Car Connectivity Consortium

CCC Digital Key®

Digital Key Applet Compliance: Test Environment

Version 1.0
(CCC-CP-012)

VERSION HISTORY

Version	Date	Comment
1.0	2023-10-16	Approved by CCC Board.
1.0	2024-08-02	Updated Legal Notice for Certification Documents.

LEGAL NOTICE

The copyright in this certification document is owned by the Car Connectivity Consortium LLC ("CCC LLC"). Use of this certification document and any related intellectual property contained in this certification document (collectively, the "Certification Document"), is governed by these license terms and the CCC Intellectual Property Rights Policy (the "IPR Policy").

Use of the Certification Document by any party who is not a member of CCC LLC (each such party, a "Member") is prohibited unless such party has obtained the express written consent of CCC LLC or has duly executed a license agreement with CCC LLC. The IPR Policy governs the legal rights applicable to the creation and licensing of the Certification Document, as documentation created by CCC or one of its Committees, as such term is defined in the IPR Policy. This Certification Document, regardless of its title or content, is not a Final Specification as defined in the IPR Policy.

CCC LLC hereby grants each Member a right to use and to make verbatim copies of the Certification Document for the purposes of developing, performing, and administering interoperability testing (the "Purpose"). Members are not permitted to make available or distribute this Certification Document or any copies thereof to non-Members other than to their Affiliates (as defined in the IPR Policy) and subcontractors but only to the extent that such Affiliates and subcontractors have a need to know for carrying out the Purpose and provided that such Affiliates and subcontractors accept confidentiality obligations similar to those contained in the Agreement. Each Member shall be responsible for the observance and proper performance by such of its Affiliates and subcontractors of the terms and conditions of this Legal Notice and the IPR Policy. No other license, express or implied, by estoppel or otherwise, to any intellectual property rights are granted herein.

Any use of the Certification Document not in compliance with the terms of this Legal Notice, the IPR Policy and CCC Membership Agreement (the "Membership Agreement") is prohibited, and any such prohibited use may result in termination of the applicable Membership Agreement and other liability permitted by the applicable Agreement or by applicable law to CCC LLC or any of its members for patent, copyright and/or trademark infringement.

THE CERTIFICATION DOCUMENT IS PROVIDED "AS IS" WITH NO WARRANTIES, EXPRESS OR IMPLIED, INCLUDING WITHOUT LIMITATION ANY WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, NONINFRINGEMENT OF ANY THIRD-PARTY INTELLECTUAL PROPERTY RIGHTS, AND COMPLIANCE WITH APPLICABLE LAWS.

Each Member is solely responsible for the compliance by their products and services with any applicable laws and regulations and for obtaining any and all required authorizations, permits, or licenses for their products and services related to such regulations within the applicable jurisdictions. Each Member acknowledges that nothing in the Certification Document provides any information or assistance in connection with securing such compliance, authorizations or licenses. Each Member is responsible for the correct use of the Certification Document.

NOTHING IN THE CERTIFICATION DOCUMENT CREATES ANY WARRANTIES, EITHER EXPRESS OR IMPLIED, REGARDING SUCH LAWS OR REGULATIONS. ALL LIABILITY, INCLUDING LIABILITY FOR INFRINGEMENT OF ANY INTELLECTUAL PROPERTY RIGHTS OR FOR NONCOMPLIANCE WITH LAWS, RELATING TO USE OF THE CERTIFICATION DOCUMENT IS EXPRESSLY DISCLAIMED. BY USE OF THE CERTIFICATION DOCUMENT, EACH MEMBER EXPRESSLY WAIVES ANY CLAIM AGAINST CCC LLC AND ITS MEMBERS RELATED TO USE OF THE CERTIFICATION DOCUMENT.

CCC LLC reserves the right to adopt any changes or alterations to the Certification Document as it deems necessary or appropriate.

TABLE OF CONTENTS

ABBREVIATIONS AND ACRONYMS

ACL	Abstract Communication Layer
BLE	Bluetooth Low Energy
BT	Bluetooth
CA	Certificate Authority
CCC	Car Connectivity Consortium
DK	Digital Key
DUT	Device Under Test
GP	GlobalPlatform
ICS	Implementation Conformance Statement
IXIT	Implementation eXtra Information for Testing
NFC	Near Field Communication
SCP	Secure Channel Protocol
SE	Secure Element
UA	User Authentication
USB	Universal Serial Bus
UWB	Ultra-Wideband

TRADEMARKS

Digital Key is a registered trademark of Car Connectivity Consortium LLC.

Bluetooth is a registered trademark of Bluetooth SIG Inc.

Other names or abbreviations used in this document may be trademarks of their respective owners.

ABOUT

This document forms part of the documentation related to the CCC Digital Key certification program. The CCC Digital Key specifies a system that permits a device, such as a mobile phone, to open and start a vehicle.

The document focuses on the functional certification of the CCC Digital Key applet that runs on the secure element of the device.

Specifically, this document provides the required information for the functional certification of the CCC Digital Key applet based on the CCC Digital Key Specification [2].

The specification lists a series of requirements, either explicitly or within the text, which are mandatory elements for a compliant solution. Recommendations are given, to ensure optimal usage and to provide suitable performance. All recommendations are optional.

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are following the notation as described in RFC 2119 [1].

> MUST: This word, or the terms "REQUIRED" or "SHALL", mean that the definition is an absolute requirement of the specification.
>
> MUST NOT: This phrase, or the phrase "SHALL NOT", mean that the definition is an absolute prohibition of the specification.
>
> SHOULD: This word, or the adjective "RECOMMENDED", mean that there may exist valid reasons in particular circumstances to ignore a particular item, but the full implications must be understood and carefully weighed before choosing a different course.
>
> SHOULD NOT: This phrase, or the phrase "NOT RECOMMENDED" mean that there may exist valid reasons in particular circumstances when the particular behavior is acceptable or even useful, but the full implications should be understood and the case carefully weighed before implementing any behavior described with this label.
>
> MAY: This word, or the adjective "OPTIONAL", means that an item is truly optional. One vendor may choose to include the item because a particular marketplace requires it or because the vendor feels that it enhances the product while another vendor may omit the same item. An implementation which does not include a particular option MUST be prepared to interoperate with another implementation which does include the option, though perhaps with reduced functionality. In the same vein an implementation which does include a particular option MUST be prepared to interoperate with another implementation which does not include the option (except, of course, for the feature the option provides.)

1 INTRODUCTION

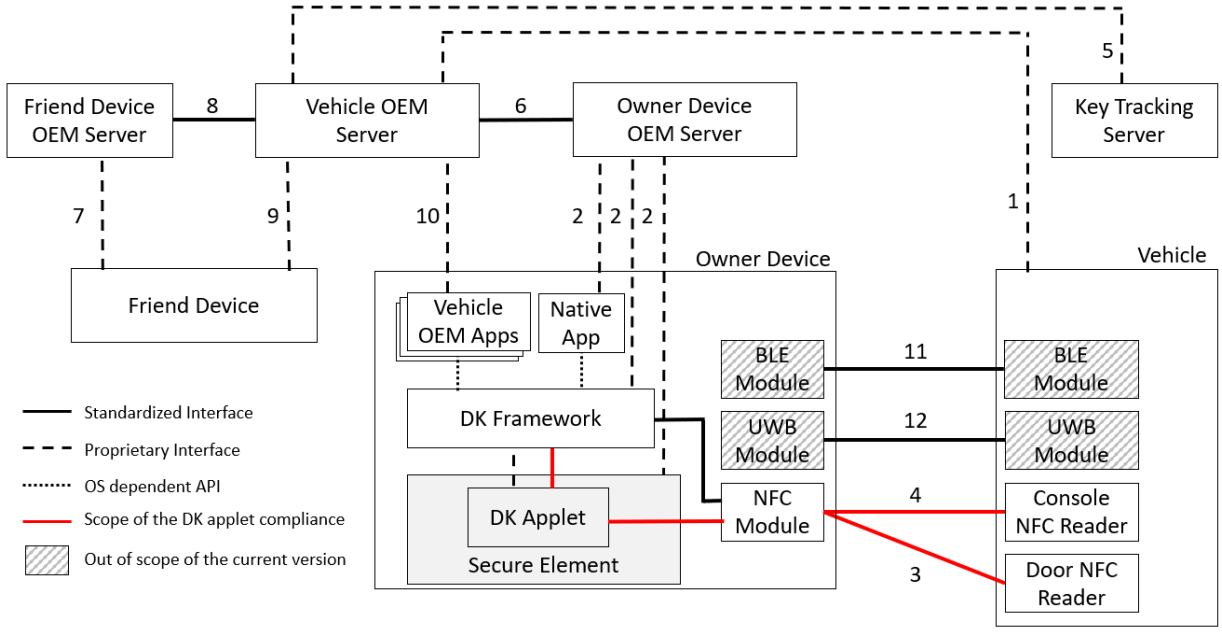
This document describes the test environment for the CCC Digital Key Applet Compliance testing.

NOTE: This version of the document is based on Digital Key Release 3, version 1.1.1 or later [2]. This version of the document doesn't cover the CREATE RANGING KEY and DELETE RANGING KEYS commands.

2 DIGITAL KEY APPLET

The following diagram shows the overall Digital Key architecture. The diagram is a composition of two separate diagrams from the CCC Digital Key Specification [2].

Figure 2-1 Architecture View of Digital Key System



The Digital Key applet is defined in Section 15 of the CCC Digital Key Specification [2]. The functional certification testing will be performed in a specific sequence. Test scripts will test the commands as specified in Section 15.3 of the CCC Digital Key Specification [2].

The stated requirements are listed in detail, together with the required test scenarios in the CCC Digital Key Applet Compliance Test Suite [3].

