CCC Digital Key
The Future of Vehicle Access

DIGITAL KEY

Car Connectivity Consortium Overview

Global consortium, bringing car, handset and head-unit industries together

- Established in February 2011.
- Membership open to any interested company.

Objective: develop smartphone-based connected-car solutions

- Solutions are standardized, platform agnostic and not owned/governed by a single member.
- Runs certification programs to ensure interoperability.

Established standards rolled out globally

- MirrorLink®.
- CCC Digital Key.

Celebrating 200 Members

CARCONNECTIVITY consortium

200

MEMBERS

BY THE NUMBERS

15	81	104
CHARTER	CORE	ADOPTER

AUSTRIA	4	ISRAEL	1	SWEDEN	3
CANADA	1	JAPAN	25	SWITZERLAND	2
CHINA	52	NETHERLANDS	1	TAIWAN	5
FINLAND	1	NORWAY	1	THAILAND	1
FRANCE	9	POLAND	2	UNITED KINGDOM	5
GERMANY	31	SOUTH KOREA	14	UNITED STATES	32
INDIA	5	SPAIN	4	VIETNAM	1

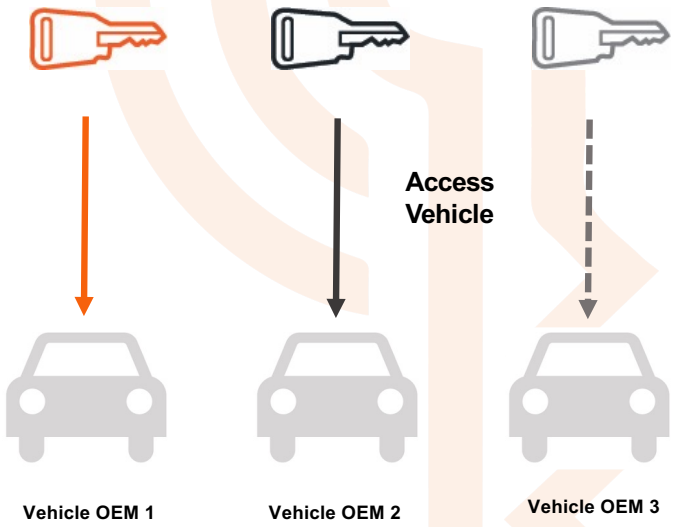
FOUNDING MEMBERS

DENSO Crafting the Core, gm, HONDA, HYUNDAI, Mercedes-Benz, Panasonic, TOYOTA

Vehicle Access Today

Industry is segregated:

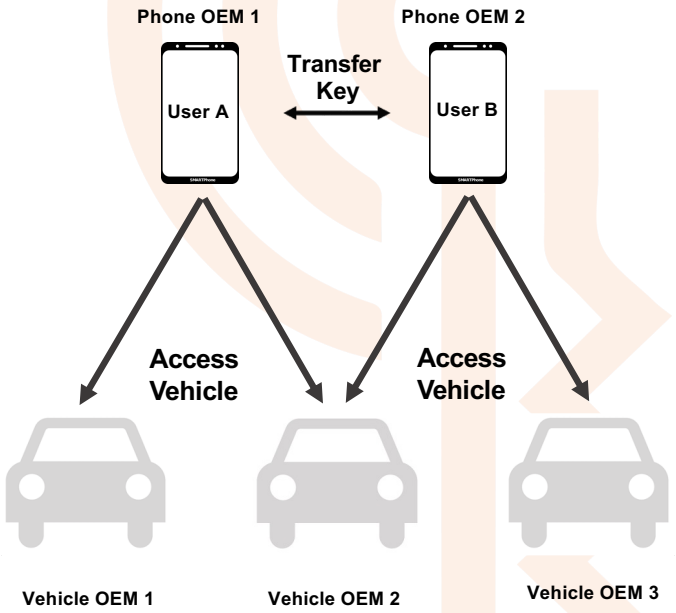
- Each Vehicle OEM uses proprietary key fobs & technology.
- No scale / parallel development without technology differentiation.
- Similar user story on all vehicles and devices.



Vehicle Access with CCC Digital Key

Standardized Vehicle Access for all vehicles and devices

- Digital keys are transferrable between devices.
- Common user experience on all vehicles and devices.
- High Security.



