Automotive eSE training in CCC digital key demo
汽车级加密芯片实践培训

Tianyi Zheng

Application Engineer

Oct 2024

Navigation section

Agenda

Introduction of CCC digital key architecture

NXP CCC reference demo system

Start OP or transaction in phone mode

Start OP or transaction in card mode

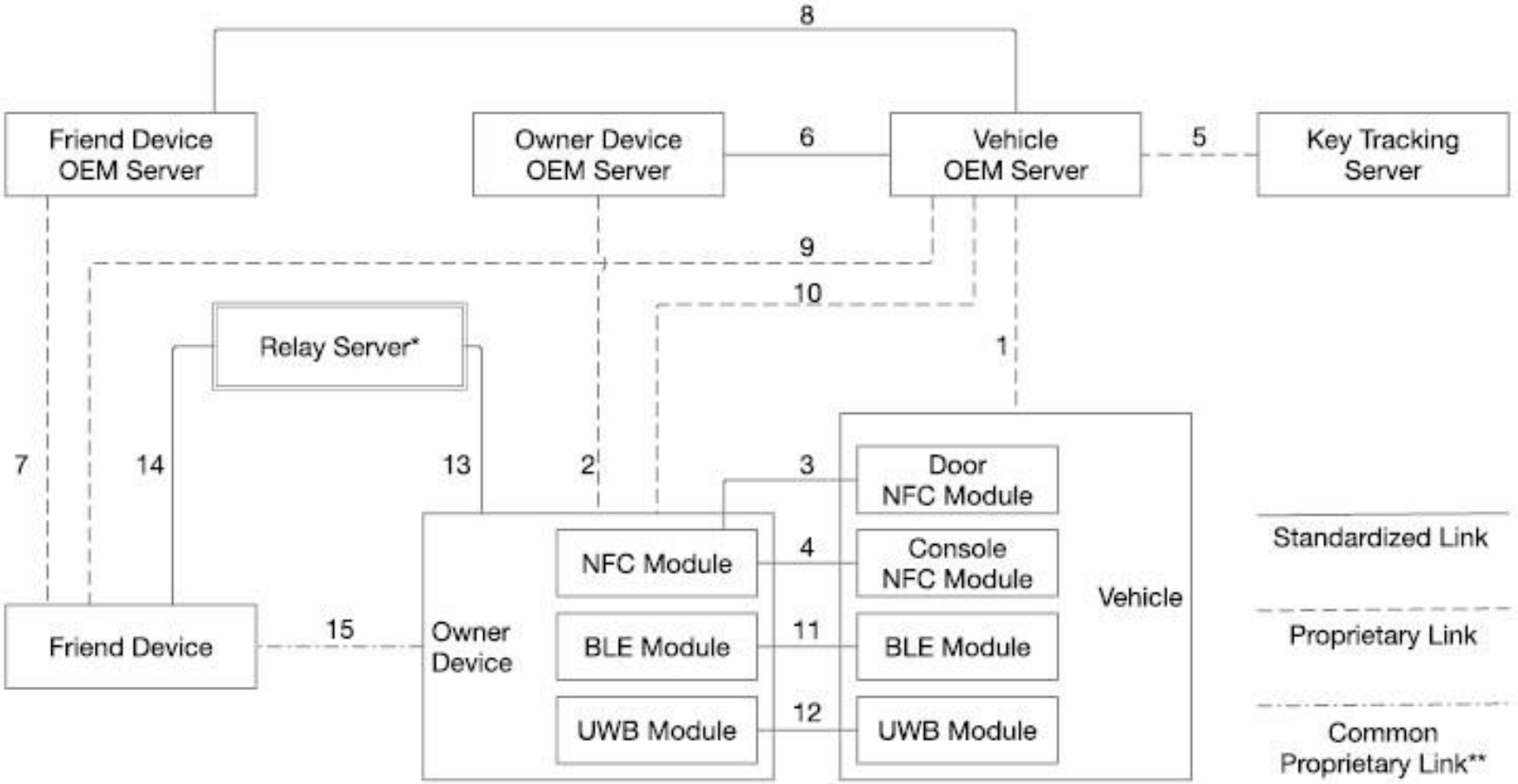
Personalize in NCJ38A0HN

Personalize in key fob

Introduction of CCC digital key architecture

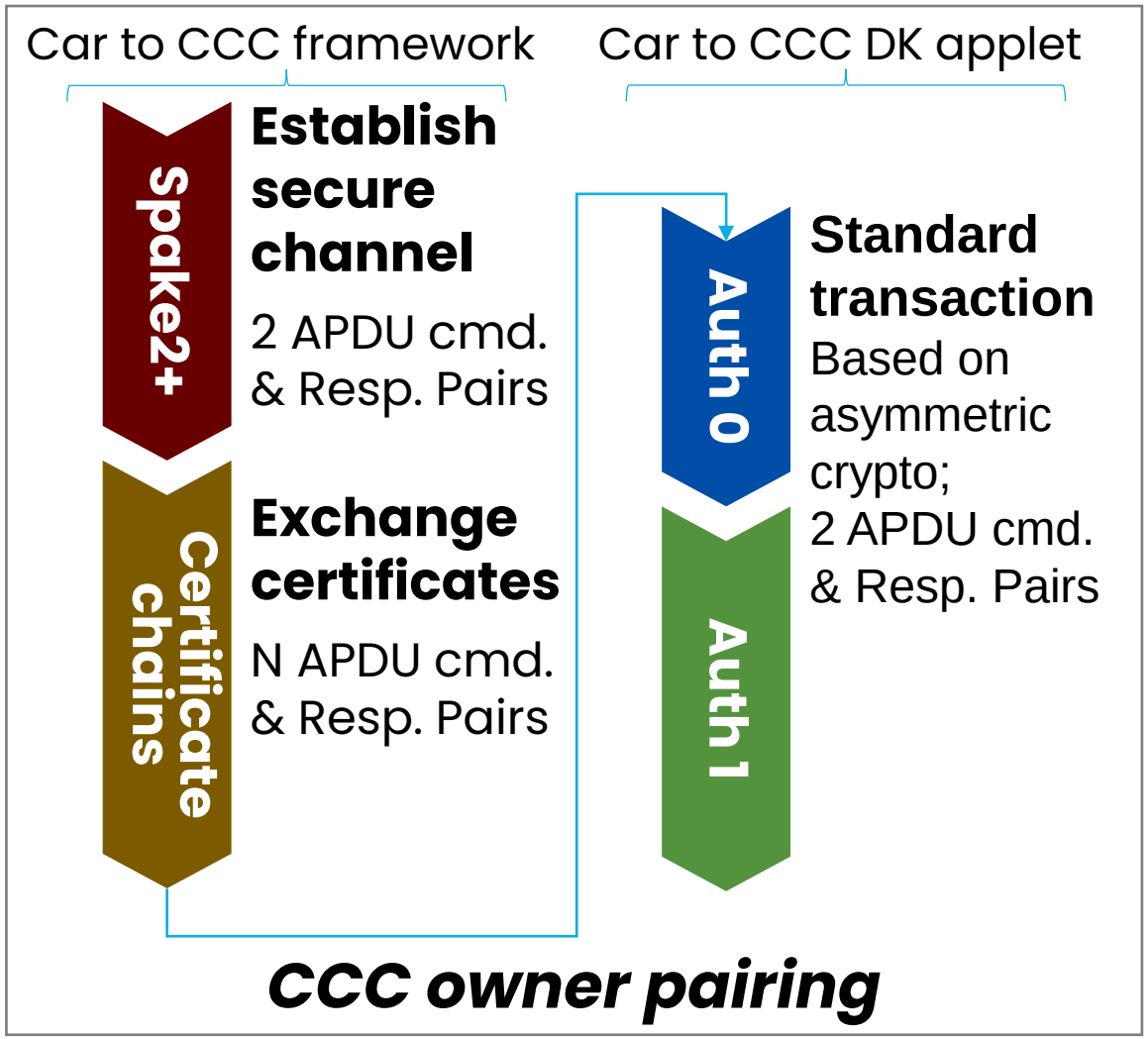
CCC-TS-101-Digital-Key-R3-1.2.2 -> 2.3 High level architecture

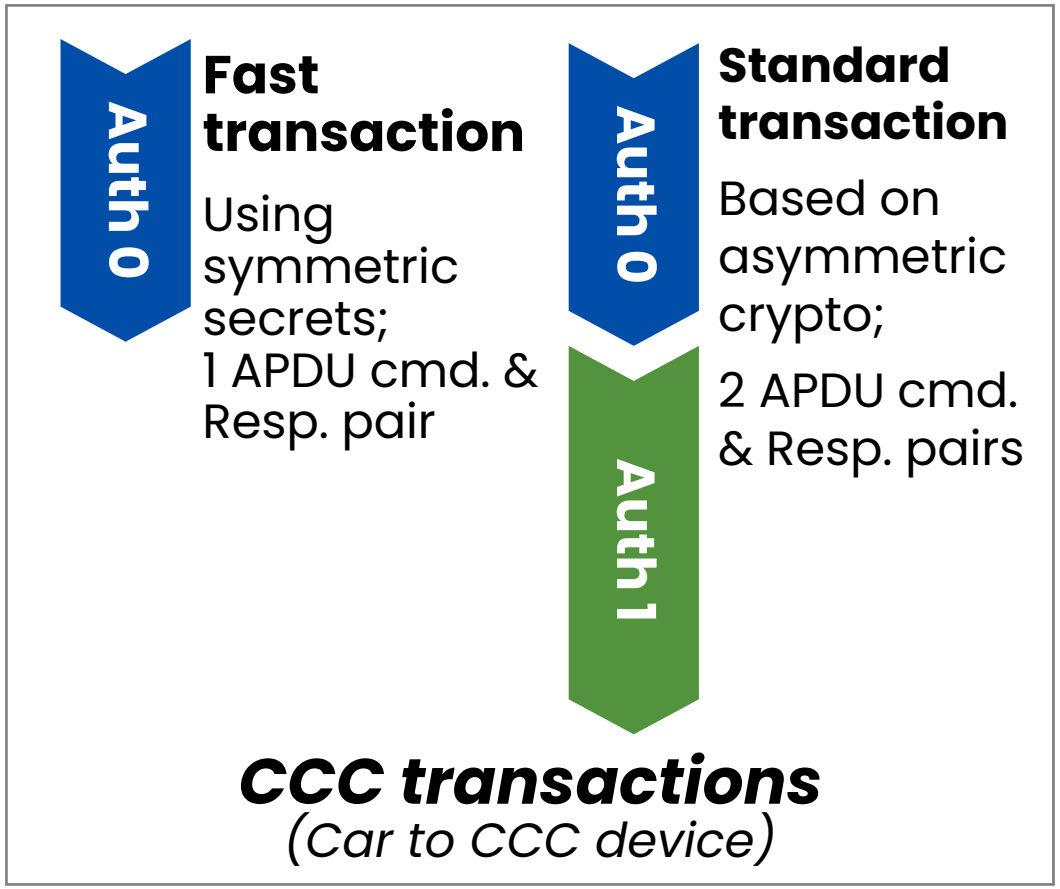
Figure 2-1: Digital Key Architecture with Actors and Their Relationships