The Digital Key Applet Compliance ICS [4] and IXIT [5] defines the implementation conformance statement (ICS) and the implementation extra information for testing (IXIT). It has to be filled in by the Client (i.e., SE vendor) seeking certification of a Digital Key Applet. The ICS part defines the capabilities and options supported by a Digital Key applet implementation. The IXIT part provides additional information required by the test tool to execute the test plan. An XML format is specified in [6], which is imported from the Digital Key Applet Compliance test tool. An example XML file is provided in [7]. The XML schema is given in [8].

The profiles for the samples (Device Under Test) to be provided by a client seeking certification of a Digital Key applet are defined in Section 3.6.1 of this document.

The test tool requirements are defined in [9].

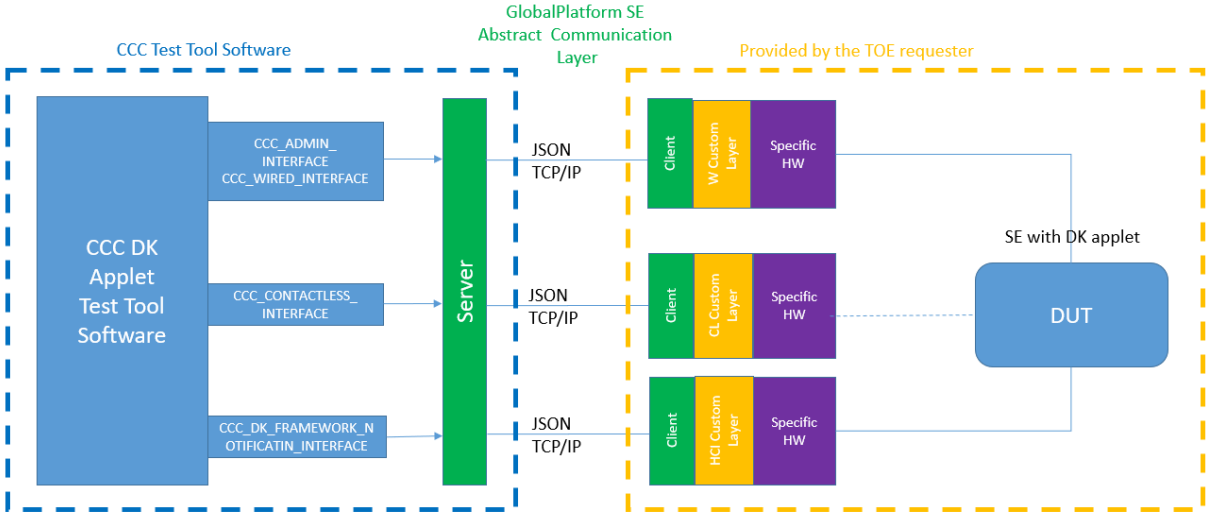
3 TEST ENVIRONMENT

The Device Under Test (DUT) consists of an application running on a Secure Element, which itself is mounted on an evaluation board. The communication between the DUT and the Digital Key Applet Compliance test tool is to be performed by the 'GlobalPlatform SE Abstract Communication Layer' specified by GlobalPlatform [10] (Apache License Version 2.0, January 2004).

To enable this, the DUT has to be submitted to the Authorized Laboratory with all required hardware (i.e. evaluation board), middleware and custom software, required to enable the operation of a Secure Element IP Connector client. The Digital Applet Compliance test tool implements a GlobalPlatform SE Abstract Communication Layer.

The following diagram shows the test setup for the Digital Key applet.

Figure 3-1 Digital Key Applet Test Setup

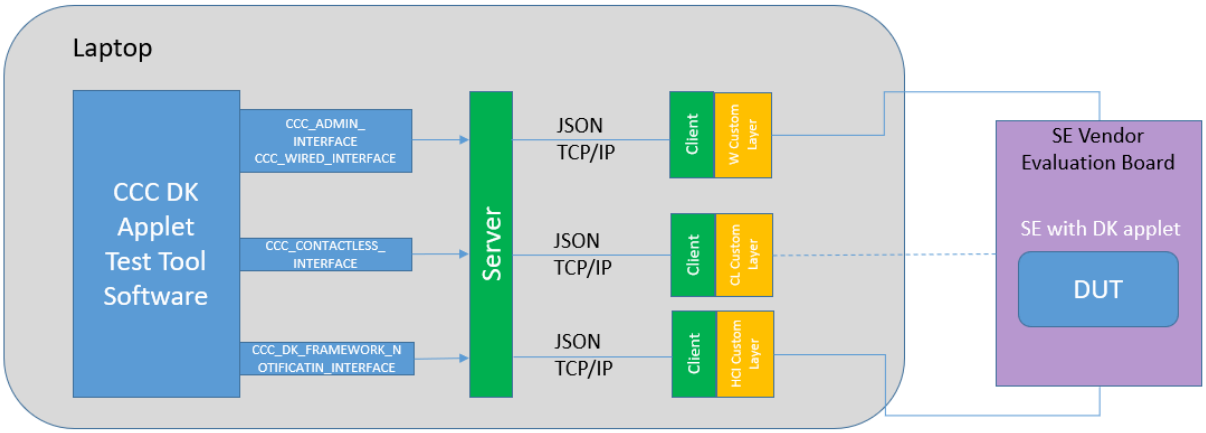


The test system has to implement the setup as defined in Figure 3-2 or Figure 3-3.

3.1 Local Testing

If the evaluation board embedding the DUT and the test tool are physically connected, the system setup is described in Figure 3-2. This setup is the typical setup at the test laboratory and the vendor provides the evaluation board and required software (i.e., the client(s) part of the GlobalPlatform SE Abstract Communication Layer).

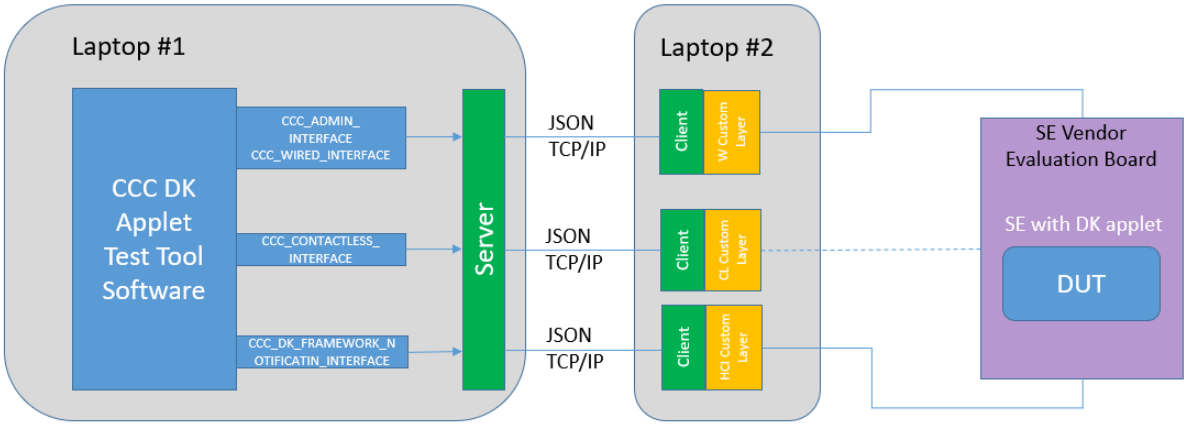
Figure 3-2 Local Test Setup



3.2 Remote Testing

If the tests are performed remotely (e.g., laptop hosting the test tool software and laptop connected to the evaluation board are not in the same location), the system setup is described in Figure 3-3.

Figure 3-3 Remote Test Setup



3.3 GlobalPlatform SE Abstract Communication Layer

The following text is an adapted reproduction of the GlobalPlatform SE Abstract Communication Layer [10].

Messages are exchanged over a TCP socket between the Secure Element (client) and the Digital Key Applet Compliance Test Tool (server).

3.3.1 *Message Format*

Each message consists of a length and a value field. The length value is a 32-bit integer (big-endian). The content of the message body depends on the message.

3.3.1.1 Client Name Message

The first message sent by the client is its name. The body consists of the client's name as an ASCII string.

3.3.1.2 Command Message

The test tool (server) sends command messages to the client. These messages have an ASCII encoded body containing a JSON object.

Table 3-1 GP SE Abstract Communication Layer Command Message

JSON property	Value
Data	The command data as a hexadecimal string (optional).
Request	An integer, identifying the request type (See *Request Types* table).
Timeout	The maximum allowed time for executing this command in milliseconds.

3.3.1.3 Request Types

Table 3-2 describes the usage of the Requests defined in GlobalPlatform SE Abstract Communication Layer [10] for the CCC Digital Key Applet Compliance.

Table 3-2 GP SE Abstract Communication Layer Request Types

Value	Name	Interface	Description
0	REQ_CONNECT	N/A	Currently not in use
1	REQ_DIAG	CCC_ADMIN_INTERFACE	Get diagnostic information from the SE.
2	REQ_DISCONNECT	CCC_ADMIN_INTERFACE	The client disconnects. No response expected.
3	REQ_ECHO	CCC_ADMIN_INTERFACE	Echo the command data.
4	REQ_INIT	N/A	Currently not in use
5	REQ_RESTART	N/A	Currently not in use
6	REQ_COMMAND	CCC_WIRED_INTERFACE	Send an ISO-7816 command APDU.
7	REQ_COMMAND_A	CCC_CONTACTLESS_INTERFACE	Send a type A command.
8	REQ_COMMAND_B	CCC_CONTACTLESS_INTERFACE	Send a type B command.
9	REQ_COMMAND_F	CCC_CONTACTLESS_INTERFACE	Send a type F command.
10	REQ_COLD_RESET	CCC_ADMIN_INTERFACE	Perform a cold reset of the SE.

