5.1 Extended Components Definition (ASE_ECD)	17
5.2 TOE Security Functional Requirements	17
5.2.1 Cryptographic Key Management	17
5.2.2 Cryptographic Operation	19
5.2.3 Access Control Policy Security Domain	20
5.2.4 Access Control Functions Security Domain	20
5.2.5 Information Flow Control Functions Secure Channel Protocol	21
5.2.6 Information Flow Control Functions Secure Channel Protocol	21
5.2.7 Residual information protection (FDP_RIP)	22
5.2.8 Stored data integrity (FDP_SDI)	22
5.2.9 Inter-TSF user data integrity transfer protection	23
5.2.10 Identification and Authentication	23
5.2.11 Security Management TSF data	23
5.2.12 Specifications of Management Functions TSF data	24
5.2.13 Unlinkability	24
5.2.14 Protection of the TSF	25
5.2.15 Internal TOE TSF data transfer (FPT_ITT)	25
5.2.16 Replay Detection	26

Security Target

Table of contents

5.2.17	Trusted Recovery	26
5.2.18	TSF Self-Tests	26
5.2.19	Inter-TSF trusted channel	27
5.2.20	Physical Resistance	27
5.3	Security Assurance Requirements	27
5.4	Security Requirements Rationale	28
5.4.1	Security Functional Requirements Rationale	28
5.4.2	Rationale for SFR's Dependencies	29
5.4.3	Rationale for the Exclusion of Dependencies	30
5.4.4	Security Assurance Requirements Rationale	30
6	TOE Summary Specification	31
6.1	SF.AccessControl	31
6.2	SF.CryptoServices	31
6.3	SF.Management	31
6.4	SF.Authentication	32
6.5	SF.SecureMessaging	32
6.6	SF.Integrity	32
6.7	SF.Protection	32
	References	35
	Revision history	37

1 Security Target Introduction (ASE_INT)

1.1 ST Reference

The title of this document is “SECORA™ Connect SLS21 D1 Infineon CCC Digital Key Applet V1.0”.

Version: Rev 1.1

Publication date: 2026-09-09

Sponsor: Infineon Technologies AG, 81726 Munich, Germany

Editor: Infineon Technologies AG, 81726 Munich, Germany

1.2 TOE Reference

The name of the TOE is “SECORA™ Connect SLS21 D1 Infineon CCC Digital Key Applet V1.0” interchangeably called TOE in this ST.

The TOE is a secure chip implementing a Digital Key for Car Connectivity. The TOE is subject to a composite certification based on the Infineon Java Card ‘SECORA™ Connect SLS21 D1’ platform.

EMVCo certificate number of underlying Java Card OS Platform: PCN0223

EMVCo certificate number of underlying HW: ICCN0315

CC certificate number of underlying HW: BSI-DSZ-CC-1206-V5-2025

1.3 TOE Identification

The TOE identification data is as shown in the following table:

Table 1 TOE identification data

Topic	Value	
TOE release date	27-July-2026	
Applet name	"Infineon CCC Digital Key Applet"	
Applet version	1.3.1026	
Applet life cycle state	• '03' - Personalization state • '07' - Operational state	
TOE version number	1.0	
HW identification data	Common Criteria certification identifier (CCI) of underlying HW platform	One of the following: • '00 00 97' (IFX_CCI_000097h) • '00 00 80' (IFX_CCI_000080h)
JC OS Platform related identification data	EMVCo Certification Identifier of underlying hardware platform (ECI)	One of the following: • '00 A0 00 01 00 00' (IFX_ECI_A0h[0x01]) • '00 85 00 02 00 00' (IFX_ECI_85h[0x02])
	Embedded OS version	'01 00 09 00 0E 00 00 00 43'
	CryptoSuite version (Symmetric/Asymmetric)	05.02.003
	Hardware Support Library (HSL) Version	04.05.0040

Security Target

Security Target Introduction (ASE_INT)

Topic	Value	
	Hash Crypto Library (HCL) version	05.02.003
	UMSLC version	02.01.0040

The CCC-DK Applet provides a command ‘GET DATA’ with tags ‘8000’, ‘8100’ and ‘8200’ to retrieve Applet name, Applet version and Applet life cycle state respectively. For more information, refer to Chapter 4.4 in [\[UserGuide\]](#).

The underlying SECORA™ Connect SLS21 D1 platform provides the APDU command “GET TOE Info” which returns the EMVCo Certification Identifier of the platform, the OS version, the specific versions of the cryptographic and hardware support libraries.

1.4 TOE Overview

1.4.1 TOE Definition

This section presents the architecture and common usages of the Target of Evaluation (TOE). The Target of Evaluation (TOE) is the DK Applet embedded in a SE Java Card and GlobalPlatform platform intended to be embedded in a mobile device in order to enable an end user to easily and confidently use their mobile devices as a key to their vehicle granting access to the owner, sharing with a friend, starting the engine, etc.

The TOE comprises:

- the Secure Element – a chip (IC layer)
- the Java Card Platform and GlobalPlatform (OS layer)
- the DK applet (Application layer)

The generic architecture of the TOE is described hereafter (see [Figure 1](#)) and detailed in the following paragraphs.

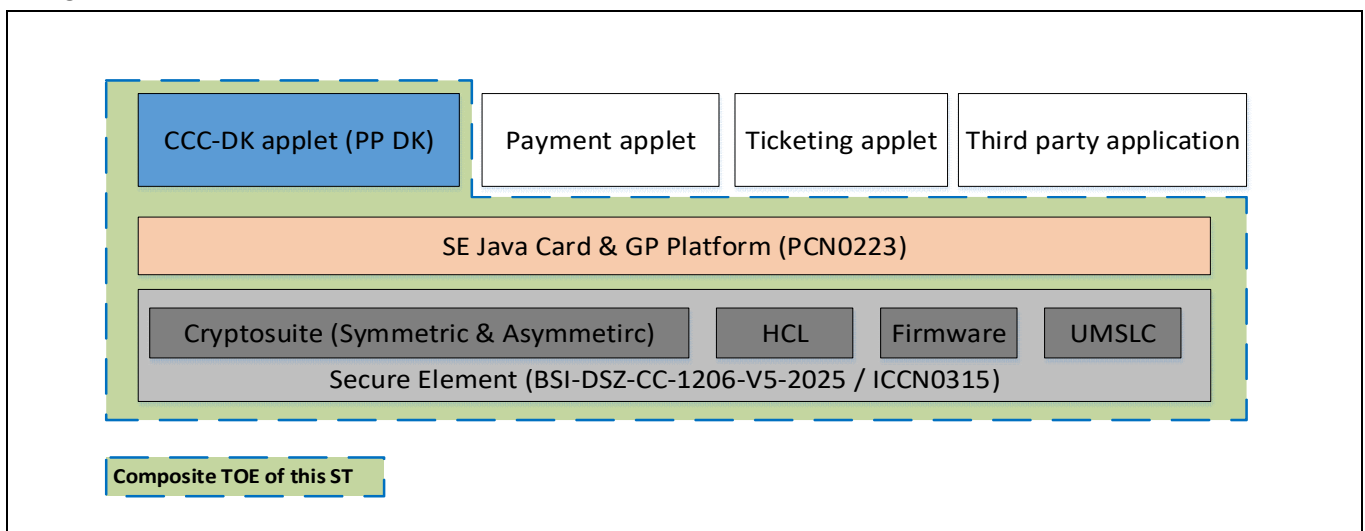


Figure 1 TOE Architecture

The Digital Key architecture uses standards-based public key infrastructure to establish end-to-end trust. Mobile devices create and store Digital Keys in Secure Elements – embedded technology that provides a tamper-resistant secure implementation – to provide the highest-level of protection from the plethora of known hardware- and software-based attacks, including tampering, storage intrusion, cloning, and unauthorized access as well as side channel, fault injection, and many other forms of attack.

Security Target**Security Target Introduction (ASE_INT)**

The Digital Key applet, which resides within the Secure Element, performs all security-critical processing – authentication, encryption protocols, and key generation used for owner pairing, sharing, and vehicle access and engine start transactions – while also providing secure, tamper-proof storage for Digital Keys and their metadata.

The NFC interface is routed directly to the Digital Key applet, providing a communications path that is protected from, and that operates independently of, the rest of the mobile device.

The Digital Key applet provides the following services:

- Hosts Digital Keys (one applet instance hosts Digital Keys of all Vehicle OEMs)
- Implements relevant (fast and standard) transactions
- Implements Instance CA to support offline use cases and privacy protection
- Stores immobilizer tokens when required by the vehicle, offline attestations, access pro-files, and other data associated with a Digital Key
- Verifies authenticity of the vehicle
- Verifies certificate chain of friend public key
- If the Digital Key applet is the SE-centric applet model, the applet also provides the following service:
 - o Verifies the Vehicle Public Key Certificate

The preparation of the TOE and its lifecycle is described more detail in chapter [1.5.4](#).