* Relay Server Selected by Owner Device OEM to Share keys with Friend Device from a different Device OEM. Relay Server may be implemented by Device OEM, Vehicle OEM or by a Third Party

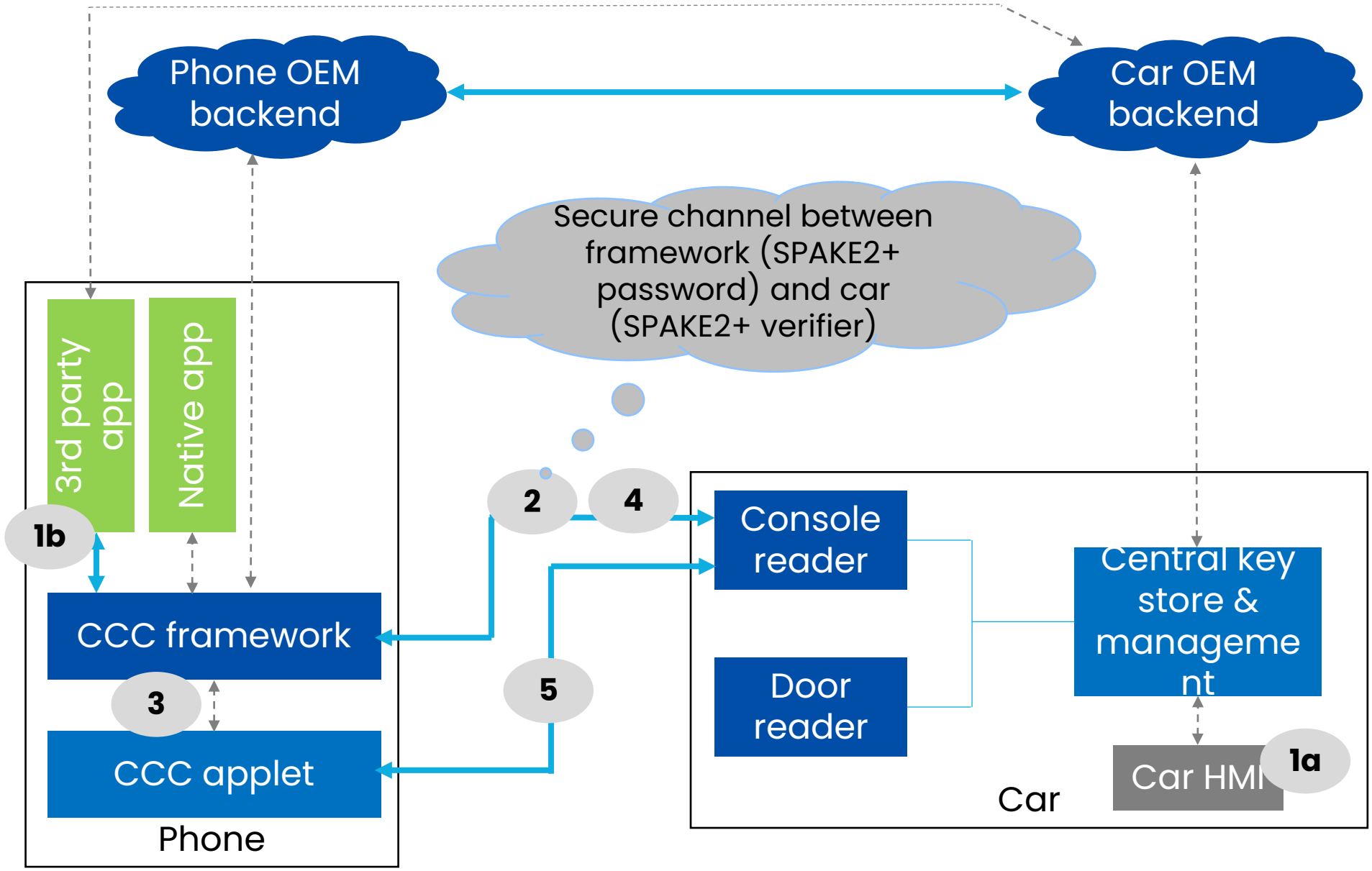
Transactions and owner pairing



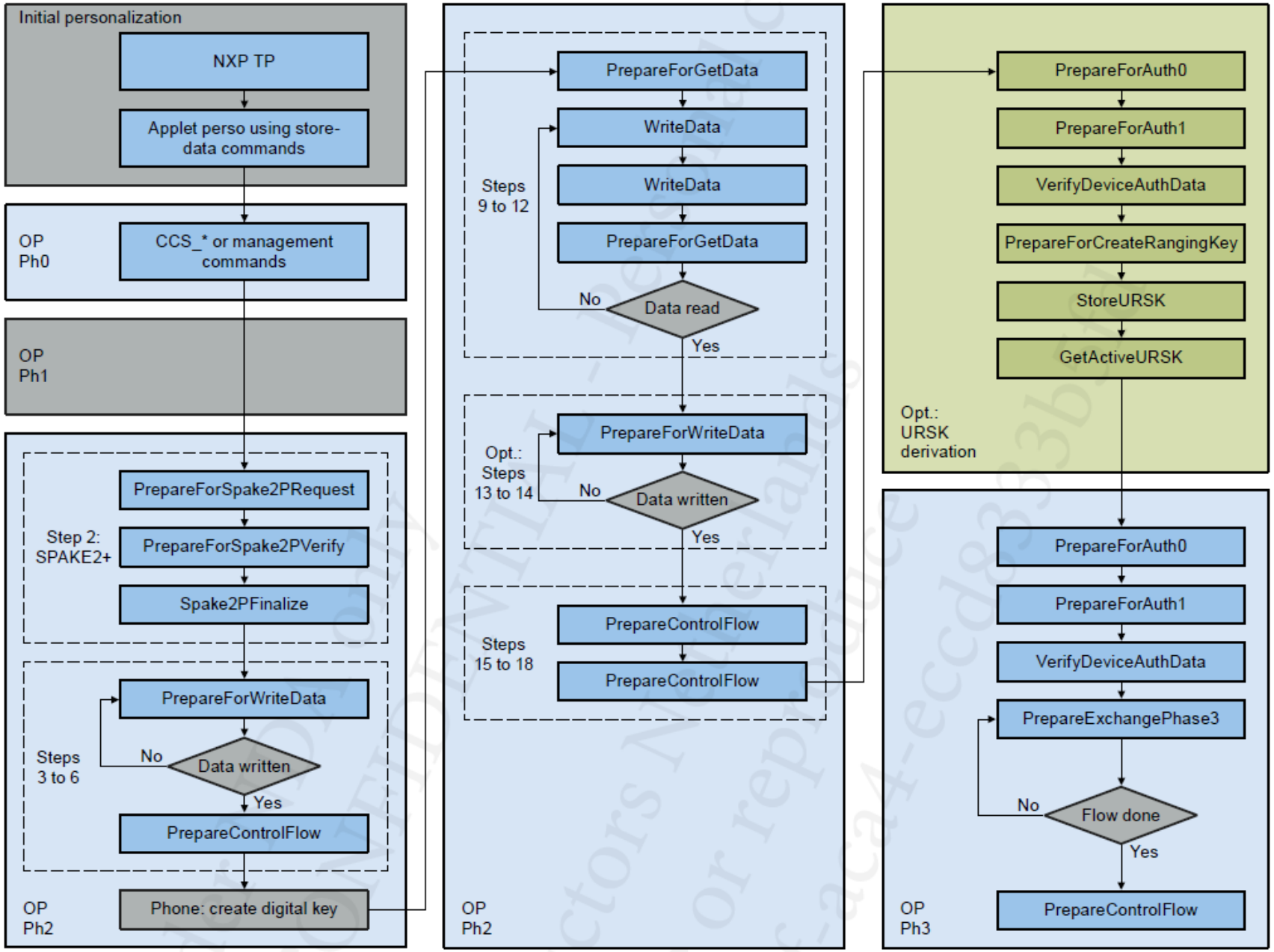


Pairing flow

1) **Initiate pairing**
   a) on car side: start polling for framework
   b) on phone side: framework running HCE, requesting pairing password
2) Use SPAKE2+ to **establish a secure channel**
3) **Creation of new digital key** + attestation
4) Exchange of **certificate (chains) & attestations**
5) **Finalize pairing** using a standard transaction