Value	Name	Interface	Description
11	REQ_WARM_RESET	CCC_ADMIN_INTERFACE	Perform a warm reset of the SE.
12	REQ_POWER_OFF_FIELD	CCC_ADMIN_INTERFACE	Power off the CLF.
13	REQ_POWER_ON_FIELD	CCC_ADMIN_INTERFACE	Power on the CLF.
14	REQ_POLL_A	CCC_CONTACTLESS_INTERFACE	Enable exclusive Contactless Type A polling
15	REQ_POLL_B	CCC_CONTACTLESS_INTERFACE	Enable exclusive Contactless Type B polling
16	REQ_POLL_F	CCC_CONTACTLESS_INTERFACE	Enable exclusive Contactless Type F polling
17	REQ_POLL_ALL_TYPES	CCC_CONTACTLESS_INTERFACE	Enable all Contactless Types supported by the contactless reader (e.g., A, B, F)
18	REQ_DEACTIVATE_INTERFACE	CCC_ADMIN_INTERFACE, CCC_WIRED_INTERFACE, CCC_CONTACTLESS_INTERFACE	Inform the SE Agent that the addressed interface will no more process commands other than a REQ_ACTIVATE_INTERFACE
19	REQ_ACTIVATE_INTERFACE	CCC_ADMIN_INTERFACE, CCC_WIRED_INTERFACE, CCC_CONTACTLESS_INTERFACE	Inform the SE Agent that the addressed interface is to be activated to process further commands
20	REQ_GET_NOTIFICATIONS	CCC_DK_FRAMEWORK_NOTIFICATION_INTERFACE	Return content of the notification buffer which contains all the collected notifications associated to a specified AID
21	REQ_CLEAR_NOTIFICATIONS	CCC_DK_FRAMEWORK_NOTIFICATION_INTERFACE	Clear all the collected notifications associated to a specified AID

3.3.1.4 Response Message

The secure element (client) sends response messages when receiving a command message from the server. Like the command messages, they have an ASCII encoded JSON body.

Table 3-3 GP SE Abstract Communication Layer Response Message

JSON property	Value
response	The response data (See Response Data table).
err_server_code	An integer identifying error or success on the server layer (See Error Codes table).
err_server_description	A string describing the error on the server layer, or "OK" in case of success.

JSON property	Value
err_client_code	An integer identifying error or success on the client layer (See Error Codes table).
client_description	A string describing the error on the client layer, or "OK" in case of success.
err_terminal_code	An integer identifying error or success on the terminal layer (See Error Codes table).
terminal_description	A string describing the error on the terminal layer, or "OK" in case of success.
err_card_code	An integer identifying error or success on the card layer (See Error Codes table).
err_card_description	A string describing the error on the card layer, or "OK" in case of success.

The properties `err_server_code` and `err_server_description` are always set to "`0`" and "`OK`" when transmitted by the client. When working with response message objects, the server may internally set these properties to handle internal server errors.

3.3.1.5 Response Data

Table 3-4 describes the Requests defined in GlobalPlatform SE Abstract Communication Layer [10] that are used in the context of the CCC Digital Key Applet Compliance.

Table 3-4 GP SE Abstract Communication Layer Response Message

Request	Data
REQ_CONNECT	N/A
REQ_DIAG	A string containing diagnostic information.
REQ_DISCONNECT	N/A
REQ_ECHO	The data from the command.
REQ_INIT	N/A
REQ_RESTART	N/A
REQ_COMMAND	The response APDU as a hexadecimal string.
REQ_COMMAND_A	The response as a hexadecimal string.
REQ_COMMAND_B	The response as a hexadecimal string.
REQ_COMMAND_F	The response as a hexadecimal string.
REQ_COLD_RESET	The ATR as a hexadecimal string.
REQ_WARM_RESET	The ATR as a hexadecimal string.
REQ_POWER_OFF_FIELD	N/A
REQ_POWER_ON_FIELD	N/A
REQ_POLL_A	N/A
REQ_POLL_B	N/A
REQ_POLL_F	N/A
REQ_POLL_ALL_TYPES	N/A
REQ_DEACTIVATE_INTERFACE	N/A
REQ_ACTIVATE_INTERFACE	N/A

Request	Data
REQ_GET_NOTIFICATIONS	The notification buffer which contains all the collected notifications associated to a specified AID
REQ_CLEAR_NOTIFICATIONS	N/A

3.3.1.6 Return Codes

Table 3-5 describes the Return Codes defined in GlobalPlatform SE Abstract Communication Layer [10] that are used in the context of the CCC Digital Key Applet Compliance.

Table 3-5 GP SE Abstract Communication Layer Return Codes

Value	Name	Description
0	SUCCESS	The command was successfully executed.
-1	ERR_TIMEOUT	The command could not be executed within the given time.
-2	ERR_NETWORK	A network error occurred.
-3	ERR_CLIENT_CLOSED	The client disconnected.
-4	ERR_INVALID_STATE	The command cannot currently be executed.
-5	ERR_INVALID_REQUEST	The command was not understood by the client.
-6	ERR_JSON_PARSING	The command (or response) could not be parsed.
-7	ERR_INVALID_TERMINAL	The terminal is not available.

3.4 Management of the Notifications of the Digital Key framework

When the commands are processed over the contactless interface, the notification of the Digital Key Framework may use the Host Controller Interface (HCI) event EVT_TRANSACTION as defined in Section 15.3.1.9 of CCC Digital Key Specification [2].

In such a case the client appends the notification(s), tag(s) 7F60h as defined in Table 15-8 of CCC Digital Key Specification [2] into the notification buffer corresponding to the AID of the DK Applet as defined in GlobalPlatform SE Abstract Communication Layer [10]. The notifications are appended to the list in sequential order they are generated by the Digital Key applet. As defined in GlobalPlatform SE Abstract Communication Layer [10], the content of the buffer can be retrieved using the request REQ_GET_NOTIFICATIONS.

When the commands are processed over the wired interface, the notifications of the Digital Key Framework may use the GET NOTIFICATION command as defined in Section 15.3.1.9 of CCC Digital Key Specification [2].

3.5 Test PC and Application

The test application running on the test PC meets the requirements as specified in the CCC Digital Key Applet Compliance Test Tool Requirements [9] document.

3.6 Device Under Test Preparation

To ease the test tool implementation, the Digital Key applet will be loaded, installed and with specific numbers of Instance CA created in the SE. This section will provide the pre-requisite parameters for the Digital Key applet before testing.

3.6.1 *DUT Profiles' Information*

In order to perform the functional certification testing, the Client (i.e., SE vendor) needs to provide SE samples with Digital Key applet installed and Instance CAs created according to the two different DUT Profiles defined in Table 3-6, which includes:

- The values to be used in tag C9h during the INSTALL for INSTALL parameters as defined in Table 15-4 of CCC Digital Key Specification [2].
- The number of Instance CAs to be created. The elements needed to create the different Instance CAs are defined in Section 4.

Table 3-6 Device Under Test Profiles

All values are in hexadecimal.	DUT Profile (All values are in hexadecimal)	
	1 Default Profile	2
install_param_endpoint_count (default=0Ah)	Default	34h
install_param_instance_CA_count (default=03h)	Default	Default
install_param_internal_buffer_size (default=0900h)	Default	0440h
install_param_max_allocatable_private_mailbox_size (default=0800h)	Default	Default
install_param_max_allocatable_confidential_mailbox_size (default=0800h)	Default	Default
install_param_oid_external_ca (default=2B0601040182C4690502)	Default	Default
install_param_oid_instance_ca (default=2B0601040182C4690503)	Default	Default
install_param_oid_endpoint (default=2B0601040182C4690504)	Default	Default
Number of Instance CAs (default=3)	Default	1

3.6.2 *DUT Information*

Each individual DUT sample is configured with specific information. This section defines the information items that are DUT sample specific and specifies how this information is transferred to the CCC and the relevant authorized test laboratory.

Table 3-7 Device Under Test Information

	DUT Information
instance_ca_identifier_tst1	Vendor specific
instance_ca_identifier_tst2	Vendor specific
instance_ca_identifier_tst3	Vendor specific

4 INSTANCE CA MANAGEMENT

Creation of Instance CAs onto the samples is a pre-requisite prior to any tests being carried out with the test software.

The SE vendor has to create instance CA(s) on the samples according to the following requirements:

- The number of Instance CAs to be created on a given sample is defined in Table 3-6.The Device OEM SK defined in Section 4.3.1 will be used to sign the Instance CA Certificate [E].
- The first Instance CA will be created with identifier TST1. Subsequent Instance CAs will be created in sequence, TST2, TST3 etc.

Each SE vendor has to provide the Instance CA.PK corresponding to each Instance CA created on the various samples defined in Table 3-6. This information is part of the ICS [6].