CCC Digital Key brings new features and use cases

DIGITAL KEY

- CCC Digital Key standardization has brought together all the relevant industries to create a solution that serves everyone.
- Standardized vehicle access protocol over NFC and BLE in combination with UWB.
- Common Criteria evaluated digital key applet to allow highest level of security.
- Scalable architecture to support wide-scale deployment of the digital key services across different vehicle and device OEMs.

Digital Key Security and Privacy Concept

CCC Digital Key in Mobile Device: **this is secure.**

Malware on Device:
Use Secure Elements for all security relevant functions

RF Relay:
Distance bounding with NFC / Secure distance measurement with UWB

Standardization target:
Highest achievable security

Attack Credentials:
Use Secure Element for storage of credentials

Software Relay:
Direct binding between SE and NFC / UWB

Privacy:
Smart phone identity not revealed to vehicles

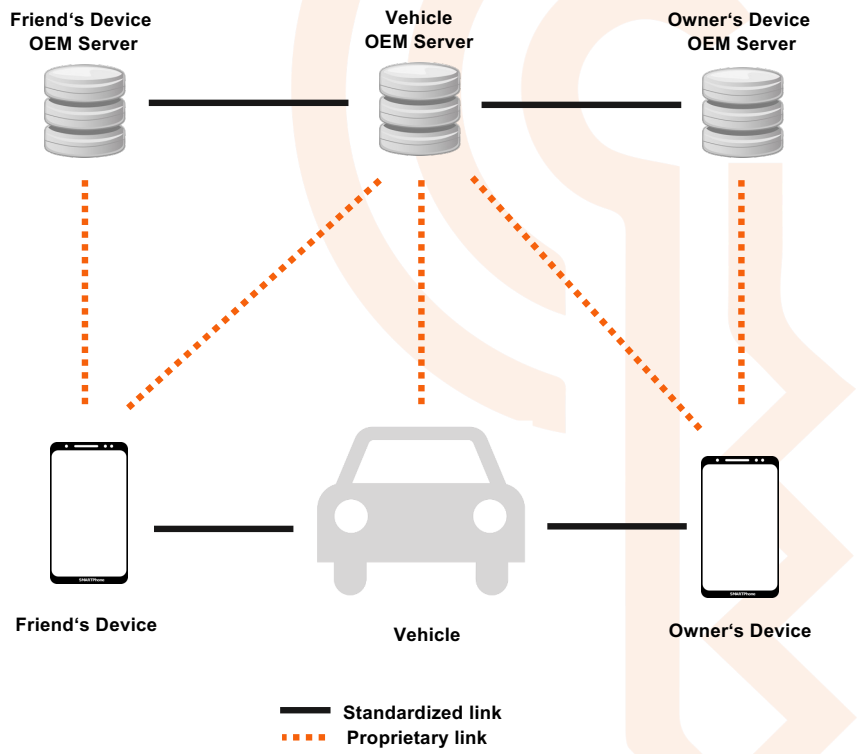
CCC Digital Key Standardized Use Cases

- Lock and Unlock the Vehicle
- Remote Keyless entry
- Passive entry / Passive start
- Start the Engine
- Digital Key Provisioning / Owner Pairing
- Friend Key Sharing
- Entitlements – Restricting Key Usage
- Digital Key Termination

CCC Digital Key Architecture

Standardized Interfaces:

- Interface Vehicle – Mobile Device
- Interface Vehicle OEM Backend – Device OEM Backend