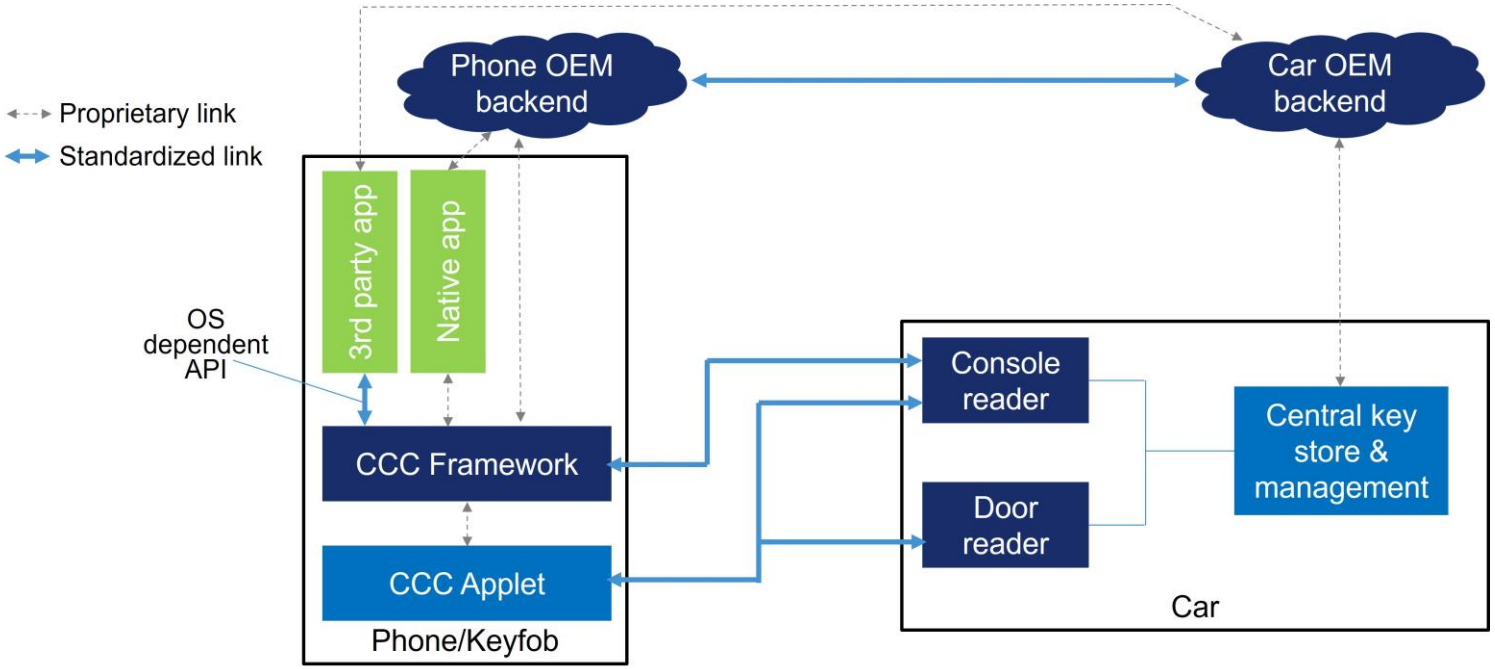


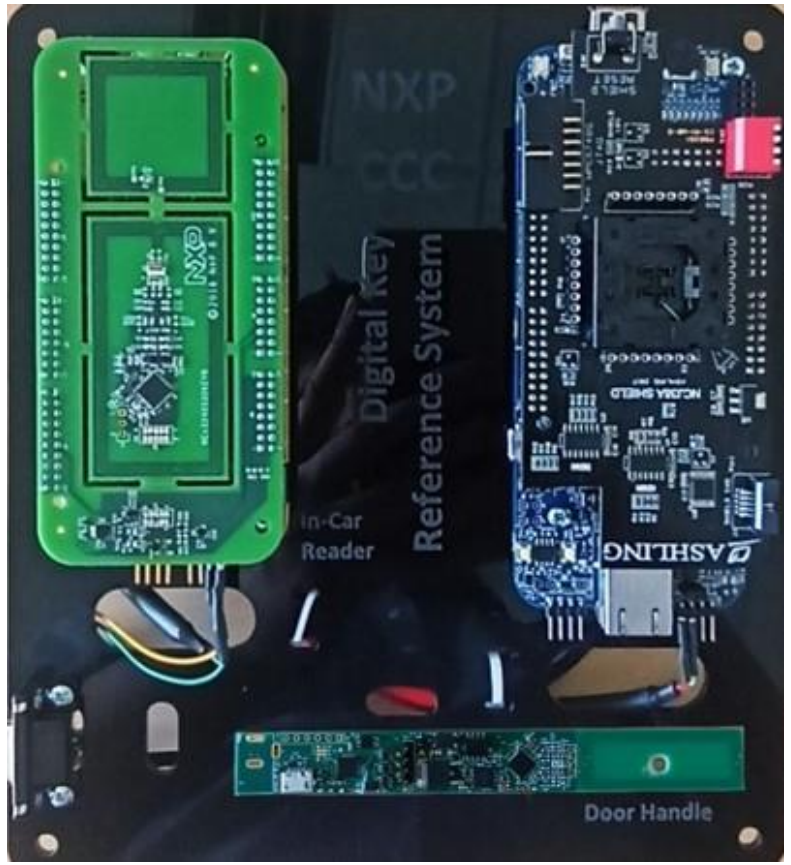
OP car-side applet overview

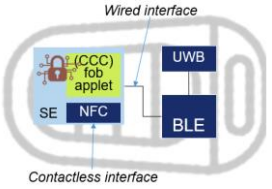


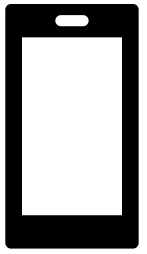
NXP CCC reference demo system

- Full CCC compliant reference system
- Automotive MCU with automotive Secure Element
  - NCJ38A0HN
  - Door handle/In-car NFC reader
- Mobile Phone/Smart keyfob(NCJ37B0HN)





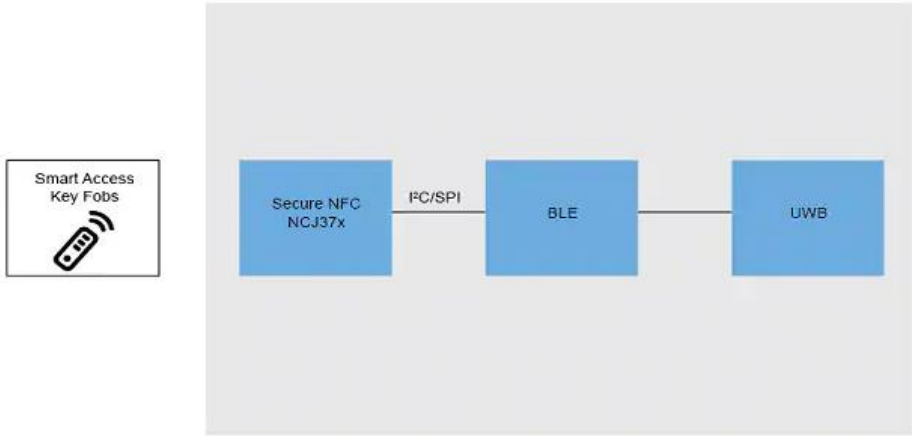




NCJ37B0HN “NESTOR” HARDWARE PLATFORM

ULTRA LOW POWER SECURE ELEMENT WITH NFC (FIELD-POWERED)

	Metric	Value
MCU	Node	40 nm CMOS NV
	Architecture	MRK3-SC 16 bit
	Clock speed	48 MHz
Memory	Flash	Up to 400 kB
	RAM	18.5 kB*
Interfaces	Supported interfaces	SPI, I2C, ISO/IEC 14443 NFC
Physical	Supply voltage	1.8 – 3.3 V
	Temperature range	-40°C to 105°C
	AEC-Q100 grade	Grade 2
	Package	4x4 mm HVQFN20
Software & security	Operating System	JCOP 4.x
	Security certification	CC EAL 6+



Target Applications

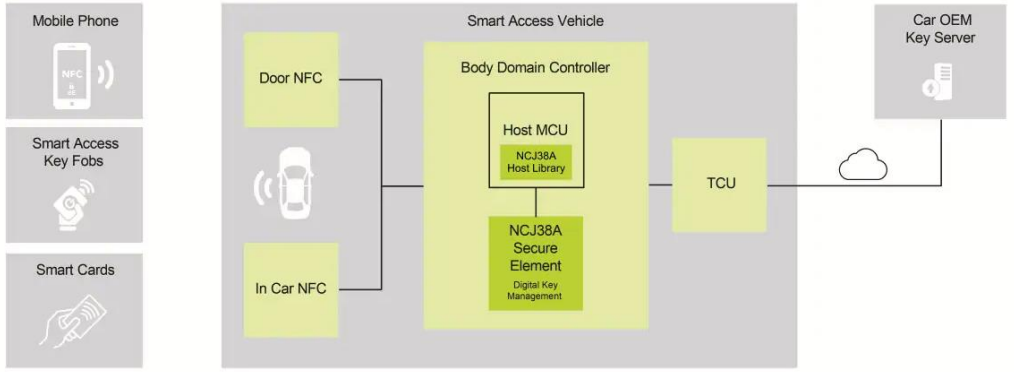
- Smart Key Fob
- Qi 1.3 Authentication
- Secure BMS and Battery Passport
- Plug & Charge (ISO15118-20)

* Available RAM memory for JCOP applet development is less and depending on OS configuration.