Owner Pairing CA Set

Owner pairing (device verifying vehicle, only for SE centric model):

```
-> Device OEM CA [D] (self-signed, PK stored in applet) -> Pregenerated
--> Vehicle OEM CA Certificate [M] (signed by Device OEM CA) -> Pregenerated
---> (optional) Intermediate CA Certificate (signed by Vehicle OEM CA) ->
Pregenerated
----> Vehicle Public Key Certificate [K] (signed by either Vehicle OEM CA or
Intermediate CA) -> Generated on the fly by the test tool
```

Owner pairing (vehicle verifying device):

```
-> Vehicle OEM CA [J] (self-signed) -> Pregenerated
--> Device OEM CA [F] (signed by Vehicle OEM CA) -> Pregenerated
---> Instance CA [E] -> (signed by Device OEM CA) -> Provided by eSE vendor
for each Instance CA in the sample, to be validated by the test tool
----> DK Certificate [H] -> Generated in the applet, to be validated by the
test tool
```

4.1 Friend Key Sharing CA Set

Friend key sharing (i.e. AUTHORIZE ENDPOINT):

```
-> Vehicle OEM CA [J] (PK stored in applet during CREATE ENDPOINT for owner)
-> Pregenerated
--> friend Device OEM CA [F] (signed by Vehicle OEM CA) -> Pregenerated
```

```
---> friend Instance CA certificate [E] (signed by friend Device OEM CA) ->
Pregenerated
----> friend DK Certificate [H] -> generated on the fly by the test bench,
based on TC requirements
```

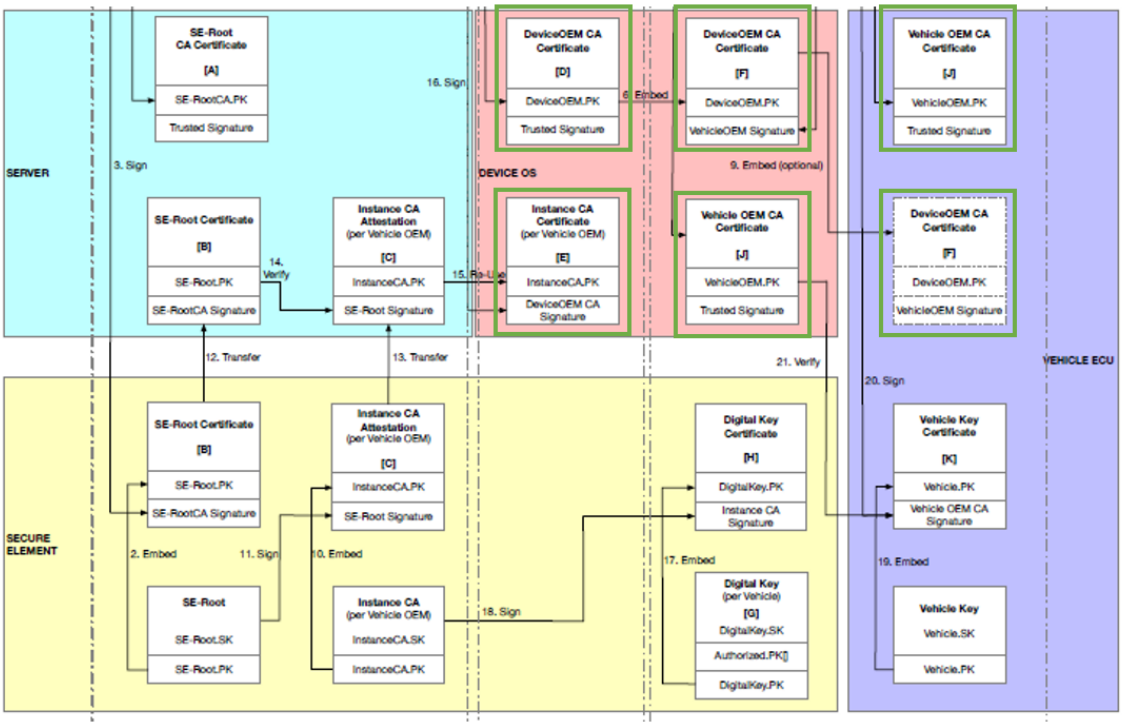
4.2 Certificate Common Name definitions

Proposed certificate Common Name definitions:
Vehicle OEM CA [J][M]: TEST-VEHICLE-ROOT-CA-E
Vehicle OEM Intermediate CA: TEST-VEHICLE-ROOT-CA-INTERMEDIATE-WW-E
Device OEM CA [D][F]: TEST-DEVICE-ROOT-CA
Instance CA [E]: TSTx
Vehicle Public Key Certificate [K]: V.TSTx.WWE.BRND.[dynamic vehicle identifier]

4.3 CA Key Pairs

The following diagram taken from the CCC Digital Key Specification [2] shows the specified test certificates highlighted in green boxes.

Figure 4-1 Device and Vehicle Certificates



4.3.1 *Device OEM CA key pair*

PK:

```
0487FCFA316608A03209DE09A0279E2CAC06BAC27037491E9CC0807DF523F3628ADCE8C82488
08DD03C967904FFF7B9D1EC5BF0C74F7EB2C27F952DD1F46AC5D38
```

SK:

```
6B3A4E5AA2A2DC1483114D4F182172D0890EDDAB47AAC45290845BF5FBF97D03
```

4.3.2 *Friend's Device OEM CA keypair*

PK:

```
04A87028532805919FAD3F3818C6BCCA228BC314A5066F54A2F3D8DA1B31596A988D44B15C27
A7561F1AAEE608E2D35AAA91B40C38FD0836732636C8C40216B398
```

SK:

```
02F8294560AE1442E8B4814878B615671FFBDA9AE430F0029EC3CDFA01C81AC0
```

4.3.3 *Vehicle OEM CA keypair #1*

PK:

```
04B28E59010AEAE66FD0346957D8162CB58FAB6AD9F6264EAAAC997737C67140DCF646822F3E
1B1C6F76BF7E75A4F081868763C22F0412658B6E8F2300CF6DDCC1
```

SK:

```
5123C54F23EE59F75E7AD5E3DC14814BB9F73298F774F2FDEAF73CA5B1E8329E
```

4.3.4 *Vehicle OEM Intermediate CA keypair #1*

PK:

```
04063A89481D67C9855CB3D773D1BE0C7AAC98E4CC5DB47CDCA9411267CFE2E1550FB8656169
D1F8A4EF08745D980D070C9E6E907C3FF98C4723D6ED1A50E2CA4F
```

SK:

```
E49298E5C786CC1E840009F39C67813C3661CF736B7A83AD015E7AC0F2A28CFA
```

4.3.5 *Friend's Instance CA keypair #1*

PK:

```
047C4DE84D474C3BE9F57278EAB83C7AA3AC2DE5277D63B17696AA77BDBBCA09D52FCEDF2523
3D4A1A69F11263159037E18D9426591A20729E37F5A3423B8A6649
```

SK:

```
31FFC50CA7CA0F350A035E6531DE5B4D4609BEF23DCE67D791A9259CD4759834
```

4.3.6 *Vehicle OEM CA keypair #2*

PK:

```
0490EC0BC25D9D715A38EE9AB136CF7BD9BD9E207275219ACEBAA5CF89986B075A196F6B5CAD
D4F638DF3D362673CE65FE5DA0F202632B46E886D0106BC4E91899
```

SK:

```
D2948397A63A1B9A22ADB744CBCC97CCFE4A2B6DD0A6053F26584917844ABFBC
```

4.3.7 *Vehicle OEM Intermediate CA keypair #2*

PK:

```
043A8F98E3BC8ECAE230F0A77E8D9851FD06F703043FBA7065A067B4220F07C25CD89076740E
1DFDCAB7C78A5704F8D2BA78293F9746695D28F4374E3A27F425F4
```

SK:

```
E29384423E91BC325722C2437F858E5059A2E9C7AEAFC37A7899C8ED231F19D2
```

4.3.8 *Friend's Instance CA keypair #2*

PK:

```
0471F31E6C6492B23EE09F1880048CF55B91279F859B3A30AF5514E2AEA55C493AD3DAAE0604
6241A6A7156CCDD64DD13AA1783754E6FB31D42197F8202E3D8673
```

SK:

```
19B10A63ACE24E2055A8DBFF7164573BA05DE4443A71E3EA69C2127A693CB006
```

4.3.9 *Vehicle OEM CA keypair #3*

PK:

```
041811CB872C282770BF95954AE2B4277A2109C7B931C6DFBFDA2A845070F6C1072BCB1866F4
C56F207CFC0B2632ABC4AE4247A8F11753CF8279AD64ED421CA3FF
```

SK:

```
E3B4D58378A59CC7E0523C5EF12BEC237D478F7A9CC536820FE5F43F6AE8E001
```

4.3.10 *Vehicle OEM Intermediate CA keypair #3*

PK:

```
04750A710B0A83691EC0807BBDE46DEEDF7209EEC48E646A389B21D696790E51E7A4078A8492
B5DAC872B97882B1AB1EA7D5D1192A0DE4BCEB83B3B8325BAB39BB
```

SK:

```
FEFCF1AAD066B94736851DF92DCBDFC8153B29C799A9AEB03247A396ED315D9D
```

4.3.11 *Friend's Instance CA keypair #3*

PK:

```
040BDEC80365AFB2C88028A23B2793BB013C9A4B6518F43CE38427437A1647307115314B4A3A
8FE00E318CE19EBB012AF94DEC56E781500A1E13F31D5BFE627E75
```

SK:

```
CBC8619E93616B5DF2972A88044315F8D859FAA3BD2267BAC9D1366930E1A224
```

4.3.12 *Device OEM CA [D] (self-signed)*

```
308201B230820158A003020102020802A986F77F65E16F300A06082A8648CE3D040302301E31
1C301A06035504031313544553542D4445564943452D524F4F542D43413020170D3230303130
313030303030305A180F323035303031303130303030303030305A301E311C301A06035504031313
544553542D4445564943452D524F4F542D4341305930130607 2A8648CE3D020106082A8648CE
3D0301070342000487FCFA316608A03209DE09A0279E2CAC06BAC27037491E9CC0807DF523F3
628ADCE8C8248808DD03C967904FFF7B9D1EC5BF0C74F7EB2C27F952DD1F46AC5D38A37E307C
3016060A2B0601040182C46905020101FF040530030201013 00E0603551D0F0101FF04040302
020430120603551D130101FF040830060101FF020101301F0603551D230418301680142766 62
923C2331A74393AF4AEDC035F44E41C950301D0603551D0E041604142766629 23C2331A74393
AF4AEDC035F44E41C950300A06082A8648CE3D040302034800304502207891 6B77B6ECE53046
04E12724511AE4A5E8C0A7C5BD2C4ABD259A08FA9932F7022100BC95E52CE07326A51A6417AF
75FE0E28C009CB1D8467177C5766FF89F5CD7FBE
```