1.4.2 Non-TOE HW/SW/FW Available to the TOE

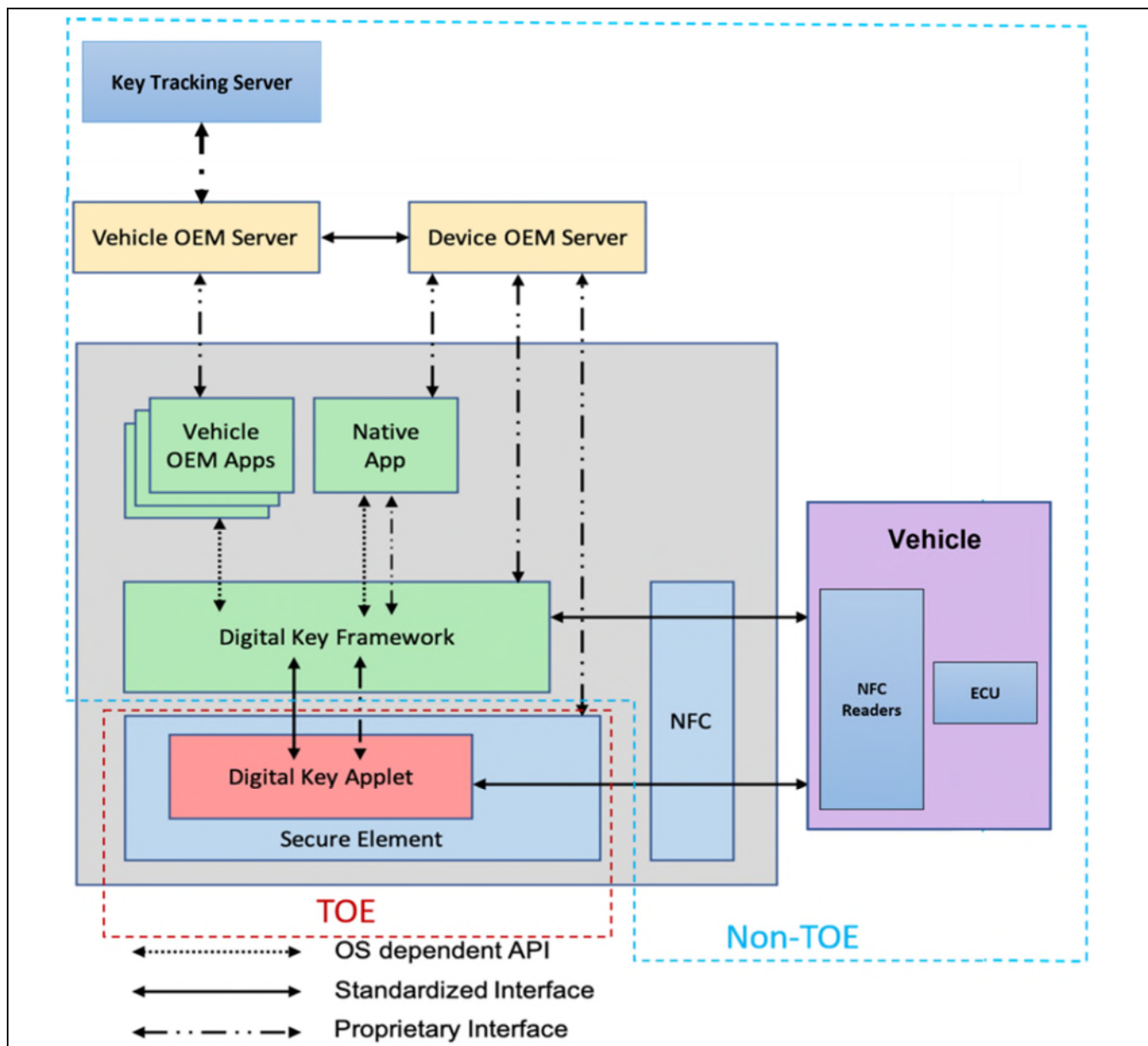


Figure 2 Non-TOE

The Figure 2 depicts the regions including TOE, Non-TOE and the Device region. The region inside red discrete lines (---) shows the TOE region, the one with blue discrete lines (---) shows the Non-TOE region and the region inside ash colored box depicts the Device region.

The TOE relies on each one of the non-TOE components shown in Figure 2 in order to fulfil a functionality.

Note that Vehicle OEMs and Device OEMs provide their own PK infrastructure and the root CA each in their context. The Vehicle OEM signs Device OEM root CA certificate.

Section 2.3.3 of [CCC-CP-023] explains in detail about the Non-TOE region consisting of the Digital Key Framework, Vehicle OEM Apps, Native Apps, Device OS, etc.

The Device OEM also can install and personalize the CCC Digital Key Applet by interacting directly with the SE over the wired or contactless interface. For more details refer to Chapter 2 of [UserGuide].

1.4.3 TOE Operational Usage

Digital Key enables mobile devices to store, authenticate, and share Digital Keys for vehicles in a secure, privacy preserving way that works everywhere, even when the mobile device's battery is low. It is an important addition to the automotive industry, enabling a significantly improved vehicle access experience that builds consumer confidence through its ease of use, convenience, security and privacy protections, and extensive capability. The CCC, representing the majority of the global automotive and mobile device industries, enables the Digital Key's broad cross-industry support and facilitates the coordination of mobile Device OEMs and Vehicle OEMs to provide a consistent user experience by increasing interoperability and reducing market fragmentation.

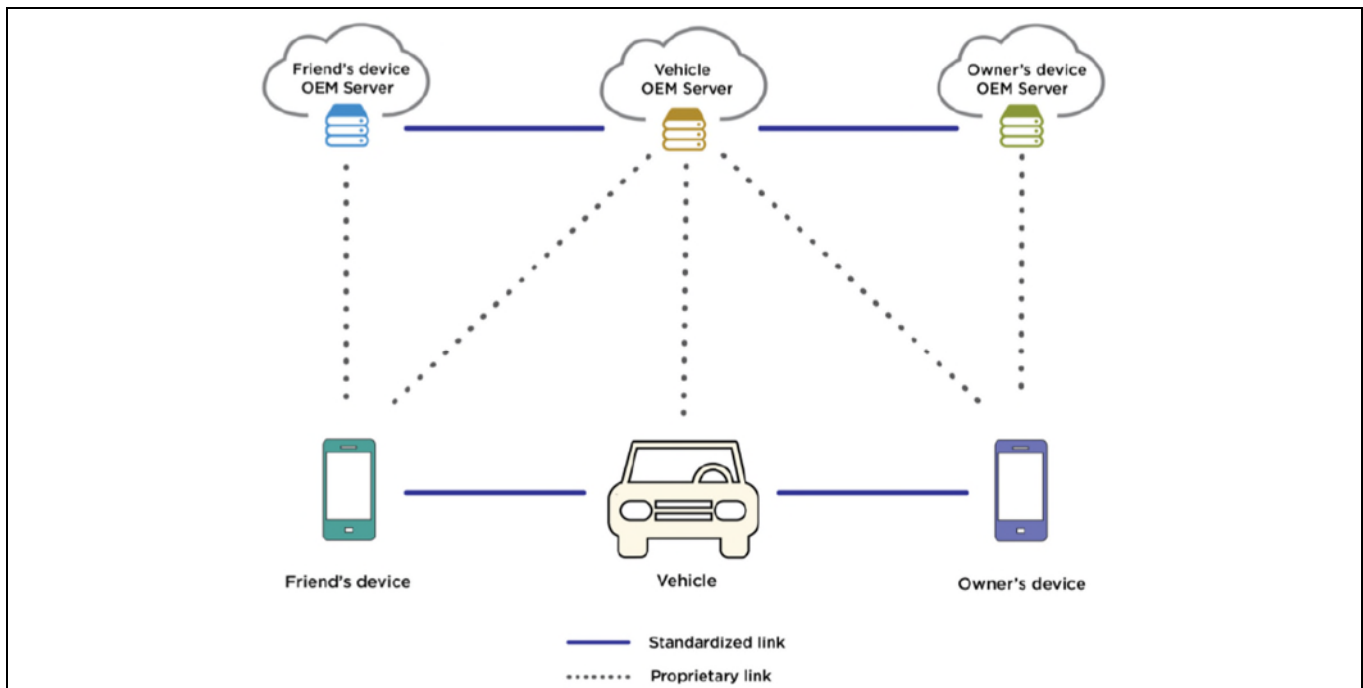


Figure 3 DK System Architecture

The mobile device's native app allows consumers to use and manage Digital Keys without any extra apps, and its Digital Key framework enables developers to build custom apps that provide enhanced services and vehicle-specific features. Mobile devices and vehicles interact with their respective OEM servers to share and manage Digital Keys across mobile devices and vehicle platforms. The system ensures that you're able to access your vehicle even when neither your mobile device nor vehicle has Internet connectivity, while still allowing OEMs to add features that require Internet connectivity for certain operations.

The different use cases of CCC-DK Applet include:

- Owner Pairing
- Vehicle Access/Engine start
- Sharing Digital Keys
- Termination/Suspension of Digital Keys

For more information, please refer to section 1.7 of [\[CCC-CP-023\]](#).

1.4.4 TOE Major Security Features

The following TOE security features are the most significant for its operational use as described in section 1.6 of [\[CCC-CP-023\]](#):

Security Target**Security Target Introduction (ASE_INT)**

- Secure Owner Pairing
- Secure Standard Transaction
- Secure Fast Transaction
- Secure Check Presence Transaction
- Secure DK Sharing
- Key Termination & Suspension
- Secure Applet Management

1.5 TOE Description**1.5.1 Component Overview**

The TOE is a Secure Element chip with the SECORA™ Connect SLS21 D1 Infineon CCC Digital Key Applet V1.0.