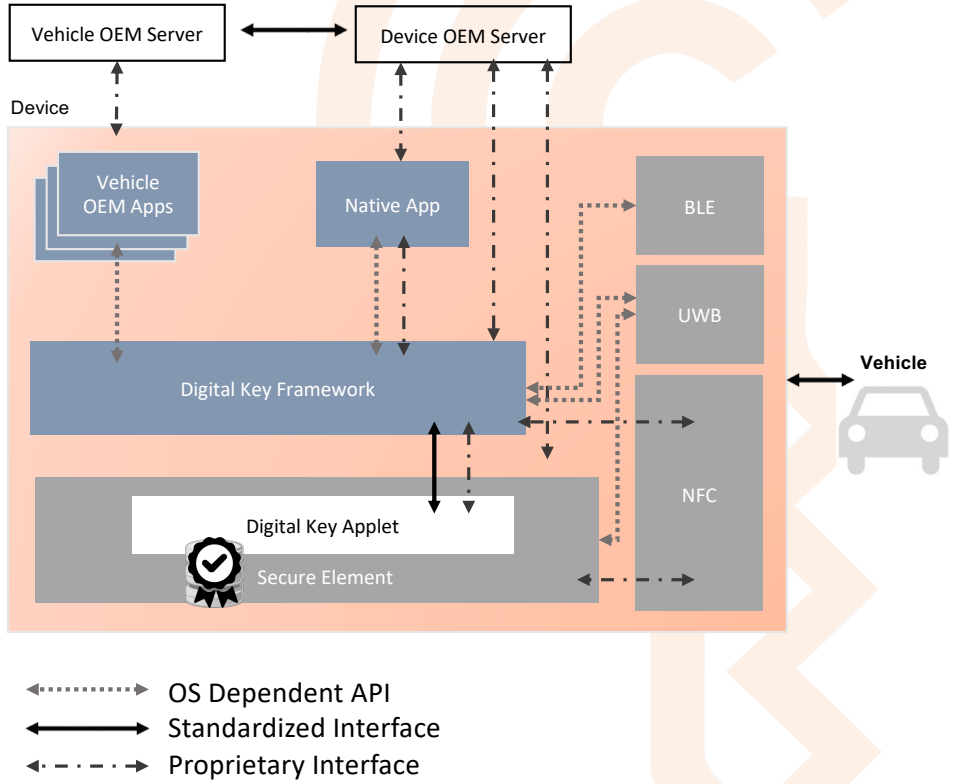
CCC Digital Key Architecture

Use of a Secure Element:

The Digital Key Applet, which resides within the Secure Element, performs all security-critical processing.

Providing secure, tamper-proof storage for digital keys.

Secure Elements evaluated against the highest security requirements by recognized Security Laboratories.

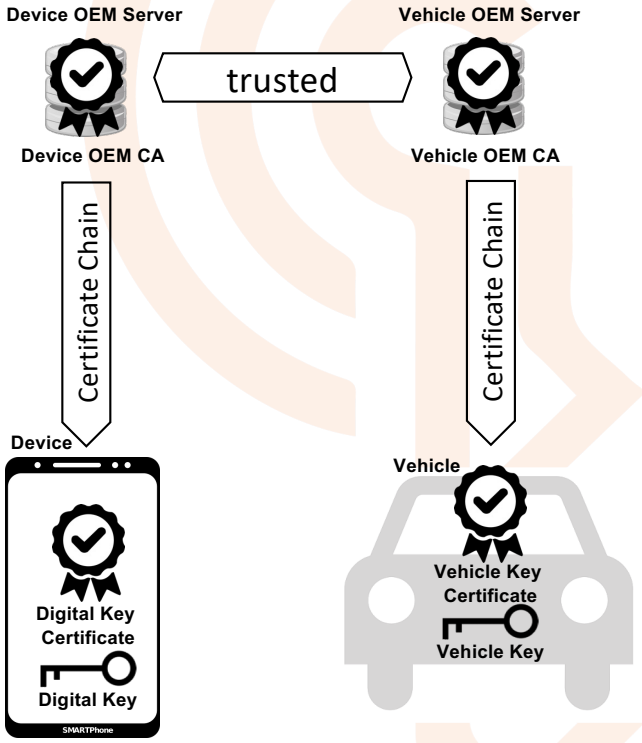


Security Concept PKI

Device OEM and Vehicle OEM have trusted Certification Authorities (CA)