NCJ38A0HN “PHANTOM” HARDWARE PLATFORM

HIGH PERFORMANCE AUTOMOTIVE SECURITY CONTROLLER

	Metric	Value
MCU	Node	40 nm CMOS NV
	Architecture	ARM SC300 32 bit
	Clock speed	96 MHz
Memory	Flash	Up to 750 kB
	RAM	52 kB*
Interfaces	Supported interfaces	SPI and I2C
Physical	Supply voltage	1.8 V
	Temperature range	-40°C to 105°C
	AEC-Q100 grade	Grade 2
	Package	5x5 mm HVQFN32
Software & security	Operating System	JCOP 4.4
	Security certification	CC EAL 5+



Target Applications

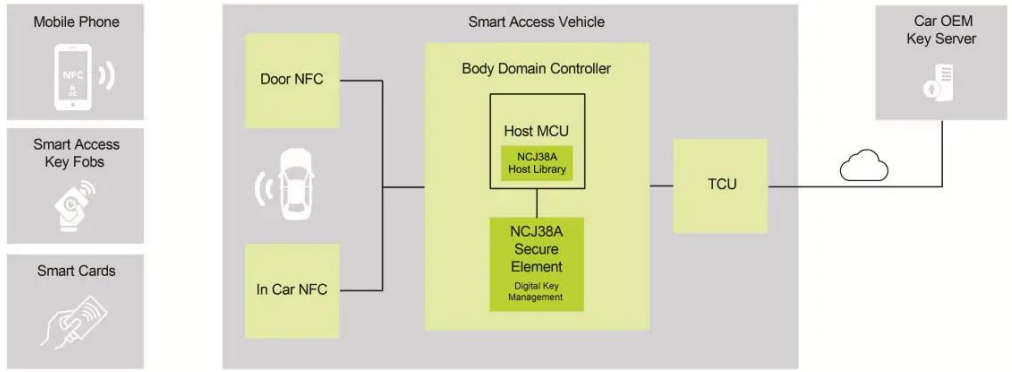
- CCC Digital Key Management
- Infotainment & connectivity
- Secure BMS and Battery Passport
- EV Charging authentication (e.g. Plug & Charge)

* Available RAM memory for JCOP applet development is less and depending on OS configuration.

NCJ39A0HF “PHANTOM PRO” HARDWARE PLATFORM

NEXT-GEN HIGH PERFORMANCE AUTOMOTIVE SECURITY CONTROLLER

	Metric	Target Value
MCU	Node	28 nm CMOS NV
	Architecture	Cortex M33 32 bit
	Clock speed	240 MHz
Memory	Flash	Up to 750 kB
	RAM	96 kB*
Interfaces	Supported interfaces	SPI and I2C
Physical	Supply voltage	3.3 V
	Temperature range	-40°C to 105°C
	AEC-Q100 grade	Grade 2
	Package	5x5 mm HVQFN32
Software & security	Operating System	JCOP 8.x**
	Security certification	CC EAL 5+



Target Applications

- CCC Digital Key Management
- Infotainment & connectivity
- Secure BMS and Battery Passport
- EV Charging authentication (e.g. Plug & Charge)

*Available RAM memory for JCOP applet development is less and depending on OS configuration.
**Exact JCOP release t.b.d.

NXP CCC reference demo - NXP CCC applet offering

NXP is developing CCC applets for the car, phone as well as key fob and smartcard.

→ Ensure interoperability already on applet level!

Car-side applet features

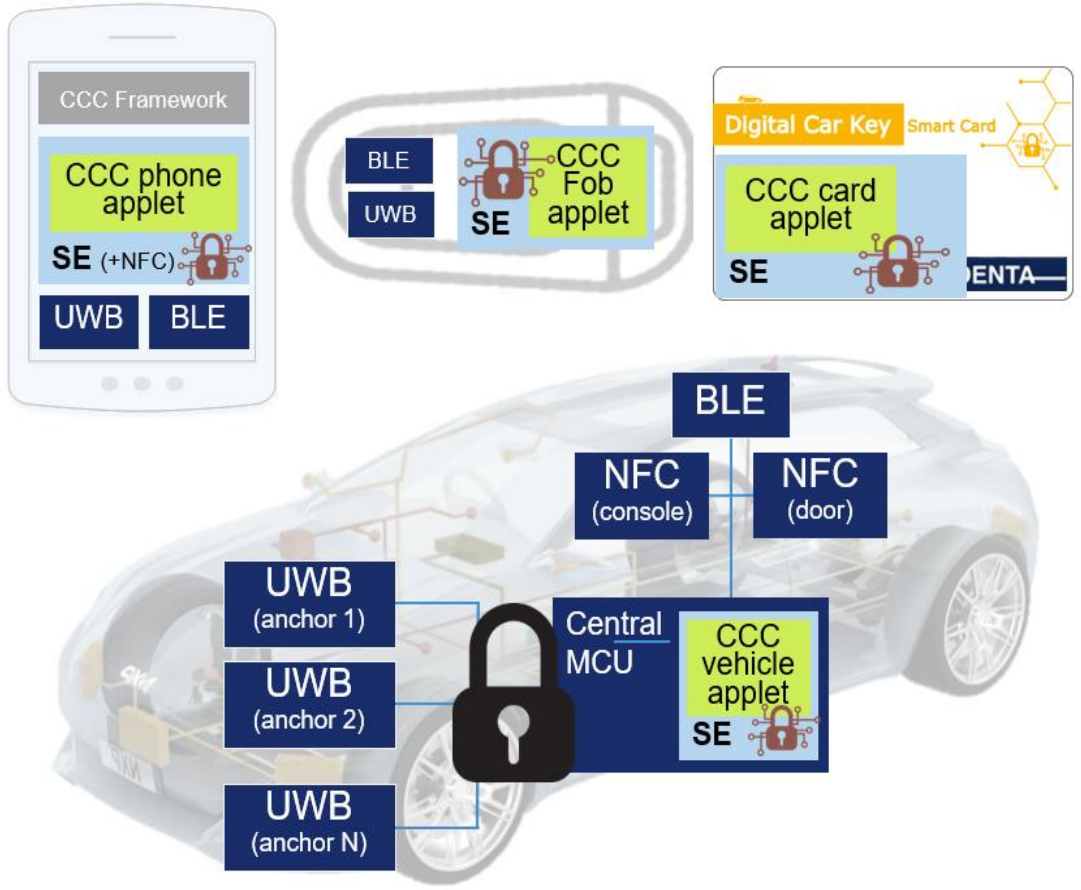
- Full support of CCC functionality (rel2 and rel3)
- Support for remote DK management
- Configurable security features
- Binding of SE and UWB

Mobile-side applet

- Full support of CCC functionality (rel2 and rel3)
  - Including standard transaction, fast transaction and friend sharing
- Fully compatible with CCC standardized DK framework

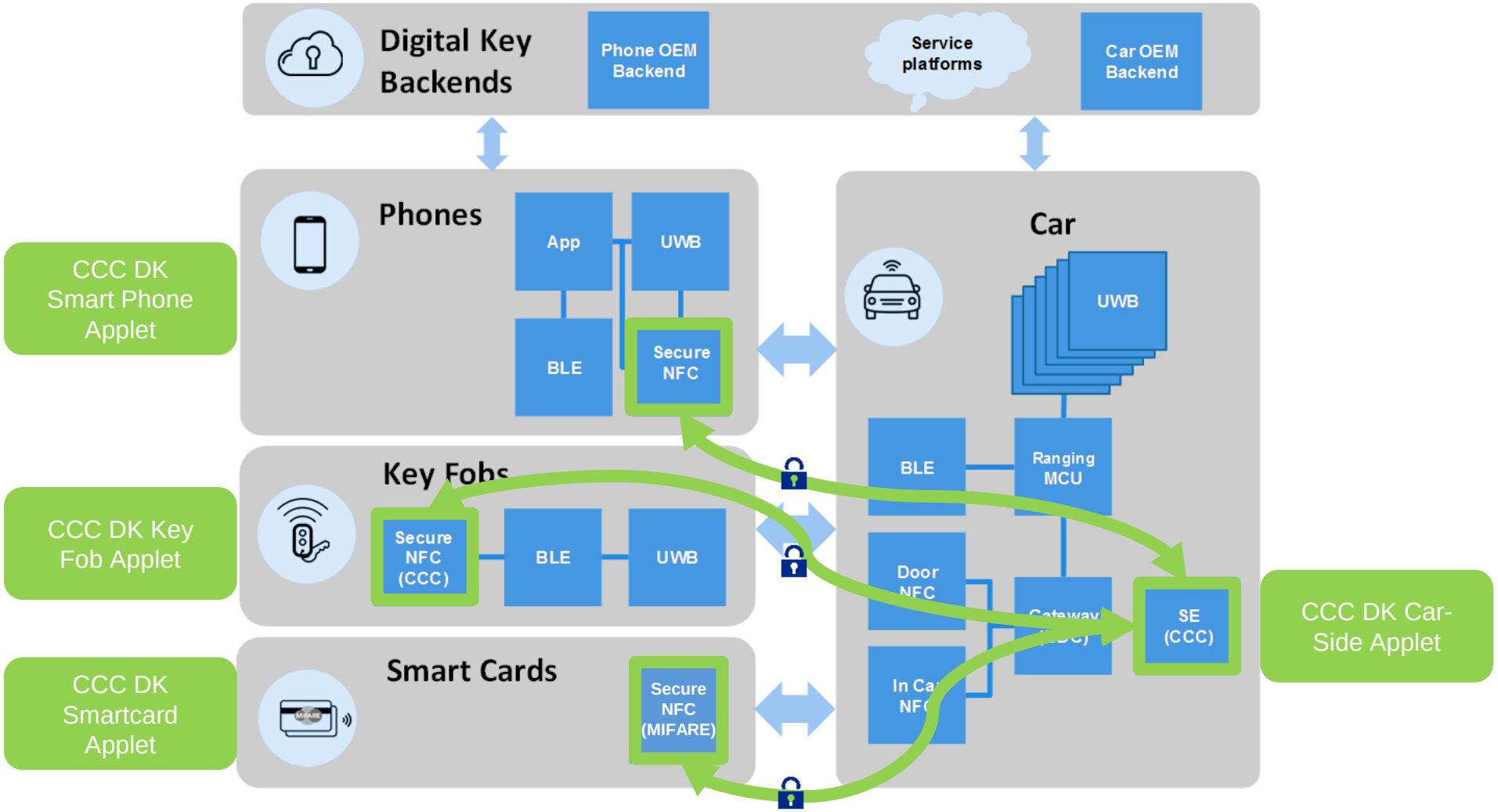
Key fob/card applet

- Full support of CCC functionality (rel2 and rel3)
  - Including owner pairing, standard transaction, fast transaction