[Figure 1](#) shows the TOE in terms of its components. The two lower layers in the picture represent the smart card controller referenced by IFX_ECI_A0h[0x01] together with the Firmware, Cryptosuite (Symmetric & Asymmetric Cryptographic Library). Note that these components are certified by the same EMVCo certificate ICCN0315. The hardware platform provides effective protection mechanisms against fault attacks. The platform contains hardware coprocessors, which support cryptographic standards such as AES, RSA and EC. The hardware coprocessor SCP has integrated measures against successful SCA.

The white color indicates optional components which are not in the scope of the security claims of this ST, in CC terminology these are non interfering with the TSF of the TOE.

The OS platform called “SECORA™ Connect SLS21 D1” is a Java Card OS and offers services for:

- The standard Java Card features like API, the Java Card Runtime Environment and the Java Card Virtual Machine
- GP for content management
- Crypto operations (hash, EC, RSA, TDES and AES)
- Communication via the contactless interface and contact interface.
- It is certified in EMVCo under the Certificate: PCN0223.

The Java Card OS supports the standard open Java Card mode as well as the proprietary static mode (installation of preloaded code is possible). Open and static modes are the two possible modes during personalization of the TOE.

SECORA™ Connect SLS21 D1 Infineon CCC Digital Key Applet V1.0 is a Java Card applet which provides the functions of the CCC Digital Key as per [\[CCC-DK-TS\]](#).

The installation of CCC Digital Key applet is done by the customer. The applet uses the services of the Java Card OS described above. It manages the various stages of the product's lifecycle once the application is onto the hardware up to its end of life. The application also implements the following set of features:

- CCC Digital Key Applet features as specified in CCC Digital Key specification [\[CCC-DK-TS\]](#)
- Personalization via GlobalPlatform STORE DATA
- OPTION A: secure channel protocol 03 (SCP03) secure channel
- OPTION B: 4 (0-3) logical channels on both wired and contactless interface
- OPTION C: Notifications for application protocol data unit (APDU) commands over the contactless interface via host control interface (HCI) events
- OPTION D: Notifications for APDU commands over the wired interface via GET NOTIFICATION command
- Implementation model: SE-Centric

Security Target

Security Target Introduction (ASE_INT)

- Certificate chain model: Variant 2
- User authentication via MANAGE UA
- APDU format 2 for READ BUFFER, GET PRIVATE DATA, and TERMINATE ENDPOINT commands
- Support for 5 authorized public keys

It does not implement any cryptographic primitives, as these are provided by the underlying Java Card OS. Further it manages role-based access control to distinguish between an admin and a normal user based on KVN used to establish the secure channel. Also, the application controls the secure messaging including error handling using the Java Card OS Crypto services, which subsequently relies on the features of the underlying hardware providing high integrity and side channel protection. The claims in terms of SFRs in this Security Target of SECORA™ Connect SLS21 D1 Infineon CCC Digital Key Applet V1.0.

1.5.2 Interfaces of the TOE

The physical interface of the TOE to the external environment is the entire surface of the IC.

The product supports contact-based communication compliant with NCI or GlobalPlatform T=1' over I2C according to [\[ISO-7816-3\]](#) and [\[ISO-7816-4\]](#). It also supports T=CL contactless communication Type A according to [\[ISO14443-3\]](#) and [\[ISO14443-4\]](#). Contactless communication is accessible to a terminal via a booster chip. The booster chip communicates with the secure element via a package internal SWP interface.

The command interface to the TOE is provided by the CCC Digital Key Application.

1.5.3 Package Types

The TOE package type is a hardware multi-chip package (LGA25) and includes:

- SLC21 secure element
- SLS10WNO002 NFC frontend

1.5.4 Lifecycle and Delivery

As per PP [\[CCC-CP-023\]](#) the CCC-DK applet life cycle is composed of four stages as shown in [Figure 4](#):

Security Target

Security Target Introduction (ASE_INT)

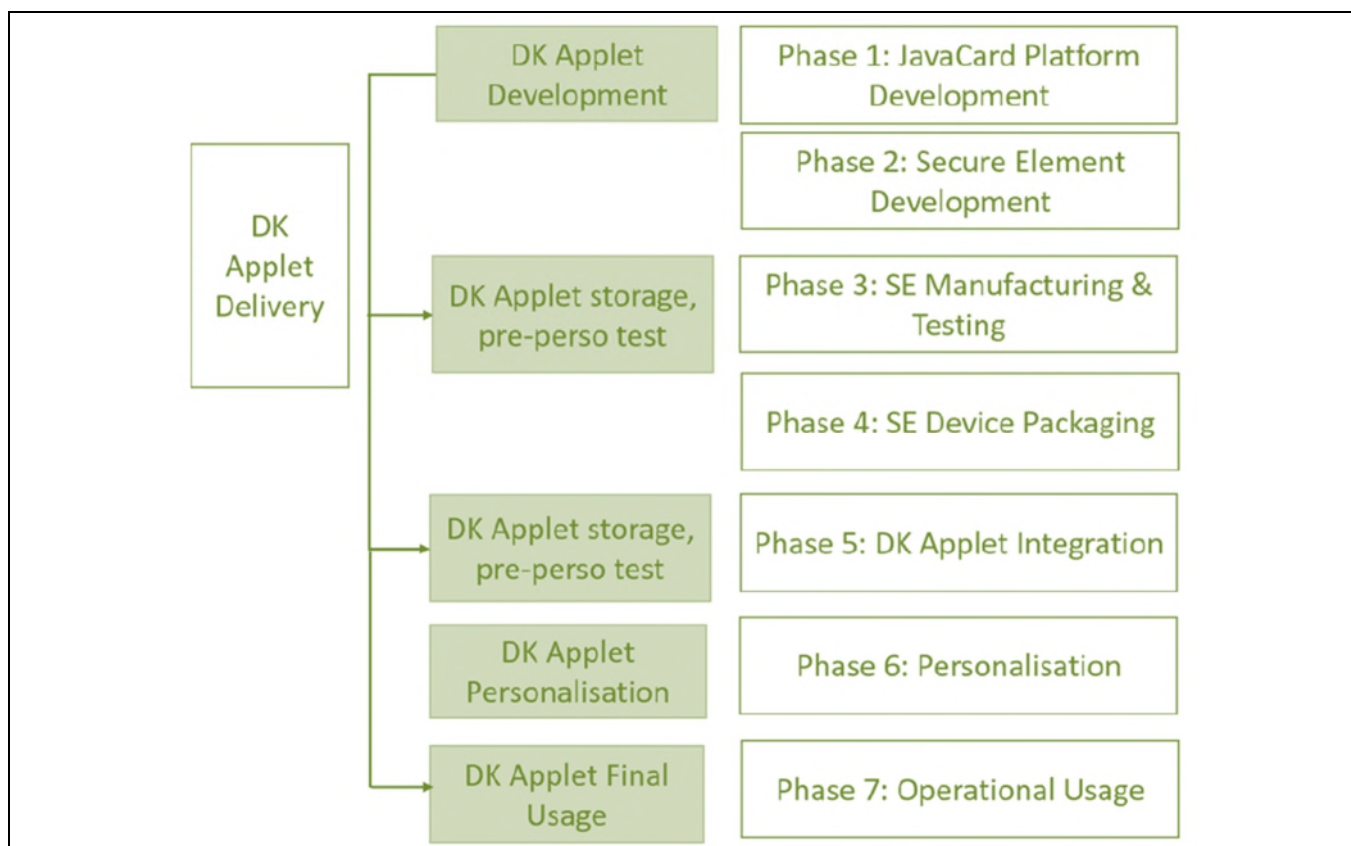


Figure 4 TOE Lifecycle

1. Development:

- Phase 1: Development of Secure Element and its dedicated software (firmware)
- Phase 2: Development of Java Card Platform and CCC-DK applet development

2. Storage, pre-personalisation, and test:

- Phase 3: manufacturing Secure Element and its dedicated software. As the TOE does not provide any user ROM, manufacturing of secure element embedded software parts in ROM are not relevant here.
- Phase 4: Combination of Secure Element with contactless booster interface for NFC
- Phase 5/Option-1 (Prepersonalization): loading on the device of the executable Java Card OS image. Loading of the application JC package containing the TOE code. The TOE is delivered to the customer (Step 6) for further personalization of the CCC Digital Key.
- Phase 5/Option-2 (Prepersonalization): loading on the device of the executable Java Card OS image. Loading of the application JC package containing the TOE code is done in phase 6. The base TOE is delivered to customer along with artefacts mentioned in [Table 2](#).

3. Personalization and test:

- Phase 6/Option-1: this step is performed by the customer. The customer receives from Infineon the TOE composed of the following components:
 - The underlying hardware
 - The underlying Java Card OS can be in two possible modes: either in the standard Java Card open mode (loading and installation of applets are possible) or in the proprietary Java Card static mode (preloaded by Infineon packages can be installed, applet loading is not possible).

Security Target

Security Target Introduction (ASE_INT)

- The cap file of SECORA™ Connect SLS21 Infineon CCC Digital Key Applet V1.0 is preloaded by Infineon.
- Phase 6/Option-2: this step is performed by the customer. The customer receives from Infineon the TOE composed of the following components:
 - The underlying hardware
 - The underlying Java Card OS is in open mode (loading and installation of applets are possible)
 - The cap file of SECORA™ Connect SLS21 Infineon CCC Digital Key Applet V1.0 for post loading in the form of encrypted scripts

The customer then proceeds to load the SECORA™ Connect SLS21 Infineon CCC Digital Key Applet V1.0 (*if not done through Phase 6/Option-1*) and installation. In case the Java Card OS is in open mode, the customer can load and install 3rd party applets. During this step the customer also performs the personalisation and configuration of the TSF, if necessary. Personalization is done using a secure channel offered by the GlobalPlatform framework which ensures the confidentiality and integrity of the data being personalized.