4.3.13 *Friend's Device OEM CA [D] (self-signed)*

```
308201C130820166A003020102020820E7A51BF018576B300A06082A8648CE3D040302302531
233021060355040313 1A544553542D465249454E442D4445564943452D524F4F542D43413020
170D3230303130313030303030305A180F323035303031303130303030305A302531233021
0603550403131A544553542D465249454E442D4445564943452D524F4F542D43413059301306
072A8648CE3D020106082A8648CE3D03010703420004A87028532805919FAD3F3818C6BCCA22
8BC314A5066F54A2F3D8DA1B31596A988D44B15C27A7561F1AAEE608E2D35AAA91B40C38FD08
36732636C8C40216B398A37E307C3016060A2B0601040182C46905020101FF04053003020101
300E0603551D0F0101FF040403020204301206035 51D130101FF040830060101FF020101301F
0603551D230418301680142C751100BF23DCAFEEA4503F8B961EFF36967C32301D0603551D0E
041604142C751100BF23DCAFEEA4503F8B961EFF36967C32300A06082A8648CE3D0403020349
003046022100A3A2C3B9DB687A3D4CB4244BC2DE23B219BD5AB80FAE6B2F5A8B6C205744DCA2
022100AA93E848BA3FAFF51C4ABB974F9409D23068E6DCBE8B910784B20B4DB18446F5
```

4.3.14 *Device OEM CA [F] (signed by vehicle OEM CA #1)*

```
308201B73082015DA00302010202081C3942CDB246EED4300A06082A8648CE3D040302302331
21301F06035504031318544553542D56454849434C452D524F4F542D43412D312D453020170D
32303031303130303030305A180F32303530303130313030303030305A301E311C301A0603
55040313135445535542D4445564943452D524F4F542D4341305930130607 2A8648CE3D020106
082A8648CE3D030107034200048 7FCFA316608A03209DE09A0279E2CAC06BAC27037491E9CC0
807DF523F3628ADCE8C8248808DD03C967904FFF7B9D1EC5BF0C74F7EB2C27F952DD1F46AC5D
38A37E307C3016060A2B0601040182C46905020101FF040530030201013 00E0603551D0F0101
FF040403020204301206035 51D130101FF040830060101FF020101301F0603551D2304183016
8014AC7CF4C686C7F9184F276F95415496EF367C3D7B301D0603551D0E04160414276662923C
2331A74393AF4AEDC035F44E41C950300A06082A8648CE3D040302034800304502207024185 5
B9DC59E52682DF86823C9623F7E4A1FF7D7E1425B7399A56EB035B4A022100F2A58D0D627F6D
E371DD52905C51D6F67C9A08C3B16021BF3511C705EABB0D2F
```

4.3.15 *Friend's Device OEM CA [F] (signed by vehicle OEM CA #1)*

```
308201BE30820164A00302010202083377FC9F5B8F5DF9300A06082A8648CE3D040302302331
21301F06035504031318544553542D56454849434C452D524F4F542D43412D312D453020170D
32303031303130303030305A180F32303530303130313030303030305A3025312330210603
550403131A544553542D465249454E442D4445564943452D524F4F542D4341305930130607 2A
8648CE3D020106082A8648CE3D03010703420004A87028532805919FAD3F3818C6BCCA228BC3
14A5066F54A2F3D8DA1B31596A988D44B15C27A7561F1AAEE608E2D35AAA91B40C38FD083673
2636C8C40216B398A37E307C3016060A2B0601040182C46905020101FF040530030201013 00E
0603551D0F0101FF040403020204301206035 51D130101FF040830060101FF020101301F0603
551D23041830168014AC7CF4C686C7F9184F276F95415496EF367C3D7B301D0603551D0E0416
04142C751100BF23DCAFEEA4503F8B961EFF36967C32300A06082A8648CE3D040302034800 30
45022001CBAB2A13FC3D4961747AF7015681BFC448207322AD38B254FEC697B636DF3A022100
C87D52721FB1F99881B85A407DF17A6F67C9078BB5EE882A0A2D233114338337
```

4.3.16 *Vehicle OEM CA #1 [J] (self-signed)*

```
308201A73082014DA00302010202086A2BC91299CD04F1300A06082A8648CE3D040302302331
21301F06035504031318544553542D56454849434C452D524F4F542D43412D312D453020170D
32303031303130303030305A180F32303630303130313030303030305A30233121301F0603
55040313185445535542D56454849434C452D524F4F542D43412D312D453059301306072A8648
CE3D020106082A8648CE3D03010703420004B28E59010AEAE66FD0346957D8162CB58FAB6AD9
F6264EAAAC997737C67140DCF646822F3E1B1C6F76BF7E75A4F081868763C22F0412658B6E8F
2300CF6DDCC1A3693067300E0603551D0F0101FF040403020204301206035 51D130101FF0408
30060101FF020101302206035 51D230101FF041830168014AC7CF4C686C7F9184F276F954154
96EF367C3D7B301D0603551D0E04160414AC7CF4C686C7F9184F276F95415496EF367C3D7B30
0A06082A8648CE3D040302034800304502210083B8B2F463B3754F29818F17C82DE84FDABED4
4DA07DFCC46B34A5B7980F3ACD0220065D07D983EB71E4B3542DA754587429A10FEA01473C7C
1004F88EFEB31179A5
```

4.3.17 *Vehicle OEM CA #1 [M] (signed by device OEM CA)*

```
308201A330820148A003020102020208639EA26F03563A19300A06082A8648CE3D040302301E31
1C301A06035504031313544553542D4445564943452D524F4F542D43413020170D3230303130
313030303030305A180F323036303031303130303030305A30233121301F06035504031318
544553542D56454849434C452D524F4F542D43412D312D453059301306072A8648CE3D020106
082A8648CE3D03010703420004B28E59010AEAE66FD0346957D8162CB58FAB6AD9F6264EAAAC
997737C67140DCF646822F3E1B1C6F76BF7E75A4F081868763C22F0412658B6E8F2300CF6DDC
C1A3693067300E0603551D0F0101FF040403020204301206035 51D130101FF040830060101FF
02010130220603551D230101FF041830168014276662923C2331A74393AF4AEDC035F44E41C9
50301D0603551D0E04160414AC7CF4C686C7F9184F276F95415496EF367C3D7B300A06082A86
48CE3D040302034900304602210 0E25550568346175DCC9F7EF2A47BB47FB31429366E8E91A3
BE674EB6A1838085022100E4319BBF5AEEF1D452442833108DC66769C486E4576B97A4CBCFBB
D1040F1FEA
```

4.3.18 *Vehicle OEM Intermediate CA (signed by vehicle OEM CA #1)*

```
308201B63082015DA003020102020857096883 81FF7C10300A06082A8648CE3D040302302331
21301F06035504031318544553542D56454849434C452D524F4F542D43412D312D453020170D
323030313031303030303030305A180F323036303031303130303030305A30333131302F0603
55040313285445535 42D56454849434C452D524F4F542D43412D494E5445524D454449415445
2D312D57572D453059301306072A8648CE3D020106082A8648CE3D03010703420004063A8948
1D67C9855CB3D773D1BE0C7AAC98E4CC5DB47CDCA9411267CFE2E1550FB8656169D1F8A4EF08
745D980D070C9E6E907C3FF98C4723D6ED1A50E2CA4FA3693067300E0603551D0F0101FF0404
030202043012060 3551D130101FF040830060101FF020101302206 03551D230101FF04183016
8014AC7CF4C686C7F9184F276F95415496EF367C3D7B301D0603551D0E041604147F6643A662
2F1D739556AC8E41B50D269FFDA0A9300A06082A8648CE3D040302034700304402202603 62B0
8116F66699B4CB584218002E1600224A9F4E938E2C59D0BFFE48936C022069EDADE6D9691AD7
7EDC35D2FAEFBD4A2D86FB563A4EBC1E8EF36D45D628A528
```

4.3.19 *Friend's Instance CA #1 [E] (signed by friend's device OEM CA)*

```
308201B930820160A00302010202082F326ED8F2E06C11300A06082A8648CE3D040302302531
233021060355040313 1A544553542D465249454E442D4445564943452D524F4F542D4341301E
170D323030313031303030303030305A170D343030313031303030303030305A300F310D300B0603
55040313045453543130593013060 72A8648CE3D020106082A8648CE3D030107034200047C4D
E84D474C3BE9F57278EAB83C7AA3AC2DE5277D63B17696AA77BDBBCA09D52FCEDF25233D4A1A
69F11263159037E18D9426591A20729E37F5A3423B8A6649A3818F30818C3026060A2B060104
0182C46905030101FF04153013020101040400000001040870 6C6174666F726D300E0603551D
0F0101FF040403020204301206035 51D130101FF040830060101FF020100301F0603551D2304
18301680142C751100BF23DCAFEEA4503F8B961EFF36967C32301D0603551D0E0416041424C8
F977621FDE7C07875CC240A74FB60A888104300A06082A8648CE3D040302034700304402204D
F6E52DE90EC6544D3FB1E40B36C38A66E5545B5EA4DA86E4B8706D66A76DAB02201BE4A0DF87
AC4743D61A657A2FB0977C8ED1D30EC3726642607BE9B230A8FCFB
```