SMART CAR ACCESS SYSTEM WITH SECURE ELEMENTS

NXP SE AND APPLET PORTFOLIO GUARANTEES HIGHEST INTEROPERABILITY BETWEEN CARS AND DEVICES



Start demo

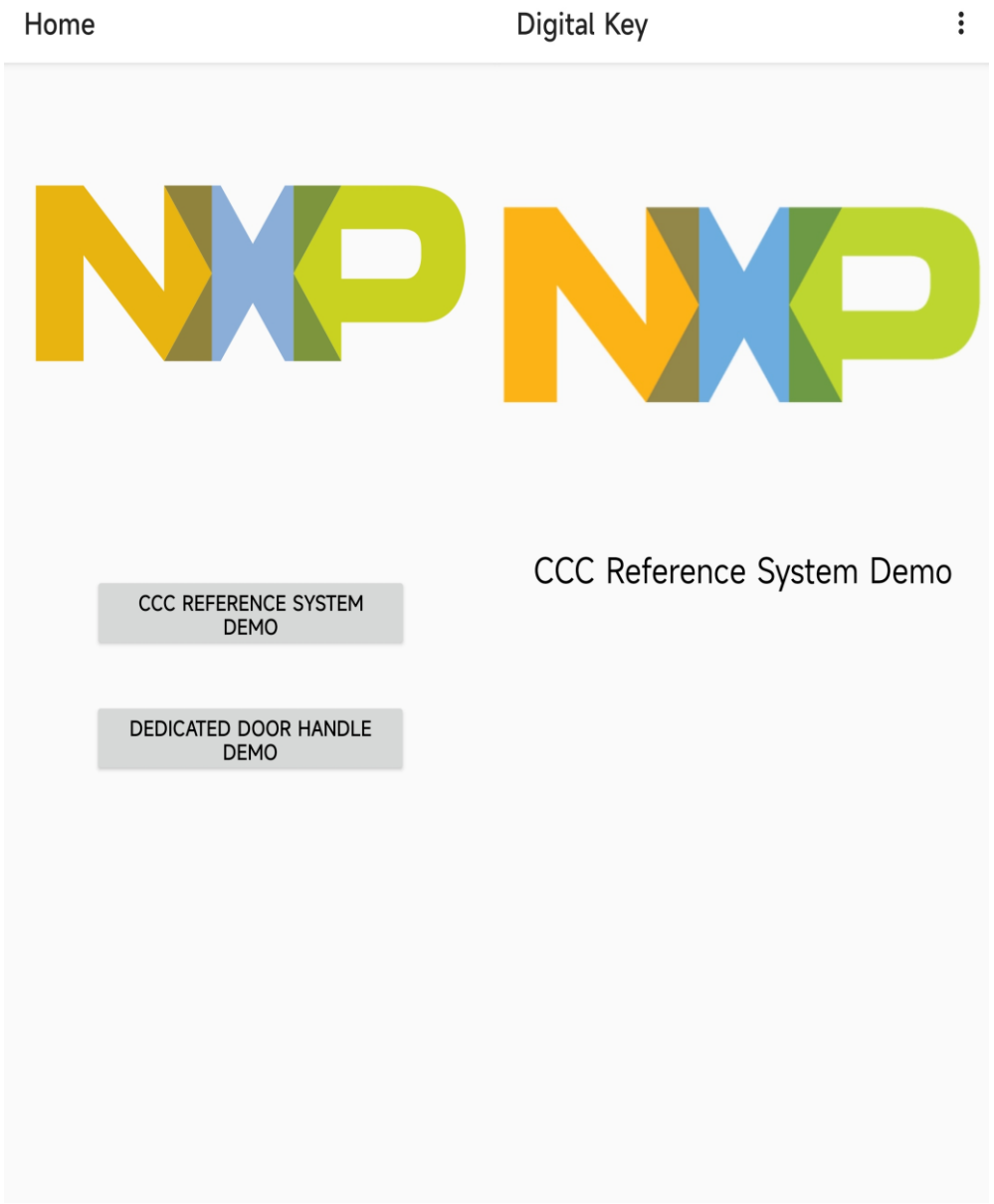
1. Powerup demo
2. Personalize NCJ38A0HN
3. Connect CAN cable
4. Start python tool
5. Prepared for OP&ST

time.py | ConfigSettings.py | builtins.py

```
68
69
    1 usage
70  def config_logger(show_can=True, show_jumbo=False, show_figaro=False):
71      if not show_figaro:
72          ccc.LOGGER.parent.setLevel(ccc.LOGGER.CCC + 1)
73      if not show_jumbo:
74          figaro.LOGGER.parent.setLevel(figaro.LOGGER.FIGARO + 1)
75      if not show_can:
76          jumbo.LOGGER.parent.setLevel(jumbo.LOGGER.JUMBO + 1)
77
78
    2 usages
79  def run_config(bus):
80
81      configHandler = ConfigHandler(bus)
82      configHandler.init_config_session()
83
84
85      configHandler.set_target_ccc_mission(ConfigCccTargetMission.NFC_OWNER_PAIRING)
86      #configHandler.set_target_ccc_mission(ConfigCccTargetMission.CARD_PAIRING)
87      configHandler.set_target_ccc_mission(ConfigCccTargetMission.STANDARD_TRANSACTION)
88      #configHandler.set_target_ccc_mission(ConfigCccTargetMission.CARD_ST_TRANSACTION)
89      #configHandler.view_all_dks()
90      #configHandler.delete_all_dks()
91      configHandler.end_config_session()
92
```

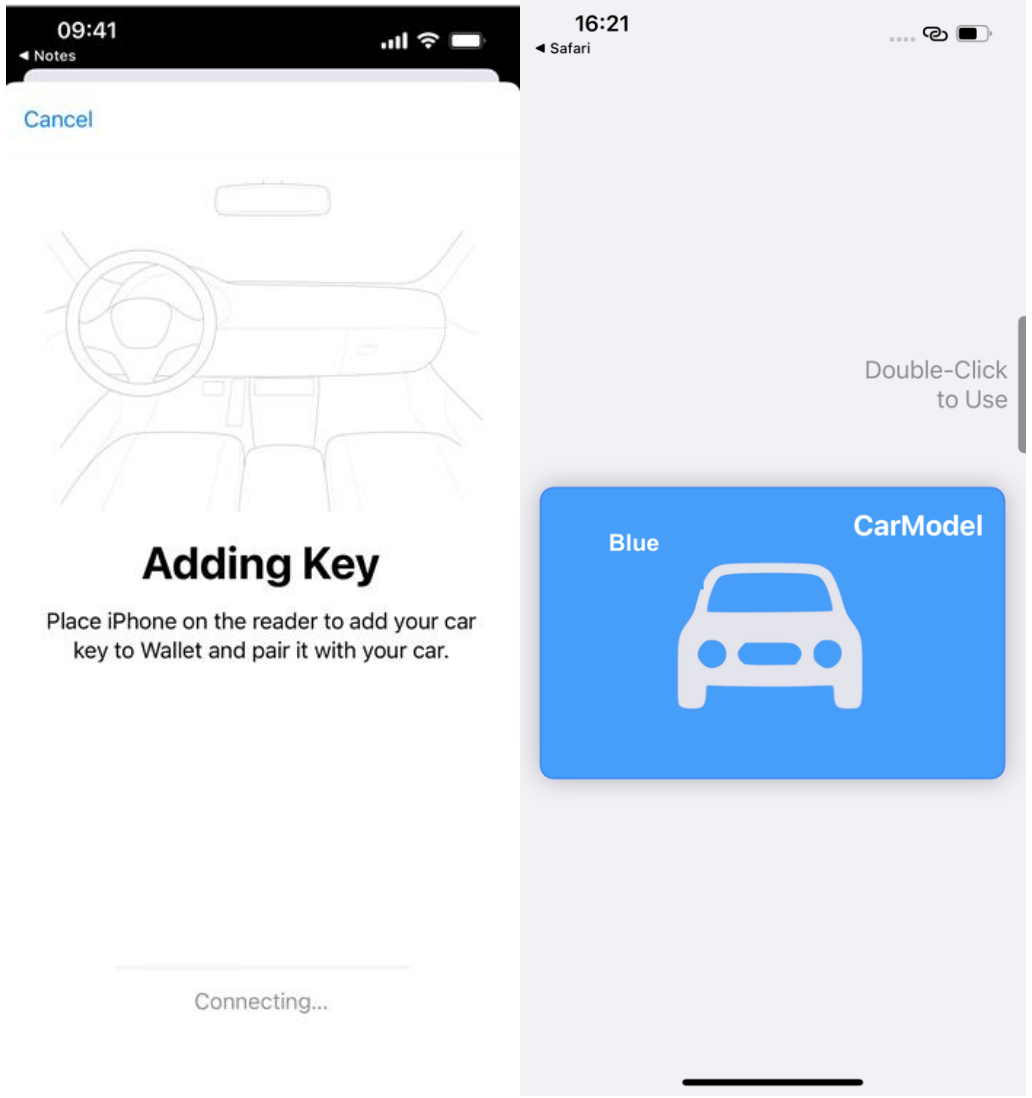
Start OP or transaction with Android phone