The TOE will be set to operational use in Phase 7.

4. Final Usage:

- Phase 7: The CCC-DK applet and the product provide the full set of security functionalities.

1.5.5 Forms of delivery

The composite TOE is delivered to customers with the Infineon Java Card 'SECORA™ Connect SLS21 D1' platform via Postal transfer in cages. All materials are delivered to distribution centers in cages, locked.

For the post loading option, the encrypted cap file is shared with additional pgp encryption via webservice portal IDC.

The guidance documentations are delivered to the customer together with the TOE as a personalized PDF via webservice portal MyICP.

Table 2 Delivery artefacts

Delivery item	Name	Version	Date
CCC-DK applet software	Encrypted cap file of SECORA™ Connect SLS21 D1 Infineon CCC Digital Key Applet V1.0	v1.3.1026	2026-07-27
Guidance documents	SLS21 Infineon CCC Digital Key Applet User Guide	Rev. 1.3	2026-07-24
	SLS21 Infineon CCC Digital Key Applet Release notes	Rev 1.3	2026-07-24
Platform Guidance documents	SLS21 SECORA™ Connect X and E Administration guide	Rev. 1.3	2025-12-05
	SLS21 SECORA™ Connect X and E Extended datasheet	Rev. 1.3	2025-12-05
	SLS21 SECORA™ Connect X and E Security guide	Rev. 1.2	2025-12-05
	SLS21 SECORA™ Connect X and E Security Guide - Addendum (for Mastercard application)	Rev. 1.0	2025-09-09
	SLS21 SECORA™ Connect X and E Sandbox Application Programmer's Reference Manual	Rev. 1.2	2025-12-05

2 Conformance Claims (ASE_CCL)

2.1 CC Conformance Claim

This Security Target and the TOE claim conformance to CC:2022. This ST claims conformance to Common Criteria version CC:2022 revision 1 part 2 [CCPart2] and Common Criteria version CC:2022 revision 1 part 3 [CCPart3] conformant. Also conformant to Common Criteria evaluation methods and activities [CEM2022]. [CCErrata] and [CCTrans] are taken into consideration.

2.2 PP Claim

The TOE is strictly conformant to [CCC-CP-023] Car Connectivity Consortium Digital Key, Protection Profile of the Digital Key Applet.

2.3 Package Claim

The assurance level for the TOE is EAL4 augmented with the components ALC_DVS.2 and AVA_VAN.5.

2.4 Conformance Rationale

With CC:2022 several SFR changes are introduced. Due to this ST claiming conformance to CC:2022 and [CCC-CP-023], rationales are provided that these changes do not affect the conformance claim to [CCC-CP-023]:

- FCS_COP.1: for this SFR dependencies are changed in CC:2022. FCS_CKM.4 is removed and instead FCS_CKM.6 is added. Further FCS_CKM.5 is added for key derivation as an alternative.
- FCS_CKM.1: for this SFR dependencies are changed in CC:2022. Additionally, to FCS_CKM.2 and FCS_COP.1, one further SFR is introduced as alternative: FCS_CKM.5. This SFR targets key derivation, subsequent to FCS_CKM.1. FCS_CKM.4 is removed and instead FCS_CKM.6 is added. All other dependencies (i.e. FCS_RNG.1 or FCS_RBG.1) are in addition to the already existing ones, i.e. add stricter requirements.
- FCS_CKM.6 replaces FCS_CKM.4 and adds further requirements on the timing of key destruction. As an alternative dependency to FCS_CKM.1, FCS_CKM.5 (key derivation) can be used. As FCS_CKM.5 is neither used within [CCC-CP-023] nor within this ST, it has no relevance in this context.
- FCS_RNG.1: this SFR is taken from [CCPart2] rather than [CCC-CP-023]. The SFR is refined in [CCPart2].
- FMT_LIM.1 and FMT_LIM.2 in CC:2022 are slightly rephrased (i.e. removing redundancy from FMT_LIM.1) and availability and capability policy mentioned in both SFR's. The meaning though is the same as in [CCC-CP-023] and therefore conformance can still be claimed.

Further with CC:2022 some SAR changes were introduced. Rationales are provided that these changes do not affect the conformance claim to [CCC-CP-023]:

- ASE_CCL.1: for CC:2022 several extensions were introduced (e.g. exact conformance to PP), which add to the already existing assurance requirements. No relaxation was introduced.
- ASE_INT.1: introduction of multi-assurance in combination with PP-configuration: not relevant for [CCC-CP-023].
- ASE_REQ.2: extended for multi assurance: not relevant for [CCC-CP-023].
- AVA_VAN.5: extension about third party components introduced. No relaxation was introduced.
- ALC_TAT.1: extension with guidance on the minimum content for an implementation standards description and rules with ADV_COMP.1. No relaxation was introduced.

2.5 Statement of Compatibility

The EMVCo PCN covers the ASE composition activity between the underlying Secure Element and the Java Card and GlobalPlatform platform. The required security requirements for [\[CCC-CP-023\]](#) are fulfilled implicitly with the EMVCo PCN. Refer to section 2.2 of [\[CCC-CP-024\]](#).

This ST does not contradict with the relevant subset security requirements of the underlying EMVCo platform. For detailed Statement of Compatibility, refer to [\[SOC\]](#).

3 Security Problem Definition (ASE_SPD)

All assets, subjects and external entities, threats, organisational security policies and assumptions from [\[CCC-CP-023\]](#) section 3 “Security Problem Definition” are applicable for this TOE.

4 Security Objectives (ASE_OBJ)

Here follows a concise description of the security objectives applying to this ST followed by the security objective rationale.

4.1 Security Objectives defined in the claimed PPs

All Security Objectives provided by the TOE or by the operational environment as well as the security objectives rationale from the claimed PP [\[CCC-CP-023\]](#) section 4 “Security Objectives” are applicable for this TOE.

4.2 Security Objectives defined in this ST

None.

4.3 Security Objective Rationale

The Security Objective Rationale from the claimed [\[CCC-CP-023\]](#) stays the same here.

5 Security Requirements (ASE_REQ)

5.1 Extended Components Definition (ASE_ECD)

[CCC-CP-023] section 5.1 “Extended Components Definition” is applicable for this TOE. However, the SFRs are replaced with SFRs from CC:2022. The mappings and its correspondence are shown in Table 3.

Table 3 Extended SFRs or SFRs from [CCC-CP-023] mapped to SFRs in CC:2022

SFRs from [CCC-CP-023]	Mapping to SFRs in CC:2022	Correspondence
FCS_RNG.1	FCS_RNG.1	Replaced and refined with SFR from CC:2022. The SFR from CC:2022 specifies more details and still fulfils required quality metric details for [CCC-CP-023].
SFRs from CC:2022		
n.a	FCS_CKM.6	Introduced in this ST from CC:2022 to support FCS_COP.1
n.a	FPT_TST.1	Introduced in this ST from CC:2022.

5.2 TOE Security Functional Requirements

The security functional requirements (SFR) for this TOE are defined in this chapter. This ST covers the SFRs from [CCC-CP-023].

Operations already performed in the underlying PP [CCC-CP-023] are marked by underlined font style. Please refer to [CCC-CP-023] for further information on details of the operation. Operations performed within this Security Target are marked by *italic underlined* font style.

Note that if an SFR has application notes as per the PP [CCC-CP-023] then these application notes apply and can be found in the PP. Some SFRs contain additional application notes to ease the understanding of the specificities of this TOE. These application notes do not come from the PP and are prefixed with [IFX specific].

5.2.1 Cryptographic Key Management

Cryptographic keys SHALL be managed throughout their life cycle. The following SFRs are intended to support that lifecycle and consequently defines requirements for the following activities:

- cryptographic key generation,
- cryptographic key distribution and
- cryptographic key destruction.

Table 4 FCS_CKM.1 Cryptographic key generation | EC Point Generation

FCS_CKM.1	Cryptographic key generation EC Point Generation
Hierarchical to:	No other components.
Dependencies:	[FCS_CKM.2 Cryptographic key distribution or FCS_CKM.5 Cryptographic key derivation or FCS_COP.1 Cryptographic operation] [FCS_RBG.1 Random bit generation or

FCS_CKM.1	Cryptographic key generation EC Point Generation
	FCS_RNG.1 Generation of random numbers] FCS_CKM.6 Timing and event of cryptographic key destruction
FCS_CKM.1.1/ECC	The TSF SHALL generate cryptographic keys in accordance with a specified cryptographic key generation algorithm <u>ECC with P-256 (SECP256r1)</u> and specified cryptographic key sizes <u>256-bit</u> that meet the following standards: <u>FIPS PUB 186-4</u> .