4.3.20 *Device OEM CA [F] (signed by vehicle OEM CA #2)*

```
308201B73082015DA00302010202083A8171020C01D35F300A06082A8648CE3D040302302331
21301F06035504031318544553542D56454849434C452D524F4F542D43412D322D453020170D
32303031303130303030305A180F32303530303130313030303030305A301E311C301A0603
55040313135445535542D4445564943452D524F4F542D4341305930130607 2A8648CE3D020106
082A8648CE3D030107034200048 7FCFA316608A03209DE09A0279E2CAC06BAC27037491E9CC0
807DF523F3628ADCE8C8248808DD03C967904FFF7B9D1EC5BF0C74F7EB2C27F952DD1F46AC5D
38A37E307C3016060A2B0601040182C46905020101FF040530030201013 00E0603551D0F0101
FF040403020204301206035 51D130101FF040830060101FF020101301F0603551D2304183016
8014BD3513CF0B7FAA73E903058D45CB7A36F9883498301D0603551D0E04160414276662923C
2331A74393AF4AEDC035F44E41C950300A06082A8648CE3D040302034800304502207E2FA136
C07F4DB7815522851725AC26E86E9BD1B0869E7A22069BA05BBA7927022100DA4E66ACD04D15
37238EA59A1ED71DF96BA60E63F32235DD88ADE2AFA77AA759
```

4.3.21 *Friend's Device OEM CA [F] (signed by vehicle OEM CA #2)*

```
308201BF30820164A00302010202082FB5673C9E2448A8300A06082A8648CE3D040302302331
21301F06035504031318544553542D56454849434C452D524F4F542D43412D322D453020170D
32303031303130303030305A180F32303530303130313030303030305A3025312330210603
550403131A544553542D465249454E442D4445564943452D524F4F542D4341305930130607 2A
8648CE3D020106082A8648CE3D03010703420004A87028532805919FAD3F3818C6BCCA228BC3
14A5066F54A2F3D8DA1B31596A988D44B15C27A7561F1AAEE608E2D35AAA91B40C38FD083673
2636C8C40216B398A37E307C3016060A2B0601040182C46905020101FF040530030201013 00E
0603551D0F0101FF040403020204301206035 51D130101FF040830060101FF020101301F0603
551D23041830168014BD3513CF0B7FAA73E903058D45CB7A36F9883498301D0603551D0E0416
04142C751100BF23DCAFEEA4503F8B961EFF36967C32300A06082A8648CE3D040302034900 30
46022100E6B5F292459BE325E8668D19FCD69731CEB881880618A3E5F91EB8CA94C5BE060221
00BE12EE14D1C4423C14756EF445ABA09D76CCDE4D404E4656C45C9F2E448D778E
```

4.3.22 *Vehicle OEM CA #2 [J] (self-signed)*

```
308201A73082014DA00302010202083 49A709D460A2FF6300A06082A8648CE3D040302302331
21301F06035504031318544553542D56454849434C452D524F4F542D43412D322D453020170D
32303031303130303030305A180F32303630303130313030303030305A30233121301F0603
55040313185445535542D56454849434C452D524F4F542D43412D322D453059301306072A8648
CE3D020106082A8648CE3D03010703420004 90EC0BC25D9D715A38EE9AB136CF7BD9BD9E2072
75219ACEBAA5CF89986B075A196F6B5CADD4F638DF3D362673CE65FE5DA0F202632B46E886D0
106BC4E91899A3693067300E0603551D0F0101FF040403020204301206035 51D130101FF0408
30060101FF020101302206035 51D230101FF041830168014BD3513CF0B7FAA73E903058D45CB
7A36F9883498301D0603551D0E04160414BD3513CF0B7FAA73E903058D45CB7A36F988349830
0A06082A8648CE3D040302034800304502210 0F8253D5B956C9CE81241E278101CE436A4E8A5
51836CE1D3BBB45182890675CF022036FD513546B77249811D91C164FCFC4B57D14C740AF2E6
957FFA0219E4D7789A
```

4.3.23 *Vehicle OEM CA #2 [M] (signed by device OEM CA)*

```
308201A230820148A00302010202084542FF1824BB7E0E300A06082A8648CE3D040302301E31
1C301A06035504031313544553542D4445564943452D524F4F542D43413020170D3230303130
313030303030305A180F323036303031303130303030305A30233121301F06035504031318
544553542D56454849434C452D524F4F542D43412D322D453059301306072A8648CE3D020106
082A8648CE3D030107034200490EC0BC25D9D715A38EE9AB136CF7BD9BD9E207275219ACEBA
A5CF89986B075A196F6B5CADD4F638DF3D362673CE65FE5DA0F202632B46E886D0106BC4E918
99A3693067300E0603551D0F0101FF040403020204301206035 51D130101FF040830060101FF
02010130220603551D230101FF041830168014276662923C2331A74393AF4AEDC035F44E41C9
50301D0603551D0E04160414BD3513CF0B7FAA73E903058D45CB7A36F9883498300A06082A86
48CE3D0403020348003045022 02FE9E5B90B7F2BB5D216FEE11376DCCBEC386257132BE045DD
CFC4D0FA284355022100FDC48AC5D4D42EA87110319197AAD375F04E9C0B431D6507BFC7700B
BBD0AA86
```

4.3.24 *Vehicle OEM Intermediate CA (signed by vehicle OEM CA #2)*

```
308201B73082015DA003020102020843D7F385F5DE6788300A06082A8648CE3D040302302331
21301F06035504031318544553542D56454849434C452D524F4F542D43412D322D453020170D
323030313031303030303030305A180F323036303031303130303030305A30333131302F0603
550403132854455354 2D56454849434C452D524F4F542D43412D494E5445524D454449415445
2D322D57572D453059301306072A8648CE3D020106082A8648CE3D030107034200043A8F98E3
BC8ECAE230F0A77E8D9851FD06F703043FBA7065A067B4220F07C25CD89076740E1DFDCAB7C7
8A5704F8D2BA78293F9746695D28F4374E3A27F425F4A3693067300E0603551D0F0101FF0404
030202043012060 3551D130101FF040830060101FF020101302206035 51D230101FF04183016
8014BD3513CF0B7FAA73E903058D45CB7A36F9883498301D0603551D0E041604148F8CD6E9B2
758BFA2027D56747C765CCAAED3C88300A06082A8648CE3D0403020348003045022078 0CC3CB
34F73A2ED03514FD4DAD3779D8BBAA452EAE4AB28218BA74195DA423022100D3B92DCCB16805
1E8F3F3B7602E578AAD1F6BAF48D0B1A3E8F04193A6895FB61
```

4.3.25 *Friend's Instance CA #2 [E] (signed by friend's device OEM CA)*

```
308201BB30820160A00302010202086FCF95041B0A1530300A06082A8648CE3D040302302531
233021060355040313 1A544553542D465249454E442D4445564943452D524F4F542D4341301E
170D323030313031303030303030305A170D343030313031303030303030305A300F310D300B0603
550403130454535432305 9301306072A8648CE3D020106082A8648CE3D030107034200047 1F3
1E6C6492B23EE09F1880048CF55B91279F859B3A30AF5514E2AEA55C493AD3DAAE06046241A6
A7156CCDD64DD13AA1783754E6FB31D42197F8202E3D8673A3818F30818C3026060A2B060104
0182C46905030101FF041530130201010404000000010408706C6174666F726D300E0603551D
0F0101FF040403020204301206035 51D130101FF040830060101FF020100301F0603551D2304
18301680142C751100BF23DCAFEEA4503F8B961EFF36967C32301D0603551D0E0416041437B9
FFF20F1932FC7C910C884970FEE1C1AE96E2300A06082A8648CE3D040302034900304602210 0
865F68C958C268C14C9CCAC29CFA7A7B47C84A7D48721D82729F91115DD442D9022100C7BB17
17E69C88DD237846B28D1613E0A716204A52340811D667654134783AA0
```

4.3.26 *Device OEM CA [F] (signed by vehicle OEM CA #3)*

```
308201B83082015DA003020102020876 8A24C9666DEBC2300A06082A8648CE3D040302302331
21301F06035504031318544553542D56454849434C452D524F4F542D43412D332D453020170D
323030313031303030303030305A180F323035303031303130303030305A301E311C301A0603
55040313135 44455354 2D4445564943452D524F4F542D4341305930130 6072A8648CE3D020106
082A8648CE3D030107034200048 7FCFA316608A03209DE09A0279E2CAC06BAC27037491E9CC0
807DF523F3628ADCE8C8248808DD03C967904FFF7B9D1EC5BF0C74F7EB2C27F952DD1F46AC5D
38A37E307C3016060A2B0601040182C46905020101FF040530030201013 00E0603551D0F0101
FF040403020204301 20603551D130101FF040830060101FF020101301F0603551D2304183016
80140A81A2EAA5A0F3FE1923F06C3DA6976DBB91C481301D0603551D0E04160414276662923C
2331A74393AF4AEDC035F44E41C950300A06082A8648CE3D040302034900304602210084 2E1D
3D58B7E6E284A0CF708FC25E452279879C381A6E9E247BB86B38982D11022100BF9C7F383702
95034BB255825CA660B29A0C62D65FD2D0787A175F23DD852525
```

4.3.27 *Friend's Device OEM CA [F] (signed by vehicle OEM CA #3)*

```
308201BF30820164A003020102020835133037EFB5B141300A06082A8648CE3D040302302331
21301F06035504031318544553542D56454849434C452D524F4F542D43412D332D453020170D
323030313031303030303030305A180F323035303031303130303030305A3025312330210603
550403131A544553542D465249454E442D4445564943452D524F4F542D4341305930130 6072A
8648CE3D020106082A8648CE3D03010703420004A87028532805919FAD3F3818C6BCCA228BC3
14A5066F54A2F3D8DA1B31596A988D44B15C27A7561F1AAEE608E2D35AAA91B40C38FD083673
2636C8C40216B398A37E307C3016060A2B0601040182C46905020101FF040530030201013 00E
0603551D0F0101FF040403020204301 20603551D130101FF040830060101FF020101301F0603
551D230418301680140A81A2EAA5A0F3FE1923F06C3DA6976DBB91C481301D0603551D0E0416
04142C751100BF23DCAFEEA4503F8B961EFF36967C32300A06082A8648CE3D040302034900 30
46022100DF4A44775C9954E4AB48BDAA5A0EA2D1565630131AEC310B814A99B2BD4DD65F0221
00E17CEBC35B138D81CADE11BC0776EF455EADD78444FAED37D5B24EE9FDCB1CF5
```