- Open phone and keep WIFI online
- Install “nxp_digitalkey.Apk” on android phone
- Open installed cccrefdemo app, you will see the right screenshot
- Tap the phone on the NFC pad then phone owner pairing started, you will see the data log on python tool until OP finished
- If you configure standard transaction in python tool, you will see the transaction data exchange in logs



Start OP or transaction in iPhone

- Open phone and keep WIFI online
- Open wallet, adding key
- Tap the phone on the NFC pad then phone owner pairing started, you will see the data log on python tool
- After owner pairing finished, a blue car key label added in wallet
- If you configure standard transaction in python tool, you will see the transaction data exchange in logs



Phone pairing log

```
"C:\Users\nxp52688\OneDrive - NXP\work\project\zty\CCC\CCC_demo\OneDrive_1_8-3-2022\CAN_Support_Tool\venv\Scripts\python.exe" "C:\Users\nxp52688\OneDrive - NXP\work\project\zty\CCC\CCC_demo\OneDrive_1_8-3-2022\CAN_Support_Tool\main.py"
CCC      | TX |              N/A |    N/A | From PC | CONFIG | Start config command
CCC      | RX | 16:32:17.2016711 |    N/A | From Central Node | CONFIG | Command successful
Thu Jan 25 08:32:17 2024
32303234 31 3235 38 3332 3137
CCC      | TX |              N/A |    N/A | From PC | CONFIG | Target_Mission: NFC_OWNER_PAIRING
CCC      | RX | 16:32:17.2129074 |    N/A | From Central Node | CONFIG | Command successful
Thu Jan 25 08:32:17 2024
32303234 31 3235 38 3332 3137
CCC      | TX |              N/A |    N/A | From PC | CONFIG | Stop config command
CCC      | RX | 16:32:17.2141189 |    N/A | From Central Node | CONFIG | Command successful
CCC      | RX | 16:32:29.2061212 |    N/A | From NFC Reader | Phone/Card detected
CCC      | RX | 16:32:29.2156731 |    N/A | From Central | APDU-Exchange: (SELECT: Target_Aid: CCC Framework AID [A000000809434343444B46763100])
CCC      | RX | 16:32:29.2176731 |    N/A | From NFC Reader | APDU-Exchange: Protocol_Version: [0100];
CCC      | RX | 16:32:29.2242248 |    N/A | From Central | APDU-Exchange: (OP_REQUEST)
CCC      | RX | 16:32:29.2471555 |    N/A | From NFC Reader | APDU-Exchange: RESP
CCC      | RX | 16:32:29.2703855 |    N/A | From Central | APDU-Exchange: (OP_VERIFY)
CCC      | RX | 16:32:29.2730497 |    N/A | From NFC Reader | APDU-Exchange: RESP
CCC      | RX | 16:32:29.2982960 |    N/A | From Central | APDU-Exchange: (WRITE_DATA)
CCC      | RX | 16:32:30.2019108 |    N/A | From NFC Reader | APDU-Exchange: RESP
CCC      | RX | 16:32:30.2577310 |    N/A | From Central | APDU-Exchange: (CONTROL_FLOW)
CCC      | RX | 16:32:30.2597390 |    N/A | From NFC Reader | APDU-Exchange: RESP
CCC      | RX | 16:32:30.2693138 |    N/A | From central | Start Polling
CCC      | RX | 16:32:31.2548341 |    N/A | From NFC Reader | Phone/Card detected
CCC      | RX | 16:32:31.2549323 |    N/A | From Central | APDU-Exchange: (SELECT: Target_Aid: CCC Framework AID [A000000809434343444B46763100])
CCC      | RX | 16:32:31.2569314 |    N/A | From NFC Reader | APDU-Exchange: Protocol_Version: [0100];
CCC      | RX | 16:32:31.2589233 |    N/A | From Central | APDU-Exchange: (GET_DATA)
CCC      | RX | 16:32:31.2636042 |    N/A | From NFC Reader | APDU-Exchange: RESP
CCC      | RX | 16:32:31.2692040 |    N/A | From Central | APDU-Exchange: (GET_RESPONSE)
CCC      | RX | 16:32:31.2734821 |    N/A | From NFC Reader | APDU-Exchange: RESP
CCC      | RX | 16:32:32.2561914 |    N/A | From Central | APDU-Exchange: (CONTROL_FLOW)
CCC      | RX | 16:32:32.2569920 |    N/A | From NFC Reader | APDU-Exchange: RESP
CCC      | RX | 16:32:32.2716769 |    N/A |  |  | Target mission: Nfc owner pairing | Owner Pairing Ph2 passed.
CCC      | RX | 16:32:32.2746496 |    N/A | From central | Start Polling
CCC      | RX | 16:32:33.2073565 |    N/A | From NFC Reader | Phone/Card detected
CCC      | RX | 16:32:33.2075561 |    N/A | From Central | APDU-Exchange: (SELECT: Target_Aid: CCC Applet AID [A000000809434343444B41763100])
CCC      | RX | 16:32:33.2089562 |    N/A | From NFC Reader | APDU-Exchange: Protocol_Version: [0100];
CCC      | RX | 16:32:33.2139379 |    N/A | From Central | APDU-Exchange: (AUTH0: Protocol_Version: [0100]; Vehicle_Eph_Pub_key: 65 Bytes; Transaction_Identifier: [816B26687A36630629E37E9D9CAA8FCD]; Vehicle_identifier:
CCC      | RX | 16:32:33.2194380 |    N/A | From NFC Reader | APDU-Exchange: Auth0 Resp.: Endpoint_ePK: 65 Bytes
CCC      | RX | 16:32:33.2245154 |    N/A | From Central | APDU-Exchange: (AUTH1: Vehicle signature 64 Bytes)
CCC      | RX | 16:32:33.2403917 |    N/A | From NFC Reader | APDU-Exchange: Auth1 Resp.: <encrypted> 88 Bytes
CCC      | RX | 16:32:33.2635045 |    N/A | From Central | APDU-Exchange: (EXCHANGE)
CCC      | RX | 16:32:33.2698124 |    N/A | From NFC Reader | APDU-Exchange: RESP
CCC      | RX | 16:32:33.2773867 |    N/A | From Central | APDU-Exchange: (CONTROL_FLOW)
CCC      | RX | 16:32:33.2779866 |    N/A | From NFC Reader | APDU-Exchange: RESP
CCC      | RX | 16:32:33.2780952 |    N/A |  |  | Target mission: Nfc owner pairing | Owner Pairing Ph3 passed.
CCC      | RX | 16:32:33.2781952 |    N/A | From Central | APDU-Exchange: (SELECT: Target_Aid: CCC Applet AID [A000000809434343444B41763100]
CCC      | RX | 16:32:36.2982169 |    N/A | From central | Start Polling
CCC      | RX | 16:32:38.2366791 |    N/A | From NFC Reader | Phone/Card detected
CCC      | RX | 16:32:38.2368784 |    N/A | From Central | APDU-Exchange: (SELECT: Target_Aid: CCC Applet AID [A000000809434343444B41763100])
CCC      | RX | 16:32:38.2381858 |    N/A | From NFC Reader | APDU-Exchange: Protocol_Version: [0100];
CCC      | RX | 16:32:38.2434010 |    N/A | From Central | APDU-Exchange: (AUTH0: Protocol_Version: [0100]; Vehicle_Eph_Pub_key: 65 Bytes; Transaction_Identifier: [FA240F57B420E558EB2B967DE7BF3EA1]; Vehicle_identifier:
CCC      | RX | 16:32:38.2488746 |    N/A | From NFC Reader | APDU-Exchange: Auth0 Resp.: Endpoint_ePK: 65 Bytes
CCC      | RX | 16:32:38.2532747 |    N/A | From Central | APDU-Exchange: (AUTH1: Vehicle signature 64 Bytes)
CCC      | RX | 16:32:38.2689290 |    N/A | From NFC Reader | APDU-Exchange: Auth1 Resp.: <encrypted> 88 Bytes
CCC      | RX | 16:32:38.2856326 |    N/A | From Central | APDU-Exchange: (CONTROL_FLOW)
CCC      | RX | 16:32:38.2863325 |    N/A | From NFC Reader | APDU-Exchange: RESP
CCC      | RX | 16:32:38.2863325 |    N/A |  |  | Target mission: Standard transaction | CCC transaction done successfully.
```

1. OP2:SPAKE2+

2. OP2: Cert Exchange

3. OP3: first Transaction

4. Standard Transaction

Start OP or transaction in card mode

1. Power up and prepare demo
2. Personalize NCJ37x board
3. Connect CAN cable
4. Start python tool
5. Tap NCJ37B0HN board
6. START OP&ST

time.py | ConfigSettings.py | builtins.py

```
68
69
    1 usage
70  def config_logger(show_can=True, show_jumbo=False, show_figaro=False):
71      if not show_figaro:
72          ccc.LOGGER.parent.setLevel(ccc.LOGGER.CCC + 1)
73      if not show_jumbo:
74          figaro.LOGGER.parent.setLevel(figaro.LOGGER.FIGARO + 1)
75      if not show_can:
76          jumbo.LOGGER.parent.setLevel(jumbo.LOGGER.JUMBO + 1)
77
78
    2 usages
79  def run_config(bus):
80
81      configHandler = ConfigHandler(bus)
82      configHandler.init_config_session()
83
84
85      #configHandler.set_target_ccc_mission(ConfigCccTargetMission.NFC_OWNER_PAIRING)
86      configHandler.set_target_ccc_mission(ConfigCccTargetMission.CARD_PAIRING)
87      #configHandler.set_target_ccc_mission(ConfigCccTargetMission.STANDARD_TRANSACTION)
88      configHandler.set_target_ccc_mission(ConfigCccTargetMission.CARD_ST_TRANSACTION)
89      #configHandler.view_all_dks()
90      #configHandler.delete_all_dks()
91      configHandler.end_config_session()
92
```