Table 5 FCS_CKM.1 Cryptographic key generation | Secure Channel

FCS_CKM.1	Cryptographic key generation Secure Channel
Hierarchical to:	No other components.
Dependencies:	[FCS_CKM.2 Cryptographic key distribution or FCS_CKM.5 Cryptographic key derivation or FCS_COP.1 Cryptographic operation] [FCS_RBG.1 Random bit generation or FCS_RNG.1 Generation of random numbers] FCS_CKM.6 Timing and event of cryptographic key destruction
FCS_CKM.1.1/ Session_keys	The TSF SHALL generate cryptographic keys in accordance with a specified cryptographic key generation algorithm <u>HKDF-SHA-256</u> and specified cryptographic key sizes <u>256-bit</u> that meet the following standards: <u>IETF [RFC 5869]</u> .
FCS_CKM.1.1/Long_Term_key	The TSF SHALL generate cryptographic keys in accordance with a specified cryptographic key generation algorithm <u>HKDF-SHA-256</u> and specified cryptographic key sizes <u>256-bit</u> that meet the following standards: <u>IETF [RFC 5869]</u> .
FCS_CKM.1.1/ Secret_Shared_key	The TSF SHALL generate cryptographic keys in accordance with a specified cryptographic key generation algorithm <u>HKDF-SHA-256</u> and specified cryptographic key sizes <u>256-bit</u> that meet the following standards: <u>IETF [RFC 5869]</u> .

Table 6 FCS_RNG.1 Random number generation

FCS_RNG.1	Quality metric for random numbers
Hierarchical to:	No other components.
Dependencies:	No dependencies.
FCS_RNG.1.1	The TSF shall provide a <u>hybrid physical</u> random number generator that implements: <u>Random numbers generation Class PTG.3 according to [AIS31]</u> .
FCS_RNG.1.2	The TSF shall provide <u>octets of bits</u> that meet: (1) (PTG.3.7) Statistical test suites cannot practically distinguish the internal random numbers from output sequences of an ideal RNG. The internal random numbers must pass test procedure A. (2) (PTG.3.8) The internal random numbers shall <u>use PTRNG of class PTG.2 as random source for the post-processing</u> .

Table 7 FCS_CKM.2 Cryptographic key distribution | Key Establishment

FCS_CKM.2	Cryptographic key distribution Key Establishment
Hierarchical to:	No other components.
Dependencies:	[FDP_ITC.1 Import of user data without security attributes, or FDP_ITC.2 Import of user data with security attributes, or FCS_CKM.1 Cryptographic key generation or FCS_CKM.5 Cryptographic key derivation]
FCS_CKM.2.1/ECDHE	The TSF SHALL distribute cryptographic keys in accordance with a specified cryptographic key distribution method <u>Elliptic curve-based Diffie-Hellman Ephemeral key agreement and cryptographic key sizes 256-bit</u> that meets the following: <u>NIST Special Publication 800-56A Revision 3 with approved groups from Appendix D.</u>
[IFX specific] Application Note:	The TOE implements ECDHE functionality according to BSI TR-03111 as specified in the the CCC Technical Specification.

Table 8 FCS_CKM.6 Timing and event of cryptographic key destruction

FCS_CKM.6	Timing and event of cryptographic key destruction
Hierarchical to:	No other components.
Dependencies:	[FDP_ITC.1 Import of user data without security attributes, or FDP_ITC.2 Import of user data with security attributes, or FCS_CKM.1 Cryptographic key generation]
FCS_CKM.6.1	The TSF shall destroy <u>cryptographic keys</u> when <u>no longer needed</u> .
FCS_CKM.6.2	The TSF shall destroy cryptographic keys and keying material specified by FCS_CKM.6.1 in accordance with a specified cryptographic key destruction method <u>overwriting the key values with random values</u> that meets the following: <u>none</u> .

5.2.2 Cryptographic Operation

In order for a cryptographic operation to function correctly, the operation SHALL be performed in accordance with a specified algorithm and with a cryptographic key of a specified size. The following SFRs specify all this latter information to be enforced by the TSF.

It covers the following:

- data encryption and/or decryption,
- digital signature generation and/or verification,
- cryptographic checksum generation for integrity and/or verification of checksum,
- secure hash (message digest),
- cryptographic key encryption and/or decryption,
- and cryptographic key agreement.

Table 9 FCS_COP.1 Cryptographic Operation

FCS_COP.1	Cryptographic key access
Hierarchical to:	No other components.
Dependencies:	[FDP_ITC.1 Import of user data without security attributes, or FDP_ITC.2 Import of user data with security attributes, or FCS_CKM.1 Cryptographic key generation, or FCS_CKM.5 Cryptographic key derivation] FCS_CKM.6 Timing and event of cryptographic key destruction
FCS_COP.1.1 / Hash	The TSF SHALL perform <u>Cryptographic Hashing</u> in accordance with a specified cryptographic algorithm <u>SHA-256</u> and cryptographic key sizes <u>None</u> that meet the following: <u>FIPS 180-4</u> .
FCS_COP.1.1 / HMAC	The TSF SHALL perform <u>Keyed Hash Message Authentication</u> in accordance with a specified cryptographic algorithm <u>HMAC-SHA-256</u> , and cryptographic key sizes <u>256-bit</u> that meet the following: <u>ISO/IEC 9797-2:2011</u> .
FCS_COP.1.1 / Encryption/decryption	The TSF SHALL perform <u>data encryption or decryption</u> in accordance with a specified cryptographic algorithm <u>AES with CBC mode of operation</u> and cryptographic key sizes <u>128-bit, 192-bit and 256-bit</u> that meet the following: <u>FIPS PUB 197, NIST SP 800-38A</u> .
FCS_COP.1.1 / CMAC	The TSF SHALL perform <u>Message Authentication Code</u> in accordance with a specified cryptographic algorithm <u>AES CMAC</u> and cryptographic key sizes <u>128-bit</u> that meet the following: <u>NIST SP 800-38B</u> .
FCS_COP.1.1 / ECDSA	The TSF SHALL perform <u>digital signing</u> accordance with a specified cryptographic algorithm <u>ECDSA with NIST P-256 curve</u> and cryptographic key sizes <u>256-bit</u> that meet the following: <u>ANSI X9.62</u> .

5.2.3 Access Control Policy | Security Domain

The following SFR defines the Security Functional Policy for access control to the TOE, which will be called SD_SFP. The SD_FSP is defined in the Table 16 of [CCC-CP-023] and the SFRs will refer to it.

Table 10 FDP_ACC.2 Complete access control

FDP_ACC.2	Complete access control
Hierarchical to:	FDP_ACC.1 Subset access control
Dependencies:	FDP_ACF.1 Security attribute based access control
FDP_ACC.2.1	The TSF SHALL enforce the <u>SD_SFP</u> on <u>all subjects, objects defined by the SD_FSP</u> and all operations among subjects and objects covered by the SFP.
FDP_ACC.2.2	The TSF SHALL ensure that all operations between any subject controlled by the TSF and any object controlled by the TSF are covered by an access control SFP

5.2.4 Access Control Functions | Security Domain

Table 11 FDP_ACF.1 Security attribute base access control

Security Target

Security Requirements (ASE_REQ)

FDP_ACF.1	Security attribute base access control
Hierarchical to:	No other components.
Dependencies:	FDP_ACC.1 Subset access control FMT_MSA.3 Static attribute initialisation
FDP_ACF.1.1	The TSF SHALL enforce the <u>SFP_AC</u> to objects based on the following: <u>All subjects and objects together with their respective security attributes as defined in SD_SFP.</u>
FDP_ACF.1.2	The TSF SHALL enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: <u>Rules for all access methods and access rules defined in SD_SFP.</u>
FDP_ACF.1.3	The TSF SHALL explicitly authorise access of subjects to objects based on the following additional rules: <u>none.</u>
FDP_ACF.1.4	The TSF SHALL explicitly deny access of subjects to objects based on the following additional rules: <u>when at least one of the rules R_GPF defined in the SD_SFP does not hold.</u>
Application Note:	As mentioned in Application Note 10 of [CCC-CP-023], the dependency FMT_MSA.3 will not be fulfilled here, since there is no initialisation of attributes necessary.

5.2.5 Information Flow Control Functions | Secure Channel Protocol

The Information Flow Control SFP (SC_SFP) is defined in the Table 17 of [CCC-CP-023] and the SFRs will refer to it.

Table 12 FDP_IFC.2 Complete Information Flow Control

FDP_IFC.2/SCP	Complete Information Flow Control
Hierarchical to:	FDP_IFC.1 Subset information flow control
Dependencies:	FDP_IFF.1 Simple security attributes
FDP_IFC.2.1/SCP	The TSF SHALL enforce the <u>SCP_SFP</u> on <u>subjects, information and operations</u> and all operations that cause that information to flow to and from subjects covered by the SCP_SFP.
FDP_IFC.2.2/SCP	The TSF SHALL ensure that all operations that cause any information in the TOE to flow to and from any subject in the TOE are covered by an information flow control SFP.

