TRUST AND VERIFY

TrustCB Scheme Procedures for CCC Certification Scheme for SE/Digital Key Applet security evaluation

Version 1.1

TRUST AND VERIFY

Contents

1 CCC DK Scheme

This document is an annex to TrustCB Shared Scheme Procedures (current version) [TrustCB_SP] and should be read in conjunction with the Shared Scheme Procedures. This document provides specific details related to TrustCB operational processes for the CCC Certification Scheme for SE/Digital Key Applet security evaluation (CCC DK).

1.1 Introducing the CCC DK scheme

The CCC-DK certification scheme has been designed as a means by which products implementing the Car Connectivity Consortium Digital Key Technology can demonstrate they are protected against state-of-the-art attacks on Car Connectivity Consortium Digital Key assets, at a high level of assurance.

Developers and sponsors requesting certification for their products must also be members of the Car Connectivity Consortium (CCC).

General information about Car Connectivity Consortium's Digital Key activities can be found at: https://carconnectivity.org/digital-key/The CCC authorised labs for the scheme can be found at: https://carconnectivity.org/digital-key/atl-listings/ (in the status field, look for DK Applet Security)

The scheme document that describes, among other things, the certification requirements for the scheme, is [PMD], the definite source for the scheme. In case of conflict between the [PMD] and this document, the [PMD] takes precedence.

TrustCB has been appointed by the CCC DK scheme owner as Certification Body for the CCC DK certification scheme.

1.2 CCC DK Contact details

Scheme contact address at TrustCB is CCC-DK@trustcb.com.

1.3 CCC DK TOE-type overview

The Target of Evaluation is expected to be a Secure Element/Digital Key Applet compliant with the DK Applet Protection Profile [PP] in composition with (on top of) both of the following [Scheme FW]:

a. an IC conformant with PP0084 [PP0084] certified under the SOGIS MRA, and
b. a Java Card Platform and GlobalPlatform platform certified conformant with at least **one** of the following:
    a. Java Card Protection Profile – PP0099 [PP99] under the SOGIS MRA, or
    b. GlobalPlatform SE Protection Profile [GPPP] under the SOGIS MRA, or
    c. PCN certified by EMVCo (under conditions).

Both IC and Java Card Platform certificates shall be at most 1.5 years old at the time of issuance of the DK Applet ETR.

1.4 Process

1.4.1 Submission Phase

Prior to the submission phase, the developer shall have selected and contracted a TrustCB licensed evaluation lab and, together with that lab, completed the TrustCB application form for the TOE.

To start the submission phase, a signed copy of the TrustCB application form, together with a draft Security Target, is sent by email to CCC-DK-application@trustcb.com.

TrustCB will respond with a quotation for certification for acceptance by the developer (or certification sponsor) and scheme owner. Upon receipt of acceptance of the quotation by both parties, TrustCB will issue an invoice for the payment of the certification fee to the scheme owner.

The evaluation phase can commence once the quotation has been accepted.

1.4.2 Evaluation Phase

There are two stages to the Evaluation phase in the CCC DK scheme:

- Vulnerability analysis and test plan (EM1+EM2 in [TrustCB_SP]).
- Test results (EM3 in [TrustCB_SP]).

The result of the successful completion of these two stages is the issuance of an ETR by the licensed lab.

1.4.3 Certification Phase

The final certification assessment is performed only after the ETR has been issued. The result of a successful certification assessment is issuance of a CCC DK Applet security certificate by TrustCB

The certificate validity period for CCC DK certificates is three (3) years from the ETR issue date. This applies to both first certifications and re-certifications.

In case of maintenance, the re-issued certificate will be identified through an increase in the certificate iteration identifier and the issuance date (i.e. a certificate with certificate iteration identifier '-01' will be reissued with '-02', and the date entry on the certificate will list the original certificate issuance date and the 2nd issuance date). The certificate expiry date will stay the same. The re-issued certificate will be posted on the scheme website. The original certificate will also be retained on the website.

1.5 Certification Marks and Logos

TrustCB does not issue a Certification Mark for CCC DK certified products.

The TrustCB issued certificate for a compliant product includes the scheme logo, owned by Car Connectivity Consortium.

1.6 Lab licensing

The requirements for TrustCB lab licensing are:

- Valid TrustCB licensing in the technical domain of smartcards and similar devices, and
- Valid listing on SOGIS.eu as "Qualified EAL1-7 for "Smartcards and similar devices"", and
- CCC authorization as a security evaluation lab.

2 Acceptance services

Complementing the certification services, TrustCB also performs the acceptance checks for [Scheme FW]:

- MDF PP/CMD PP acceptance
  - MDF PP/CMD PP Certification Requirements
  - Claim Hardware Equivalency
  - MDF PP/CMD PP Recertification Requirement
  - Conditional Certificate
- PCI-DSS acceptance
- ISO 27001 acceptance
- Self-Assessment questionnaire acceptance

Contact CCC-DK@trustcb.com for details of this process.

3 Reference Materials

Unless otherwise stated, the latest published version applies.

Table 1 CCC DK Documents

Title	Location	Reference
TrustCB Application Form - CCC DK	https://trustcb.com/automotive/CCC-DK	[CCC DK-AF]
TrustCB Shared Scheme Procedures	https://trustcb.com/about-us/policies-procedures/	[TrustCB_SP]
TrustCB Scheme Procedure for CCC DK	https://trustcb.com/automotive/CCC-DK	[TrustCB_CC-DK]
GlobalPlatform Technology Secure Element Protection	https://globalplatform.org/specs-library/secure-element-protection-profile/	[GPPP]
Composite product evaluation for Smart Cards and similar devices	https://sogis.eu/	[JIL-comp]
Security IC Platform Protection Profile with Augmentation Packages	https://commoncriteriaportal.org/	[PP0084]
Java Card Protection Profile – PP0099	https://www.oracle.com/java/technologies/javacard-protection-profile.html	[PP99]
Available to CCC members only:		
[CCC-CP-001] CCC Digital Key Certification Scheme Framework	CCC member access only	[Scheme FW]
[CCC-PR-010] CCC Digital Key Certification Program Management Document	CCC member access only	[PMD]
[CCC-CP-023] Protection Profile of Digital Key Applet	CCC member access only	[PP]
[CCC-CP-024] Guidance for DK Applet Protection Profile Evaluation	CCC member access only	[CCC-CP-024]
[CCC-CP-026] Digital Key Product and Certification Requirements	CCC member access only	[CCC-CP-026]

Note: Refer to the [CCC DK AF] for reference document versions