4.3.28 *Vehicle OEM CA #3 [J] (self-signed)*

```
308201A63082014DA00302010202080D1EF51FB0021A97300A06082A8648CE3D040302302331
21301F06035504031318544553542D56454849434C452D524F4F542D43412D332D453020170D
323030313031303030303030305A180F323036303031303130303030305A30233121301F0603
55040313185 44455354 2D5645484943 4C452D524F4F542D43412D332D453059301306072A8648
CE3D020106082A8648CE3D030107034200041811CB872C282770BF95954AE2B4277A2109C7B9
31C6DFBFDA2A845070F6C1072BCB1866F4C56F207CFC0B2632ABC4AE4247A8F11753CF8279AD
64ED421CA3FFA3693067300E0603551D0F0101FF040403020204301 20603551D130101FF0408
30060101FF020101302206 03551D230101FF0418301680140A81A2EAA5A0F3FE1923F06C3DA6
976DBB91C481301D0603551D0E041604140A81A2EAA5A0F3FE1923F06C3DA6976DBB91C48130
0A06082A8648CE3D040302034700304402204 7B63A8C9161EBF3E26124391CFD24DBDEAF2B31
69367D87143907DA6307C46A022000896724395AFFAD55DDDE3BE765E3B48D68815948295BA0
4C0BC78B25AF6386
```

4.3.29 *Vehicle OEM CA #3 [M] (signed by device OEM CA)*

```
308201A130820148A003020102020879FFF7757080D85F300A06082A8648CE3D040302301E31
1C301A06035504031313544553542D4445564943452D524F4F542D43413020170D3230303130
313030303030305A180F323036303031303130303030305A30233121301F06035504031318
544553542D56454849434C452D524F4F542D43412D332D453059301306072A8648CE3D020106
082A8648CE3D03010703420004181 1CB872C282770BF95954AE2B4277A2109C7B931C6DFBFDA
2A845070F6C1072BCB1866F4C56F207CFC0B2632ABC4AE4247A8F11753CF8279AD64ED421CA3
FFA3693067300E0603551D0F0101FF040403020204301206035 51D130101FF040830060101FF
020101302206035 51D230101FF041830168014276662923C2331A74393AF4AEDC035F44E41C9
50301D0603551D0E041604140A81A2EAA5A0F3FE1923F06C3DA6976DBB91C481300A06082A86
48CE3D040302034700304402200 8B3B1DCF854A2D4E33AE8A6500CB7DCF229C0D646C777D6EE
E150141A5520360220248172C95161B3C2A2E87370C9AD40AAF21D15BFF51AA76E69292DD01F
F6B5E4
```

4.3.30 *Vehicle OEM Intermediate CA (signed by vehicle OEM CA #3)*

```
308201B63082015DA00302010202081BB8396BD5D82F6B300A06082A8648CE3D040302302331
21301F06035504031318544553542D56454849434C452D524F4F542D43412D332D453020170D
323030313031303030303030305A180F323036303031303130303030305A30333131302F0603
550403132854455354 2D56454849434C452D524F4F542D43412D494E5445524D454449415445
2D332D57572D453059301306072A8648CE3D020106082A8648CE3D03010703420004750A710B
0A83691EC0807BBDE46DEEDF7209EEC48E646A389B21D696790E51E7A4078A8492B5DAC872B9
7882B1AB1EA7D5D1192A0DE4BCEB83B3B8325BAB39BBA3693067300E0603551D0F0101FF0404
030202043012060 3551D130101FF040830060101FF020101302206035 51D230101FF04183016
80140A81A2EAA5A0F3FE1923F06C3DA6976DBB91C481301D0603551D0E041604149665CCFA88
EEA4B3BCB9B1DCFA61F438BA39395B300A06082A8648CE3D040302034700304402204BEA68DE
516E52256E47D26A69F4B4E501746B67BFDE20227D60A5442286072402207070ABC6D34F733D
F14512C47B080D012F499BDDE8C849E29684C75ECAFA0B13
```

4.3.31 *Friend's Instance CA #3 [E] (signed by friend's device OEM CA)*

```
308201BA30820160A003020102020825C14D04DAB0D3E0300A06082A8648CE3D040302302531
233021060355040313 1A544553542D465249454E442D4445564943452D524F4F542D4341301E
170D323030313031303030303030305A170D343030313031303030303030305A300F310D300B0603
550403130454535433305 9301306072A8648CE3D020106082A8648CE3D030107034200040BDE
C80365AFB2C88028A23B2793BB013C9A4B6518F43CE38427437A1647307115314B4A3A8FE00E
318CE19EBB012AF94DEC56E781500A1E13F31D5BFE627E75A3818F30818C3026060A2B060104
0182C46905030101FF041530130201010404000000010408706C6174666F726D300E0603551D
0F0101FF040403020204301206035 51D130101FF040830060101FF020100301F0603551D2304
18301680142C751100BF23DCAFEEA4503F8B961EFF36967C32301D0603551D0E041604142C19
DC7AE2968A4F27CC3AAD6BC1EC89987A414B300A06082A8648CE3D040302034800304502207 5
4ECC565A7B4A066D20850E39EB56858A1959AB1030936EAC2BD584FA69D4300221009C4D638B
41A5E3BD0C433BE3C19ABD4527F074E7B376D60BD0C580210B68FFBA
```

4.4 Other Key Values

4.4.1 *Key values and attributes for SCP03 support*

Table 4-1 defines the key values and attributes to implement SCP03 between the Digital Key framework and the Digital Key applet if required by the Digital Key applet implementation as specified by vendor in ICS [4].

Table 4-1 SCP03 key attributes and values

	Value
Key version number	0x3E
Key-ENC	404142434445464748494A4B4C4D4E4F
Key-MAC	404142434445464748494A4B4C4D4E4F

4.4.2 *Key values and attributes for SCP11a support*

Table 4-2 defines the key values, key attributes and certificates to implement SCP11a between the Digital Key framework and the Digital Key applet if required by the Digital Key Applet implementation as specified by vendor in ICS [4].

Table 4-2 SCP11a key attributes, key values and certificates

	Value
ECC Curve type	
ECC curve	P-256
CA-KLOC	
CA-KLOC Identifier	CA-KLOC-01
CA-KLCC	
CA-KLCC Identifier	CA-KLCC-01
Optional Static Key-DEK	
Key-DEK KVN	0x18
Key-DEK KID	0x12
Key-DEK	404142434445464748494A4B4C4D4E4F
SD.ECKA	
SK.SD.ECKA KVN	0x18
SK.SD.ECKA KID	0x11
PK.SD.ECKA	4BBBE05CD13A9B75B5845EB69F26EED6931ED040D1E4A7C02942C0C49007A44C258DA531BEB576DCF03A564802A58889D85221D0271CBF1F15005B14EA60E532
SK.SD.ECKA	4DC3C1A1C5105ED862EE6558488FB403D7C4D6E77300AA19315FBD1F065BA2E4

	Value
CERT.SD.ECKA	7F2181D2930F73657269616c2d3030303031313131420A43412d4b4c43432d30315F200B73642d6f776e65722d3031950200805F2504202001015F2404202912314507736 42d303030317F4946B041044BBBE05CD13A9B75B5845EB69F26EED6931ED040D1E4A7C02942C0C49007A44C258DA531BEB576DCF03A564802A58889D85221D0271CBF1F15005B14EA60E532F001005F37405DD36F41E05F94E8270D0959834A2BB00DF2A1D90ADF6CFFCD2017189725C5C26B6FBF6BFAD162B92C493123F4C198D9BF449E6E9EB78503B8A5F8DFA38ECC00
CERT.SD.ECKA (detailed/commented)	7F21 81D2 93 0F 73657269616c2d3030303031313131 // serial-00001111 42 0A 43412d4b4c43432d3031 // CA-KLCC-01 5F20 0B 73642d6f776e65722d3031 // sd-owner-01 95 02 0080 // ECKA 5F25 04 20200101 5F24 04 20291231 45 07 73642d30303031 // sd-0001 7F49 46 B0 41 04 4BBBE05CD13A9B75B5845EB69F26EED6931ED040D1E4A7C02942C0C49007A44C258DA531BEB576DCF03A564802A58889D85221D0271CBF1F15005B14EA60E532 F0 01 00 // NIST P-256 5F37 40 5DD36F41E05F94E8270D0959834A2BB00DF2A1D90ADF6CFFCD2017189725C5C26B6FBF6BFAD162B92C493123F4C198D9BF449E6E9EB78503B8A5F8DFA38ECC00 //signature
CA-KLOC.ECDSA	
PK.CA-KLOC.ECDSA KVN	0x18
PK.CA-KLOC.ECDSA KID	0x10
PK.CA-KLOC.ECDSA	0471B00F2B9A5743E6BC404C671F68BD59BD561C867E3E33347B439D58AFD443C77D1AE6EB25628A6E40D9E19A5BB6D57BB3FE0D1FF4341A39D377E16FE689FF48
SK.CA-KLOC.ECDSA	00BD73501BD524A6492AD333D35D163A94FD49ECD813AA357435A1F01BDDBAA0
CA-KLCC.ECDSA	
PK.CA-KLCC.ECDSA	044D01D447C865D0362B430EE0F40B243CC1BAFFA74A932AC29092728BB32E11F7E757C865FE6884FA723686399550F30B7C358EA7AA8255B6F172921CCAF63D5B
SK.CA-KLCC.ECDSA	4100CF830A18724711E599997F42DE364E2947CDB828C7D37EFB7D13D0F26430