5.2.6 Information Flow Control Functions | Secure Channel Protocol

Table 13 FDP_IFF.1 Simple security attributes

FDP_IFF.1/SCP	Simple security attributes
Hierarchical to:	No other components.
Dependencies:	FDP_IFC.1 Subset information flow control FMT_MSA.3 Static attribute initialisation

Security Target

Security Requirements (ASE_REQ)

FDP_IFF.1/SCP	Simple security attributes
FDP_IFF.1.1/SCP	The TSF SHALL enforce the <u>SCP_SFP</u> based on the following types of subject and information security attributes: <u>Subjects and information as defined by the SCP_SFP, and for each, the security attributes as defined in [GP] and no additional security attributes.</u>
FDP_IFF.1.2/SCP	The TSF SHALL permit an information flow between a controlled subject and controlled information via a controlled operation if the following rules hold: <u>Rules R_GPF as defined by the SCP_SFP.</u>
FDP_IFF.1.3/SCP	The TSF SHALL enforce the <u>no additional information flow control SFP rules.</u>
FDP_IFF.1.4/SCP	The TSF SHALL explicitly authorise an information flow based on the following rules: <u>no additional rules.</u>
FDP_IFF.1.5/SCP	The TSF SHALL explicitly deny an information flow based on the following rules: <u>When none of the conditions listed in the element FDP_IFF.1.4 of this component hold and at least one of those listed in the element FDP_IFF.1.2 does not hold.</u>
Application Note:	Application Note 12: The on-card and the off-card subjects have security attributes such as MAC, Cryptogram, Challenge, Key Set, Static Keys, etc. Application Note 13: An SFR FMT_MSA.3 is not used here, since the security attributes used in the SCP_SFP are already contained in the ICCM when entering the TOE, therefore rules for creation of information and default values of security attributes are not applicable

5.2.7 Residual information protection (FDP_RIP)

Table 14 FDP_RIP.1 Subset residual information protection

FDP_RIP.1	Subset residual information protection
Hierarchical to:	No other components.
Dependencies:	No dependencies.
FDP_RIP.1.1	The TSF SHALL ensure that any previous information content of a resource is made unavailable upon the <u>deallocation of the resource from the following objects: Cryptographic buffers.</u>
Application Note:	Application Note 14: Cryptographic Buffers can be Cryptographic data used in runtime cryptographic computations, like a seed used to generate a key.

5.2.8 Stored data integrity (FDP_SDI)

Table 15 FDP_SDI.2 Stored data integrity monitoring and action

FDP_SDI.2	Stored data integrity monitoring and action
Hierarchical to:	FDP_SDI.1 Stored data integrity monitoring
Dependencies:	No dependencies.
FDP_SDI.2.1	The TSF SHALL monitor user data stored in containers controlled by the TSF for <u>integrity errors</u> on all objects, based on the following attributes: <u>cryptographic keys and user data.</u>

Security Target

Security Requirements (ASE_REQ)

FDP_SDI.2	Stored data integrity monitoring and action
FDP_SDI.2.2	Upon detection of a data integrity error, the TSF SHALL <u>prohibit the use of the altered data, send notification of the error where applicable.</u>

5.2.9 Inter-TSF user data integrity transfer protection

Table 16 FDP_UIT.1 Data exchange Integrity | Card Content Management

FDP_UIT.1	Data exchange Integrity Card Content Management
Hierarchical to:	No other components
Dependencies:	[FDP_ACC.1 Subset access control, or FDP_IFC.1 Subset information flow control] [FTP_ITC.1 Inter-TSF trusted channel, or FTP_TRP.1 Trusted path]
FDP_UIT.1.1/CCM	The TSF SHALL enforce the <u>Secure channel protocol Information flow control policy to <i>transmit, receive</i> user data in a manner protected from <i>modification, deletion, insertion, replay</i> errors.</u>
FDP_UIT.1.2/CCM	The TSF SHALL be able to determine on receipt of user data, whether <u><i>modification, deletion, insertion, replay</i></u> has occurred.

5.2.10 Identification and Authentication

Table 17 FIA_UAU.3 Unforgeable authentication

FIA_UAU.3	Unforgeable authentication
Hierarchical to:	No other components
Dependencies:	No dependencies.
FIA_UAU.3.1	The TSF SHALL <u><i>detect and prevent</i></u> use of authentication data that has been forged by any user of the TSF.
FIA_UAU.3.2	The TSF SHALL <u><i>detect and prevent</i></u> use of authentication data that has been copied from any other user of the TSF.

5.2.11 Security Management | TSF data

Table 18 FMT_MTD.1 Management of TSF data

FMT_MTD.1	Management of TSF data
Hierarchical to:	No other components
Dependencies:	FMT_SMR.1 Security roles FMT_SMF.1 Specification of Management Functions
FMT_MTD.1.1/deletion of keys	The TSF SHALL restrict the ability to, <u><i>delete, the keys to Digital Key framework, no other authorised identified roles.</i></u>

Table 19 FMT_MTD.3 Secure TSF data

Security Target

Security Requirements (ASE_REQ)

FMT_MTD.3	Secure TSF data
Hierarchical to:	No other components
Dependencies:	FMT_MTD.1 Management of TSF data
FMT_MTD.3.1	The TSF SHALL ensure that only secure values are accepted for <u>the applet's AID</u> .
Application Note:	Application Note 15: The value of the Applet's AID is defined in [CCC-DK-TS] , Section 15.3.2.1.

5.2.12 Specifications of Management Functions | TSF data

Table 20 FMT_SMF.1 Specification of Management Functions

FMT_SMF.1	Specification of Management Functions
Hierarchical to:	No other components
Dependencies:	No dependencies.
FMT_SMF.1.1	The TSF SHALL be capable of performing the following management functions: <u>creates a deletion attestation for the requested key (for deletion), and that it is securely deleted before the attestation is transferred to the requesting party.</u>

Table 21 FMT_SMR.1 Security Roles

FMT_SMR.1	Security Roles
Hierarchical to:	No other components
Dependencies:	FIA_UID.1 Timing of identification
FMT_SMR.1.1	The TSF SHALL maintain the roles <u>Digital Key framework, Vehicle, no other authorised identified roles.</u>
FMT_SMR.1.2	The TSF SHALL be able to associate users with roles.
Application Note:	Application Note 16: The dependency to FIA_UID.1 is not applicable to this TOE. This ST does not require the identification of the roles to be assigned which is handled by the operational environment.

5.2.13 Unlinkability

Table 22 FPR_UNL.1 Unlinkability

FPR_UNL.1	Unlinkability
Hierarchical to:	No other components
Dependencies:	No dependencies.
FPR_UNL.1.1/NFC	FPR_UNL.1.1 The TSF shall ensure that any entity (other than the TOE, the DK Framework or the Vehicle) is unable to determine whether data and key exchanged over NFC (between the TOE and the Vehicle) were caused by the same user.

5.2.14 Protection of the TSF

Table 23 FPT_ITC.1 Inter-TSF confidentiality during transmission

FPT_ITC.1	Inter-TSF confidentiality during transmission
Hierarchical to:	No other components
Dependencies:	No dependencies.
FPT_ITC.1.1	The TSF SHALL protect all TSF data transmitted from the TSF to another trusted IT product from unauthorised disclosure during transmission.

Table 24 FPT_ITI.1 Inter-TSF detection of modification

FPT_ITI.1	Inter-TSF detection of modification
Hierarchical to:	No other components
Dependencies:	No dependencies.
FPT_ITI.1.1/ Vehicle_Integrity	The TSF SHALL provide the capability to detect modification of all TSF data during transmission between the TSF and another trusted IT product within the following metric: <u>metric as defined in FCS COP.1.1/CMAC</u> .
FPT_ITI.1.2/ Vehicle_Integrity	The TSF SHALL provide the capability to verify the integrity of all TSF data transmitted between the TSF and another trusted IT product and perform <u>terminate the on-going process</u> if modifications are detected.

5.2.15 Internal TOE TSF data transfer (FPT_ITT)

Table 25 FPT_ITT.1 Basic internal TSF data transfer protection

FPT_ITT.1	Basic internal TSF data transfer protection
Hierarchical to:	No other components
Dependencies:	No dependencies.
FPT_ITT.1.1/ IMMO_TOKEN	The TSF SHALL protect TSF data from <u>disclosure</u> when it is transmitted between separate parts of the TOE.
FPT_ITT.1.1/ DIGITAL_KEY	The TSF SHALL protect TSF data from <u>disclosure</u> when it is transmitted between separate parts of the TOE.

Table 26 FPT_ITT.3/DIGITAL_KEY TSF data integrity monitoring

FPT_ITT.3/DIGITAL_KEY	TSF data integrity monitoring
Hierarchical to:	No other components
Dependencies:	FPT_ITT.1 Basic internal TSF data transfer protection
FPT_ITT.3.1/ DIGITAL_KEY	The TSF SHALL be able to detect <u>modification of data, substitution of data, re-ordering of data, deletion of data</u> , for TSF data transmitted between separate parts of the TOE.
FPT_ITT.3.2/DIGITAL KEY	Upon detection of a data integrity error, the TSF SHALL take the following actions: <u>security exception or security reset</u> .

Table 27 FPT_ITT.3/IMMO_TOKEN TSF data integrity monitoring

FPT_ITT.3/IMMO_TOKEN	TSF data integrity monitoring
Hierarchical to:	No other components
Dependencies:	FPT_ITT.1 Basic internal TSF data transfer protection
FPT_ITT.3.1/IMMO_TOKEN	The TSF SHALL be able to detect <u>modification of data</u> , <u>substitution of data</u> , <u>re-ordering of data</u> , <u>deletion of data</u> for TSF data transmitted between separate parts of the TOE.
FPT_ITT.3.2/IMMO_TOKEN	Upon detection of a data integrity error, the TSF SHALL take the following actions: <u>security reset or security exception</u> .

5.2.16 Replay Detection

The following SFR uses the Subject, S.Transaction data: This can be the data/keys being shared between the DK Applet and the vehicle (through NFC) or between the DK Framework and the DK Applet.

Table 28 FPT_RPL.1 Replay detection

FPT_RPL.1	Replay detection
Hierarchical to:	No other components
Dependencies:	No dependencies.
FPT_RPL.1.1	The TSF SHALL detect replay for the following entities: <u>S.Transaction data</u> .
FPT_RPL.1.2	The TSF SHALL perform <u>terminate the transaction</u> when replay is detected.