Card pairing log

```
"C:\Users\nxp52688\OneDrive - NXP\work\project\zty\CCC\CCC_demo\OneDrive_1_8-3-2022\CAN_Support_Tool\venv\Scripts\python.exe" "C:\Users\nxp52688\OneDrive - NXP\work\project\zty\CCC\CCC_demo\OneDrive_1_8-3-2022\CAN_Support_Tool\main.py"
CCC     | TX |            N/A |    N/A | From PC | CONFIG | Start config command
CCC     | RX | 17:04:14.2664911 |    N/A | From Central Node | CONFIG | Command successful
Thu Jan 18 09:04:14 2024
32303234 31 3138 39 34 3134
CCC     | TX |            N/A |    N/A | From PC | CONFIG | Target_Mission: CARD_PAIRING
CCC     | RX | 17:04:14.2777538 |    N/A | From Central Node | CONFIG | Command successful
Thu Jan 18 09:04:14 2024
32303234 31 3138 39 34 3134
CCC     | TX |            N/A |    N/A | From PC | CONFIG | Stop config command
CCC     | RX | 17:04:14.2789778 |    N/A | From Central Node | CONFIG | Command successful
CCC     | RX | 17:04:17.2747662 |    N/A | From NFC Reader | Phone/Card detected
CCC     | RX | 17:04:17.2796171 |    N/A | From Central | APDU-Exchange: (SELECT: Target_Aid: CCC Framework AID [A0000008094343434444B46763100])
CCC     | RX | 17:04:17.2842177 |    N/A | From NFC Reader | APDU-Exchange: Protocol_Version: [0100];
CCC     | RX | 17:04:17.2898697 |    N/A | From Central | APDU-Exchange: (OP_REQUEST)
CCC     | RX | 17:04:18.2372114 |    N/A | From NFC Reader | APDU-Exchange: RESP
CCC     | RX | 17:04:18.2567146 |    N/A | From Central | APDU-Exchange: (OP_VERIFY)
CCC     | RX | 17:04:19.2262781 |    N/A | From NFC Reader | APDU-Exchange: RESP
CCC     | RX | 17:04:19.2524332 |    N/A | From Central | APDU-Exchange: (WRITE_DATA)
CCC     | RX | 17:04:19.2599843 |    N/A | From NFC Reader | APDU-Exchange: RESP
CCC     | RX | 17:04:20.2956986 |    N/A | From Central | APDU-Exchange: (CONTROL_FLOW)
CCC     | RX | 17:04:22.2256678 |    N/A | From NFC Reader | APDU-Exchange: RESP
CCC     | RX | 17:04:22.2352200 |    N/A | From central | Start Polling
CCC     | RX | 17:04:22.2429715 |    N/A | From NFC Reader | Phone/Card detected
CCC     | RX | 17:04:22.2431716 |    N/A | From Central | APDU-Exchange: (SELECT: Target_Aid: CCC Framework AID [A0000008094343434444B46763100])
CCC     | RX | 17:04:22.2472715 |    N/A | From NFC Reader | APDU-Exchange: Protocol_Version: [0100];
CCC     | RX | 17:04:22.2492719 |    N/A | From Central | APDU-Exchange: (GET_DATA)
CCC     | RX | 17:04:22.2582230 |    N/A | From NFC Reader | APDU-Exchange: RESP
CCC     | RX | 17:04:22.2638773 |    N/A | From Central | APDU-Exchange: (GET_RESPONSE)
CCC     | RX | 17:04:23.2912162 |    N/A |  |  | Target mission: Card pairing | Owner Pairing Ph2 passed.
CCC     | RX | 17:04:23.2927164 |    N/A |  |
CCC     | RX | 17:04:23.2942161 |    N/A | From central | Start Polling
CCC     | RX | 17:04:24.2025871 |    N/A | From NFC Reader | Phone/Card detected
CCC     | RX | 17:04:24.2027856 |    N/A | From Central | APDU-Exchange: (SELECT: Target_Aid: CCC Applet AID [A000000809434343444B41763100])
CCC     | RX | 17:04:24.2064855 |    N/A | From NFC Reader | APDU-Exchange: Protocol_Version: [0100];
CCC     | RX | 17:04:24.2120371 |    N/A | From Central | APDU-Exchange: (AUTH0: Protocol_Version: [0100]; Vehicle_Eph_Pub_key: 65 Bytes; Transaction_Identifier: [C33CBEA054F87E48D2DE206E5B1F286C]; Vehicle_identifier: [9999999999999999])
CCC     | RX | 17:04:24.2285878 |    N/A | From NFC Reader | APDU-Exchange: Auth0 Resp.: Endpoint_ePK: 65 Bytes
CCC     | RX | 17:04:24.2336402 |    N/A | From Central | APDU-Exchange: (AUTH1: Vehicle signature 64 Bytes)
CCC     | RX | 17:04:24.2874728 |    N/A | From NFC Reader | APDU-Exchange: Auth1 Resp.: <encrypted> 88 Bytes
CCC     | RX | 17:04:25.2063763 |    N/A | From Central | APDU-Exchange: (CONTROL_FLOW)
CCC     | RX | 17:04:25.2080763 |    N/A | From NFC Reader | APDU-Exchange: RESP
CCC     | RX | 17:04:25.2081765 |    N/A |  |
CCC     | RX | 17:04:25.2081765 |    N/A |  |  | Target mission: Card pairing | Owner Pairing Ph3 passed.
CCC     | RX | 17:04:25.2082766 |    N/A | From Central | APDU-Exchange: (SELECT: Target_Aid: CCC Applet AID [A000000809434343444B41763100])
CCC     | RX | 17:04:28.2346468 |    N/A | From NFC Reader | Phone/Card detected
CCC     | RX | 17:04:28.2348487 |    N/A | From Central | APDU-Exchange: (SELECT: Target_Aid: CCC Applet AID [A000000809434343444B41763100])
CCC     | RX | 17:04:28.2384476 |    N/A | From NFC Reader | APDU-Exchange: Protocol_Version: [0100];
CCC     | RX | 17:04:28.2439981 |    N/A | From Central | APDU-Exchange: (AUTH0: Protocol_Version: [0100]; Vehicle_Eph_Pub_key: 65 Bytes; Transaction_Identifier: [DB7503860794A020C8E00F632A53A83E]; Vehicle_identifier: [9999999999999999])
CCC     | RX | 17:04:28.2606014 |    N/A | From NFC Reader | APDU-Exchange: Auth0 Resp.: Endpoint_ePK: 65 Bytes
CCC     | RX | 17:04:28.2657014 |    N/A | From Central | APDU-Exchange: (AUTH1: Vehicle signature 64 Bytes)
CCC     | RX | 17:04:29.2193759 |    N/A | From NFC Reader | APDU-Exchange: Auth1 Resp.: <encrypted> 88 Bytes
CCC     | RX | 17:04:29.2362265 |    N/A | From Central | APDU-Exchange: (CONTROL_FLOW)
CCC     | RX | 17:04:29.2379260 |    N/A | From NFC Reader | APDU-Exchange: RESP
CCC     | RX | 17:04:29.2380244 |    N/A |  |
CCC     | RX | 17:04:29.2380244 |    N/A |  |  | Target mission: Card st transaction | CCC transaction done successfully.
CCC     | RX | 17:04:32.2974957 |    N/A | From central | Start Polling
```