	Value
OCE.ECKA	
PK.OCE.ECKA	04BD042A16311661DDB5C6661CE3023210653F693B3496FBA399744692C02AAE2025586C17FBB570B1B0519D4D6B022B2744A2F5E357B2121E054452E9050359D2
SK.OCE.ECKA	4D3CFBF9C2F8B784B392CFEAA986CF25F2F253D67C04FEF4450AADFBD66FEFE6
CERT.OCE.ECKA	7F2181CA930F73657269616c2d3030303031313131420A43412d4b4c4f432d30315F200C6f63652d6f776e65722d3031950200805F2504202001015F2404202912317F4946B04104BD042A16311661DDB5C6661CE3023210653F693B3496FBA399744692C02AAE2025586C17FBB570B1B0519D4D6B022B2744A2F5E357B2121E054452E9050359D2F001005F37409230727B7CD53B861990A08BB382E4DCFC6F502F99C82EF470F5B41FF8D537B899AAE7109EE965405C6B7C5414171176F33811E22B0B73F81BDF08BD6D0FDFC8
CERT.OCE.ECKA (detailed/commented)	7F21 81CA 93 0F 73657269616c2d3030303031313131 // serial-00001111 42 0A 43412d4b4c4f432d3031 // CA-KLOC-01 5F20 0C 6f63652d6f776e65722d3031 // oce-owner-01 95 02 0080 // ECKA 5F25 04 20200101 5F24 04 20291231 7F49 46 B0 41 04 BD042A16311661DDB5C6661CE3023210653F693B3496FBA399744692C02AAE2025586C17FBB570B1B0519D4D6B022B2744A2F5E357B2121E054452E9050359D2 F0 01 00 // NIST P-256 5F37 40 9230727B7CD53B861990A08BB382E4DCFC6F502F99C82EF470F5B41FF8D537B899AAE7109EE965405C6B7C5414171176F33811E22B0B73F81BDF08BD6D0FDFC8 //signature

5 TEST CASES

The test cases to be executed for CCC Digital Key applet certification are listed in document CCC Digital Key Applet Compliance Test Suite [3].

NOTE: Full compliance with the listed test cases does not guarantee an absence of code errors and vendors are therefore advised to implement and execute additional test cases that may be particularly relevant for their applications.

5.1 Known Issues

5.1.1 *Proprietary Type Selector Command*

To explicitly select the NFC Type A protocol or the NFC Type B protocol and execute the NFC Type A and NFC Type B specific test cases, the Secure Element IP Connector client of the GlobalPlatform Abstract Communication Layer has to use NFC reader commands that are specific to the reader being used. The Secure Element IP Connector client provided by GlobalPlatform is known to work with a limited number of NFC readers.

NOTE: This Secure Element IP Connector client is available from the GlobalPlatform GIT Hub from https://github.com/GlobalPlatform/SE_Abstract_Communication_Layer_Over_TCP_IP/tree/RF-Management/client.

The following NFC readers are known to work:

- Identiv uTrust 3700 F
- Identiv uTrust 4701 F

The SE vendor is responsible for using an NFC reader, which can successfully pass the respective test cases. The full list of impacted test cases is given below:

- AUTH0.001.gc.check.standard.transaction.nfc.type.a (01-a0-c1)
- AUTH0.001.gc.check.standard.transaction.nfc.type.b (01-a0-d1)
- AUTH0.002.gc.check.fast.transaction.nfc.type.a (01-a0-c2)
- AUTH0.002.gc.check.fast.transaction.nfc.type.b (01-a0-d2)
- AUTH1.012.gc.check.auth1.response.nfc.type.a (01-a1-z2)
- AUTH1.012.gc.check.auth1.response.nfc.type.b (01-a1-y2)
- CONTROL_FLOW.002.gc.transaction.finished.success.nfc.type.a (01-cf-c2)
- CONTROL_FLOW.002.gc.transaction.finished.success.nfc.type.b (01-cf-d2)
- EXCHANGE.004.gc.command.verify.decrypted.data.nfc.type.a (01-ex-c4)
- EXCHANGE.004.gc.command.verify.decrypted.data.nfc.type.b (01-ex-d4)
- PRESENCE0.001.gc.verify.response.nfc.type.a (01-p0-a1)
- PRESENCE0.001.gc.verify.response.nfc.type.b (01-p0-b1)
- PRESENCE1.001.gc.verify.response.nfc.type.a (01-p1-a1)
- PRESENCE1.001.gc.verify.response.nfc.type.b (01-p1-b1)

A waiver is not accepted for this issue.

5.2 Test Suite Structure

The certification test cases are grouped in the Test Suite [3] according to Table 5-1. The order is identical to the section order in the Test Suite [3].

NOTE: The management of the Instance CAs with the CREATE CA command and the DELETE CA command are out of scope of the test plan.

If the SE vendor indicates support of the Option A in the ICS and IXIT [6], the test tool will use the indicated Secure Channel Protocol (i.e. SCP03, SCP11a) with the given Digital Key applet Minimum Security Level to execute all the APDU commands originated from the Digital Key framework defined in Section 15.3.1.4 of [2] .

When switching from wired interface to the contactless interface and vice versa, the test tool will first deselect the Digital Key applet on the current selected interface.

If the SE vendor indicates support of the Option B in the ICS and IXIT [4], the test tool will issue the APDU command MANAGE CHANNEL with P1P2=’0000’, before selecting the Digital Key applet over the wired interface.

If the DUT supports multiple options, e.g., Option A with SCP03 and SCP11a, then the SE vendor will submit multiple ICS documents, each representing a different configuration. While this will require separate testing for each DUT configuration, these can be handled within the same DK Applet compliance certification.

NOTE: The SELECT, READ BUFFER and WRITE BUFFER commands are implicitly tested by test cases for other commands (i.e., no dedicated test case has been developed).

Table 5-1 Digital Key Applet Compliance Test Case Groups

Group	Description
AUTH0	This command allows the vehicle to initiate the authentication procedure. In case a fast transaction is requested by the vehicle, a cryptogram is returned, allowing the vehicle to tentatively proceed with a fast transaction.
AUTH1	This command allows mutual authentication and establishment of a secure channel between the vehicle and device.
AUTHORIZE ENDPOINT	This command signs an endpoint public key (issued by a receiver device) and an arbitrary additional data field using a local endpoint private key (sender device).
PRESENCE0	This command allows the vehicle to initiate the Check Presence transaction.
PRESENCE1	This command allows an authenticated vehicle to retrieve the endpoint key_slot.
CONTROL FLOW	This command allows the vehicle to indicate the final success or failure of the transaction, or to signal application-specific codes.
CREATE ENCRYPTION KEY	Create a confidential mailbox encryption key attestation in order to allow data insertion in the endpoint.
CREATE ENDPOINT	The command creates a communication endpoint and provides the corresponding endpoint certificate.

Group	Description
DELETE ENDPOINT	This command will delete an endpoint and release the associated memory.
EXCHANGE	This command reads, writes, or sets data from confidential/private mailboxes.
GET NOTIFICATION	This command provides a mean to retrieve notifications to the DK Framework when the commands are processed over the wired interface.
GET PRIVATE DATA	Retrieve data in the private mailbox.
MANAGE UA	This command provides the user authentication status. Implementing this command is optional and the user authentication status may be provided using a proprietary method.
SCP	Additional test cases to validate implementation of the commands over the various security levels of the secure channel protocol supported by the SE.
SETUP ENDPOINT	This command is used to change the default private/confidential mailbox content returned in AUTH1 response; by default, no mailbox content is returned in the AUTH1 response.
SETUP INSTANCE	This command is used to enable/disable endpoint visibility of all endpoints on the contactless interface. If visibility is disabled, the endpoints appear as non-existent on the contactless interface.
SET CONFIDENTIAL DATA	Store data in the confidential mailbox.
SET PRIVATE DATA	Store data in the private mailbox.
SIGN	This command signs an arbitrary data field using the private key of the selected endpoint.
TERMINATE ENDPOINT	This command sets the endpoint in terminated state and returns a termination attestation.
VIEW	This command returns information on endpoints and Instance CAs. The response is written in internal buffer and accessible using READ BUFFER command.

6 REFERENCES

[1] IETF, RFC 2119, “Keys words for use in RFCs to Indicate Requirement Levels”, March 1997. http://www.ietf.org/rfc/rfc2119.txt

[2] Car Connectivity Consortium CCC-TS-101: "CCC Digital Key Specification (Release 3)", Version 1.1.1 or later.

[3] Car Connectivity Consortium CCC-CP-004: "Digital Key Applet Compliance: Test Suite"

[4] Car Connectivity Consortium CCC-CP-005: "Digital Key Applet Compliance: Implementation Conformance Statement (ICS)"

[5] Car Connectivity Consortium CCC-CP-006: "Digital Key Applet Compliance: Implementation Extra Information for Testing (IXIT)"

[6] Car Connectivity Consortium CCC-CP-009: "Digital Key Applet Compliance: ICS and IXIT XML Format"

[7] Car Connectivity Consortium CCC-CP-010: "Digital Key Applet Compliance: ICS XML Example"

[8] Car Connectivity Consortium CCC-CP-011: "Digital Key Applet Compliance: ICS XML Schema (XSD)"

[9] Car Connectivity Consortium CCC-CP-013: "Digital Key Applet Compliance: Test Tool Requirements"

[10] SE_Abstract_Communication_Layer_Over_TCP_IP https://github.com/GlobalPlatform/SE_Abstract_Communication_Layer_Over_TCP_IP