5.2.17 Trusted Recovery

Table 29 FPT_RCV.2 Automated recovery

FPT_RCV.2	Automated recovery
Hierarchical to:	FPT_RCV.1 Manual recovery
Dependencies:	AGD_OPE.1 Operational user guidance
FPT_RCV.2.1	When automated recovery from <u>power failure</u> is not possible, the TSF shall enter a maintenance mode where the ability to return to a secure state is provided.
FPT_RCV.2.2	For <u>power loss</u> , the TSF SHALL ensure the return of the TOE to a secure state using automated procedures.

5.2.18 TSF Self-Tests

Table 30 FPT_TST.1 TSF Self-Tests

FPT_TST.1	TSF testing
Hierarchical to:	No other components.
Dependencies:	No dependencies.

Security Target

Security Requirements (ASE_REQ)

FPT_TST.1	TSF testing
FPT_TST.1.1	The TSF shall run a suite of following self tests <u>during initial start-up</u> , to demonstrate the correct operation of <u>the TSF: the Java Card OS the UMSLC (User Mode Security Life Control) selftest offered by the hardware platform is performed</u> .
FPT_TST.1.2	The TSF shall provide authorised users with the capability to verify the integrity of the <u>TSF data</u> .
FPT_TST.1.3	The TSF shall provide authorised users with the capability to verify the integrity of <u>stored TSF executable code</u> .

5.2.19 Inter-TSF trusted channel

Table 31 FTP_ITC.1 Inter-TSF trusted channel

FTP_ITC.1	Inter-TSF trusted channel
Hierarchical to:	No other components
Dependencies:	No dependencies.
FTP_ITC.1.1	The TSF SHALL provide a communication channel between itself and another trusted IT product that is logically distinct from other communication channels and provides assured identification of its end points and protection of the channel data from modification or disclosure.
FTP_ITC.1.2	The TSF SHALL permit <u>another trusted IT product</u> to initiate communication via the trusted channel.
FTP_ITC.1.3	The TSF SHALL initiate communication via the trusted channel for <u>sharing of secret keys, user data, immobiliser token</u> .

5.2.20 Physical Resistance

Table 32 FPT_PHP.3 Resistance to physical attack

FPT_PHP.3	Resistance to physical attack
Hierarchical to:	No other components
Dependencies:	No dependencies.
FPT_PHP.3.1	The TSF SHALL resist <u>physical manipulation and physical probing</u> to the <u>TSF</u> by responding automatically such that the SFRs are always enforced.

5.3 Security Assurance Requirements

The security assurance requirement level is EAL4 augmented with AVA_VAN.5 and ALC_DVS.2 covering all the Security Assurance components highlighted in the table below.

Table 33 Security assurance requirements

Assurance class	Assurance components
ADV: Development	ADV_ARC.1 Security architecture description

Security Target

Security Requirements (ASE_REQ)

Assurance class	Assurance components
	ADV_FSP.4 Complete functional specification
	ADV_IMP.1 Implementation representation of the TSF
	ADV_TDS.3 Modular design
	ADV_COMP.1 Design compliance with the base component-related user guidance, ETR for composite evaluation and report of the base component evaluation authority
AGD: Guidance documents	AGD_OPE.1 Operational user guidance
	AGD_PRE.1 Preparative procedures
ALC: Life-cycle support	ALC_CMC.4 Production support, acceptance procedures and automation
	ALC_CMS.4 Problem tracking CM coverage
	ALC_DEL.1 Delivery procedures
	ALC_DVS.2 Sufficiency of security measures
	ALC_LCD.1 Developer defined life-cycle model
	ALC_TAT.1 Well defined developer tools
	ALC_COMP.1 Integration of the dependent component into the related base component and consistency check for delivery and acceptance procedures
ASE: Security Target evaluation	ASE_CCL.1 Conformance claims
	ASE_ECD.1 Extended components definition
	ASE_INT.1 ST introduction
	ASE_OBJ.2 Security objectives
	ASE_REQ.2 Derived security requirements
	ASE_SPD.1 Security problem definition
	ASE_TSS.1 TOE summary specification
	ASE_COMP.1 Consistency of Security Target
ATE: Tests	ATE_COV.2 Analysis of coverage
	ATE_DPT.1 Testing: basic design
	ATE_FUN.1 Functional testing
	ATE_IND.2 Independent testing – sample
	ATE_COMP.1 Composite product functional testing
AVA: Vulnerability assessment	AVA_VAN.5 Advanced methodical vulnerability analysis
	AVA_COMP.1 Composite product vulnerability assessment

5.4 Security Requirements Rationale

5.4.1 Security Functional Requirements Rationale

The Security Functional Requirements Rationale is same as defined in PP [\[CCC-CP-023\]](#) section 5.4.1.

In addition, the following coverage is applicable for this ST.

Security Target

Security Requirements (ASE_REQ)

Table 34 Security Objectives and SFRs - Coverage

Security Objectives	SFR	Rationale
O.IMMO_TOK_CONFID	FPT_TST.1	The Security Objective O.IMMO_TOK_CONFID is met by the additional SFR FPT_TST.1 by enforcing a UMSLC (User Mode Security Life Control) self tests during initial start-up of underlying Java Card OS, offered by the hardware platform.

5.4.2 Rationale for SFR's Dependencies

Table 35 Rationale for SFR's Dependencies

SFR	Dependencies	Support of the Dependencies
FCS_CKM.1/ ECC FCS_CKM.1/ Session_keys	[FCS_CKM.2 or FCS_CKM.5 or FCS_COP.1], [FCS_RBG.1 or FCS_RNG.1] and FCS_CKM.6	FCS_CKM.2 FCS_COP.1 FCS_RNG.1 FCS_CKM.6
FCS_RNG.1	No dependencies.	n.a
FCS_CKM.2	[FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1 or FCS_CKM.5]	FCS_CKM.1
FCS_CKM.6	[FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1]	FCS_CKM.1
FCS_COP.1	[FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1 or FCS_CKM.5] and FCS_CKM.6	FCS_CKM.1 FCS_CKM.6
FDP_ACC.2	FDP_ACF.1	FDP_ACF.1
FDP_ACF.1	FDP_ACC.1 and FMT_MSA.3	FDP_ACC.2 Note: FMT_MSA.3 is not used
FDP_IFC.2	FDP_IFF.1	FDP_IFF.1
FDP_IFF.1	FDP_IFC.1 and FMT_MSA.3	FDP_IFC.2 Note: FMT_MSA.3 is not used
FDP_RIP.1	No dependencies.	n.a
FDP_SDI.2	No dependencies.	n.a
FDP_UIT.1	[FDP_ACC.1 or FDP_IFC.1] and [FDP_ITC.1 or FDP_TRP.1]	FDP_IFC.2 FDP_ITC.1
FIA_UAU.3	No dependencies.	n.a
FMT_MTD.1	FMT_SMR.1 and FMT_SMF.1	FMT_SMR.1 FMT_SMF.1
FMT_MTD.3	FMT_MTD.1	FMT_MTD.1
FMT_SMF.1	No dependencies.	n.a
FMT_SMR.1	FIA_UID.1	The dependency to FIA_UID.1 is not applicable to this TOE.
FPR_UNL.1	No dependencies.	n.a
FPT_ITC.1	No dependencies.	n.a

Security Target

Security Requirements (ASE_REQ)

SFR	Dependencies	Support of the Dependencies
FPT_ITI.1/ Vehicle_Integrity	No dependencies.	n.a
FPT_ITT.1	No dependencies.	n.a
FPT_ITT.3	FPT_ITT.1	FPT_ITT.1
FPT_RPL.1	No dependencies.	n.a
FPT_RCV.2	AGD_OPE.1	AGD_OPE.1
FPT_TST.1	No dependencies.	n.a
FTP_ITC.1	No dependencies.	n.a
FPT_PHP.3	No dependencies.	n.a

5.4.3 Rationale for the Exclusion of Dependencies

The dependency to FIA_UID.1 is not applicable to this TOE. This [\[CCC-CP-023\]](#) does not require the identification of the roles to be assigned which is handled by the operational environment.

5.4.4 Security Assurance Requirements Rationale

EAL4 augmented with ALC_DVS.2 and AVA_VAN.5 is appropriate for this TOE as required by the PP [\[CCC-CP-023\]](#). The rationale provided in the PP [\[CCC-CP-023\]](#) is applicable to this ST.

6 TOE Summary Specification

This TOE summary specification described in this section relies on the security services provided by the platform product.

The composite TOE provides the security functions as follows:

6.1 SF.AccessControl

The TOE implements this security functionality to manage the access rights to the objects that are maintained in the CCC-DK Applet. This also includes the functions of Security domain and secure channel protocol provided by the underlying OS platform.