1. OP2:SPAKE2+

2. OP2: Cert Exchange

3. OP3: first Transaction

4. Standard Transaction

View dk log

```
"C:\Users\nxp52688\OneDrive - NXP\work\project\zty\CCC\CCC_demo\OneDrive_1_8-3-2022\CAN_Support_Tool\venv
\Scripts\python.exe" "C:\Users\nxp52688\OneDrive - NXP\work\project\zty\CCC\CCC_demo\OneDrive_1_8-3-2022\
CAN_Support_Tool\main.py"
Thu Jan 25 08:46:31 2024
32303234 31 3235 38 3436 3331
CCC      | TX |              N/A |    N/A | From PC | CONFIG | Start config command
JUMBO    | TX |              N/A |    N/A | 0x1F00FB01 | 29 bit ID, FD | total_len: 17 [0x11] |
60010032303234303132353038343633331
JUMBO    | RX | 16:46:31.2148087 |    N/A | 0x17000A01 | 29 bit ID, FD | total_len: 1 [0x01] | 01
CCC      | RX | 16:46:31.2148699 |    N/A |  |
Thu Jan 25 08:46:31 2024
32303234 31 3235 38 3436 3331
CCC      | TX |              N/A |    N/A | From PC | CONFIG | Start config command
JUMBO    | TX |              N/A |    N/A | 0x1F00FB01 | 29 bit ID, FD | total_len: 17 [0x11] |
60010032303234303132353038343633331
JUMBO    | RX | 16:46:31.2148699 |    N/A | 0x17000A01 | 29 bit ID, FD | total_len: 1 [0x01] | 02
CCC      | RX | 16:46:31.2148699 |    N/A |  |
Thu Jan 25 08:46:31 2024
32303234 31 3235 38 3436 3331
CCC      | TX |              N/A |    N/A | From PC | CONFIG | Start config command
JUMBO    | TX |              N/A |    N/A | 0x1F00FB01 | 29 bit ID, FD | total_len: 17 [0x11] |
60010032303234303132353038343633331
JUMBO    | RX | 16:46:31.2200556 |    N/A | 0x1700FB01 | 29 bit ID, FD | total_len: 3 [0x03] | 6001FF
CCC      | RX | 16:46:31.2200556 |    N/A | From Central Node | CONFIG | Command successful
Thu Jan 25 08:46:31 2024
32303234 31 3235 38 3436 3331
CCC      | TX |              N/A |    N/A | From PC | CONFIG
JUMBO    | TX |              N/A |    N/A | 0x1F00FB01 | 29 bit ID, FD | total_len: 3 [0x03] | 600108
JUMBO    | RX | 16:46:31.2546473 |    N/A | 0x1700FB01 | 29 bit ID, FD | total_len: 191 [0xBF] |
5F13614E040000000065014D19C272F0249E417BCE1D48FADA75F83209BC75CD3066950686F6E65510F32303234303132353038333
231365A520F393939393132333132333353935395A5F1401005F16060000000000005F13614E04FFFFFF00F0147DDC396BFA17F339
05227C4465E6DAFF21C200CED3114E78705F536D6172745F4B65795F466F62510F32303234303132353038343534365A520F39393
939313233313233353935395A5F140102D901005F16060000000000005F0902A55A
CCC      | RX | 16:46:31.2546986 |    N/A |  |
JUMBO    | RX | 16:46:31.2621939 |    N/A | 0x1700FB01 | 29 bit ID, FD | total_len: 3 [0x03] | 6001FF
CCC      | RX | 16:46:31.2621939 |    N/A | From Central Node | CONFIG | Command successful
Thu Jan 25 08:46:31 2024
32303234 31 3235 38 3436 3331
CCC      | TX |              N/A |    N/A | From PC | CONFIG | Stop config command
JUMBO    | TX |              N/A |    N/A | 0x1F00FB01 | 29 bit ID, FD | total_len: 3 [0x03] | 600101
JUMBO    | RX | 16:46:31.2633719 |    N/A | 0x1700FB01 | 29 bit ID, FD | total_len: 3 [0x03] | 6001FF
CCC      | RX | 16:46:31.2633719 |    N/A | From Central Node | CONFIG | Command successful
```

Device keyslot ID

Keyfob/Card keyslot ID

Personalize in NCJ38A0HN (uUpdate by car-side applet v1.1.14 UM)

Pairing Mode	Perso Tag Name	Perso Tag	Comments
Phone Pairing	TAG_INSTALL_VEHICLE_LONG_TERM_PUBLIC_KEY	0x40	Vehicle LTK PK
	TAG_INSTALL_VEHICLE_LONG_TERM_PRIVATE_KEY	0x41	Vehicle LTK SK
	TAG_INSTALL_VEHICLE_IDENTIFIER	0x4F	Vehicle identifier
	TAG_INSTALL_ENDPOINT_CREATION_NOT_BEFORE	0x61	Endpoint certation timestamp
	TAG_INSTALL_ENDPOINT_CREATION_NOT_AFTER	0x62	
	TAG_INSTALL_INTERMEDIATE_CERTIFICATE	0x6B	Vehicle Intermediate CA
	TAG_INSTALL_VEHICLE_PUBLIC_KEY_CERTIFICATE	0x6C	Vehicle Public KEY CA[K]
	TAG_INSTALL_VEHICLE_OEM_ROOT_CA_CERTIFICATE	0x6D	Vehicle OEM CA[J]
	TAG_INSTALL_VEHICLE_OEM_ROOT_CA_PUBLIC_KEY	0x6E	Vehicle OEM PK
	TAG_INSTALL_SPAKE2P_W0	0x6F	SPAKE2 Parameter W0
	TAG_INSTALL_SPAKE2P_L	0x70	SPAKE2 Parameter L
Card Pairing	TAG_INSTALL_NUMBER_OF_ADDITIONAL_DEVICE_SUPPORTED	0x91	Keyfob/card number
	TAG_INSTALL_FOB_VEHICLE_IDENTIFIER	0xD2	Set Key Fob vehicle identifier
	TAG_INSTALL_VEHICLE_PUBLIC_KEY_CERTIFICATE_KEYFOB	0xD3	Set Key Fob Vehicle Public key CA [K]
	TAG_INSTALL_FOB_INTERMEDIATE_CERTIFICATE	0xD5	Set Key Fob Intermediate CA
	TAG_INSTALL_VEHICLE_OEM_ROOT_CA_CERTIFICATE_KEYFOB	0xD7	Set Key Fob Vehicle OEM CA[J]
	TAG_INSTALL_VEHICLE_OEM_ROOT_CA_PUBLIC_KEY_KEYFOB	0xDB	Set Key Fob Vehicle OEM PK
	TAG_INSTALL_CAR_LONG_TERM_PUBLIC_KEY_FOR_KEYFOB	0xD9	Set Key Fob Vehicle LTK PK
	TAG_INSTALL_CAR_LONG_TERM_PRIVATE_KEY_FOR_KEYFOB	0xDA	Set Key Fob Vehicle LTK SK
	TAG_INSTALL_SPAKE2P_W0_KEYFOB	0x96	Set Key Fob SPAKE2 Parameter W0
	TAG_INSTALL_SPAKE2P_L_KEYFOB	0x97	Set Key Fob SPAKE2 Parameter L

Personalize In key fob (NCJ37B0HN)

Perso Name	Comments
_setKeys	ISD key set for NCJ37B0HN
ownerKeyFriendlyName	Owner key friend name same as NCJ38A0HN
vehicleIdentifier	Vehicle identifier same as phantom
vehicleOemCA	Vehicle OEM CA[J]
deviceOemCA	Device OEM CA
vehicleIntermediateCA	Vehicle intermediate CA
vehicle.PK vehicle.SK	Vehicle public key CA [K]

```
# Vehicle identifier
/s-v vehicleIdentifier 9999999999999999
/echo ${vehicleIdentifier}

/applet JCipher

# Vehicle OEM CA
/s-v vehicleOemCA.name "Vehicle-OEM-ROOT-CA-TEST-E"

/s-v vehicleOemCA.SK 60609AD3320D4745A6DED981764C07F1F398E6B1C182E0A904D852D1CF297858

/s-v vehicleOemCA.PK 042808F56DD8F7599AEFAC433B937D1EBBF76BFFF8B472187EDF067B7258F7281E170385
/echo vehicleOemCA: ${vehicleOemCA.SK}
/echo vehicleOemCA: ${vehicleOemCA.PK}

/s-v vehicleOemCA.cert
308201403081E8A003020102020844486665C3CE7A3F3300A06082A8648CE3D0403023025312330210603550403
04030C1A56656869636C652D4F454D2D524F4F542D43412D544553542D453059301306072A8648CE3D020106082A8
881725ADFF0915A3023000300A06082A8648CE3D040302034700304402202526470066F789891FEB467BB77103C62
/echo "Vehicle OEM CA Certificate:" ${vehicleOemCA.cert}

# Device OEM CA (NXP-CCC-ROOT-CA-TEST)
/s-v deviceOemCA.name "NXP-CCC-ROOT-CA-TEST"
/s-v deviceOemCA.SK 02F488A093C905A1D1A0EF2517F340B6B3DA131C454F524E76B74F4715B004E1
/s-v deviceOemCA.PK 0430C5E5B52F741C00B691273E75DDFCEB949729F18605F768A7543984E0FDFFF8EC9895A
/s-v deviceOemCA.PK.identifier $(hash -m SHA-1 ${deviceOemCA.PK})

/s-v deviceOemCA.cert
308201BA30820160A003020102020812D906DBA67500FD300A06082A8648CE3D0403023025312330210603550403
060355040313144E58502D4343432D524F4F542D43412D544553543059301306072A8648CE3D020106082A8648CE3
8B4D5271A37E307C3016060A2B0601040182C46905020101FF0405300302010300E0603551D0F0101FF040403020
A3080439300D5C54AA8A51989CF5068D8D58300A06082A8648CE3D0403020348003045022011700097A7A1705C15AF
/echo "Device OEM CA Certificate:" ${deviceOemCA.cert}

# Vehicle Intermediate CA (signed by Vehicle OEM CA) - Why intermediate? Why not [J]?
keygen -m ECC -o keypairgen
/s-v vehicleIntermediateCA.name "Vehicle-OEM-Intermediate-CA-TEST-E"
/s-v vehicleIntermediateCA.SK ${KEY_ECC_PrivateKey}
/s-v vehicleIntermediateCA.PK 04${KEY_ECC_PublicKeyX}${KEY_ECC_PublicKeyY}

/s-v vehicleIntermediateCA.cert
308201483081F0A003020102020809366386DC9C4E41300A06082A8648CE3D0403023025312330210603550403
04030C2256656869636C652D4F454D2D496E7465726D6564696174652D43412D544553542D453059301306072A864
D8DE1D1111775178B72E85C946D9D1A3023000300A06082A8648CE3D040302034700304402203A66D7798EEEEA2AF
/echo "Vehicle Intermediate CA Certificate:" ${vehicleIntermediateCA.cert}

# Vehicle Public Key - this is transferred from Vehicle during owner pairing.Why it is config
keygen -m ECC -o keypairgen
/s-v vehicle.name "V.TST1.WWE.BRND.${vehicleIdentifier}"

/s-v vehicle.SK 0A5E077E810F8A7D201FB52ABB7D6376E006D32B1920F534B0E6CCE1C858C58B

/s-v vehicle.PK 040DFD326901DE5B8178B02EA576DBC42389C62883D3E83A55514D97D822930B48471FDB75176
```

Brighter
Together

nxp.com