This Security Functionality covers following SFRs:

- FDP_ACC.2 Complete access control for the security domain
- FDP_ACF.1 Security attribute base access control for the security domain
- FDP_IFC.2/SCP Complete Information Flow Control for the secure channel
- FDP_IFF.1/SCP Simple security attributes for the secure channel

6.2 SF.CryptoServices

The TOE supports the following cryptographic operations which are based on the security functionalities supported by the underlying OS platform. This security functionality covers the following SFRs:

- FCS_CKM.1/ECC Cryptographic key generation for EC Point Generation
- FCS_CKM.1/Session_keys Cryptographic key generation for Secure Channel
- FCS_RNG. 1 Random number generation that complies to [\[AIS31\]](#)
- FCS_CKM.2/ECDHE Cryptographic key distribution for Key Establishment
- FCS_CKM.6 Timing and event of cryptographic key destruction for Session keys
- FCS_COP.1 Cryptographic operation for Hash, HMAC, Encryption/decryption, AES CMAC and ECDSA signing
- FDP_RIP.1 Subset residual information protection

6.3 SF.Management

The TOE provides security management which includes restriction of key deletion, allowed AID and involved user roles. This comprises the following SFRs:

- FMT_MTD.1 Management of TSF data which defines the management functions to be enforced and defines the concerned roles involved during a deletion operation.
- FMT_MTD.3 Secure TSF data of the security domains
- FMT_SMF.1 Specification of Management Functions which defines the management functions concerning the attestation creation and secure transferring of the same during a deletion operation.
- FMT_SMR.1 Security Roles by enforcing a Security Domain access control policy (rules and restrictions) that ensures a secure card content management.

6.4 SF.Authentication

The TOE supports authentication management and comprises the following SFRs:

- FIA_UAU.3 Unforgeable authentication which prevents and detects forged data which could be used for key exchange operation, guaranteeing the authenticity of the key exchange operation.

6.5 SF.SecureMessaging

The TOE provides secure communication between the TOE and the Vehicle. This comprises the following SFRs:

- FTP_ITC.1 Inter-TSF trusted channel with unauthorised disclosure protection during transmission between itself and another trusted IT product, which will further ensure the confidentiality of the being transmitted such as immobilizer token, etc.
- FDP_UIT.1 Data exchange Integrity through Card Content Management: which enforces the Secure Channel Protocol information flow control policy and the Security Domain access control policy to ensure the integrity of card management operations.
- FPT_ITC.1 Inter-TSF trusted channel provides protection of TSF data from unauthorized disclosure during transmission.

6.6 SF.Integrity

The TOE provides integrity protection to the stored cryptographic keys and the user data using the underlying OS and the HW. This comprises the following SFRs:

- FDP_SDI.2 Stored data integrity monitoring and action ensures that the user data imported and stored into the TOE are monitored for integrity violations.

6.7 SF.Protection

The TOE provides security protection against physical and logical attacks. The underlying OS and HW support to achieve this protection. This comprises the following SFRs:

- FPT_PHP.3 Resistance to physical attack which enforces the appropriate mechanisms to continuously counter physical manipulation and physical probing.
- FPT_TST.1 TSF Self-Tests offered by the HW platform is performed in the underlying OS
- FPR_UNL.1 Unlinkability to ensure that any entity (other than the TOE, the DK Framework or the Vehicle) is unable to determine whether data and key exchanged over NFC (between the TOE and the Vehicle) were caused by the same user.
- FPT_RCV.2 Automated recovery which enforces the return of the TOE to a secure state using automated procedures during certain failures which can occur.
- FPT_ITI.1/Vehicle_Integrity Inter-TSF detection of modifications to TSF data when transmitted between the TOE and vehicle.
- FPT_ITT.1 Basic internal TSF data transfer protection which ensures that the keys are protected when transmitted between separate parts of the TOE against disclosure.
- FPT_ITT.3/DIGITAL_KEY TSF data integrity monitoring which enforces that the assets of the Digital Key transmitted between separate parts of the TOE are monitored for identified integrity errors.
- FPT_RPL.1 Replay detection which protects against replay attacks over transactions.

Table 36 Mapping of SFRs to TOE Summary

SFR	SF.AccessControl	SF.CryptoServices	SF.Management	SF.Authentication	SF.SecureMessaging	SF.Integrity	SF.Protection
FCS_CKM.1/ECC		X					
FCS_CKM.1/Session_keys		X					
FCS_RNG.1		X					
FCS_CKM.2		X					
FCS_CKM.6		X					
FCS_COP.1		X					
FDP_ACC.2	X						
FDP_ACF.1	X						
FDP_IFC.2	X						
FDP_IFF.1	X						
FDP_RIP.1		X					
FDP_SDI.2						X	
FDP_UIT.1					X		
FIA_UAU.3				X			
FMT_MTD.1			X				
FMT_MTD.3			X				
FMT_SMF.1			X				
FMT_SMR.1			X				
FPR_UNL.1							X
FPT_ITC.1					X		
FPT_ITI.1.1/ Vehicle_Integrity							X
FPT_ITT.1							X
FPT_ITT.3							X
FPT_RPL.1							X
FPT_RCV.2							X
FPT_TST.1							X
FTP_ITC.1					X		
FPT_PHP.3							X

References

[AIS31]	Functionality classes and evaluation methodology for physical random number generators. AIS31, Version 2.1, 2011-12-02, Bundesamt für Sicherheit in der Informationstechnik.
[CCPart1]	Common Criteria for Information Technology Security Evaluation, CC:2022, revision 1, November 2022 — Part 1: Introduction and general model
[CCPart2]	Common Criteria for Information Technology Security Evaluation, CC:2022, revision 1, November 2022 — Part 2: Security functional components
[CCPart3]	Common Criteria for Information Technology Security Evaluation, CC:2022, revision 1, November 2022 — Part 3: Security assurance components
[CCPart5]	Common Criteria for Information Technology Security Evaluation, Part 5: Pre-defined packages of security requirements, November 2022, CC:2022, Revision 1
[CCErrata]	Errata and Interpretation for CC:2022 (Release 1) and CEM:2022 (Release 1), V1.2, 2025-10-15
[CCTrans]	CCMC-2023-04-001, Transition Policy to CC:2022 and CEM:2022, 2023-04-20
[CEM2022]	Common Methodology for Information Technology Security Evaluation, Evaluation Methodology, November 2022, CEM:2022, Revision 1
[ISO9797-1]	ISO/IEC International Standard 9797-1:2011-(E), Information technology – Security techniques – Message Authentication Codes (MACs) – Part 1: Mechanisms using a block cipher, Second Edition 2011-03-01
[ISO14443-3]	ISO/IEC International Standard 14443-3 Cards and security devices for personal identification — Contactless proximity objects — Part 3: Initialization and anticollision, Fourth edition 2018-07
[ISO14443-4]	ISO/IEC International Standard 14443-4 Cards and security devices for personal identification Contactless proximity objects, Part 4: Transmission protocol, Fourth edition 2018-07
[UserGuide]	SLS21 Infineon CCC Digital Key Applet User Guide, Revision 1.4, 2026-09-02
[RelNotes]	SLS21 Infineon CCC Digital Key Applet Release Notes, Revision 1.3, 2026-07-24
[JC-PP]	Java Card System – Open Configuration Protection Profile, July 2024, Version 3.2
[CCC-CP-023]	Car Connectivity Consortium Digital Key, Protection Profile of the Digital Key Applet, Version 1.0, CCC-CP-023, 16 th October 2023.
[CCC-DK-TS]	Car Connectivity Consortium Digital Key Release 3 - Technical Specification Version 1.1.3 (CCC-TS-101)
[CCC-CP-024]	Guidance for DK Applet Protection Profile Evaluation, Version 1.0.1
[SOC]	Statement of Compatibility for SECORA™ Connect SLS21 D1 Infineon CCC Digital Key Applet V1.0, Revision 0.1, 2026-01-09
[ISO-7816-3]	ISO/IEC 7816-3:2006: Identification cards - Integrated circuit cards - Part 3: Cards with contacts - Electrical interface and transmission protocols (Third edition); 2006-11
[ISO-7816-4]	ISO/IEC 7816-4:2020: Identification cards - Integrated circuit cards - Part 4: Organization, security and commands for interchange (Fourth edition); 2020-05

Revision history

Reference	Description
Revision 1.1, 2026-09-09	
All	Updated guidance documentation references to the latest User Guide revision and updated FCS_COP.1 cryptographic operation specifications.
Revision 1.0, 2026-08-20	
All	Version for initial certification.

Trademarks

All referenced product or service names and trademarks are the property of their respective owners.

Edition 2026-09-09

Published by

Infineon Technologies AG

81726 Munich, Germany

© 2026 Infineon Technologies AG.

All Rights Reserved.

Do you have a question about this document?

Email:

csscustomerservice@infineon.com

IMPORTANT NOTICE

The information given in this document shall in no event be regarded as a guarantee of conditions or characteristics ("Beschaffenheitsgarantie").

With respect to any examples, hints or any typical values stated herein and/or any information regarding the application of the product, Infineon Technologies hereby disclaims any and all warranties and liabilities of any kind, including without limitation warranties of non-infringement of intellectual property rights of any third party.

In addition, any information given in this document is subject to customer's compliance with its obligations stated in this document and any applicable legal requirements, norms and standards concerning customer's products and any use of the product of Infineon Technologies in customer's applications.

The data contained in this document is exclusively intended for technically trained staff. It is the responsibility of customer's technical departments to evaluate the suitability of the product for the intended application and the completeness of the product information given in this document with respect to such application.

For further information on the product, technology delivery terms and conditions and prices please contact your nearest Infineon Technologies office (www.infineon.com).

WARNINGS

Due to technical requirements products may contain dangerous substances. For information on the types in question please contact your nearest Infineon Technologies office.

Except as otherwise explicitly approved by Infineon Technologies in a written document signed by authorized representatives of Infineon Technologies, Infineon Technologies' products may not be used in any applications where a failure of the product or any consequences of the use thereof can reasonably be expected to result in personal injury.