Keys are generated in Device are kept in secure storage

Certificate Chains are stored in Device and Vehicle



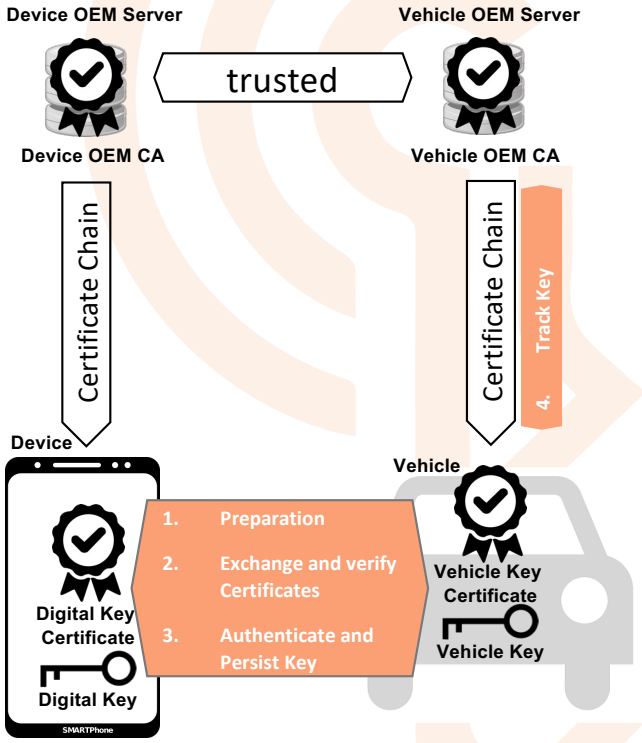
Security Concept Pairing

01. Prepare Device and Vehicle
- Create Keys and Signatures

02. Exchange and verify Certificates

03. Track Key
- Vehicle OEM to verify and track the pairing

04. Authenticate and generate Persist Key
- Transfer additional security tokens
- Verify Key Tracking

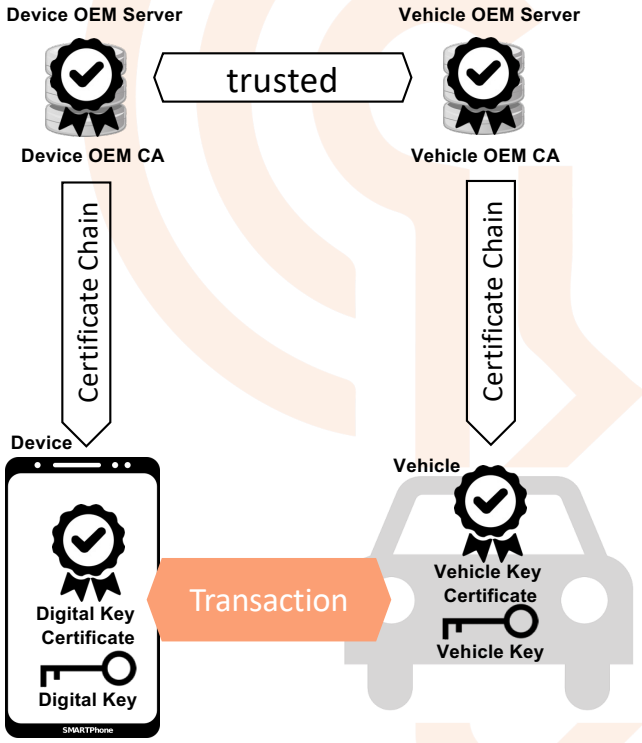


Security Concept Transaction

01. Mutual Authentication protocol executed between vehicle and device

02. Secure channel established based on the exchanged certificates

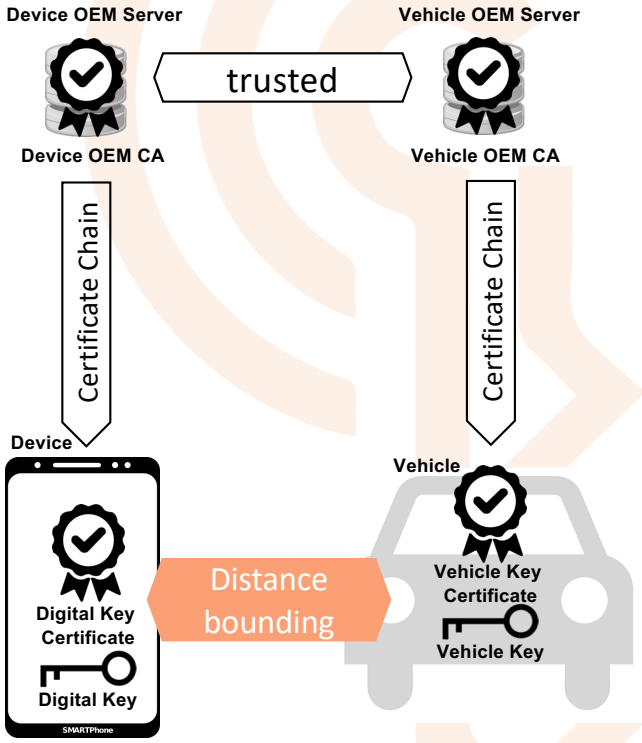
03. Transmission of command over secure channel



Security Concept Distance Bounding

In addition to the mutual authentication, proximity to the vehicle is assured.

NFC	Devices must be within a few centimeters in order to communicate
UWB	Cryptographically secured distance measurement based on IEEE 802.15.4z



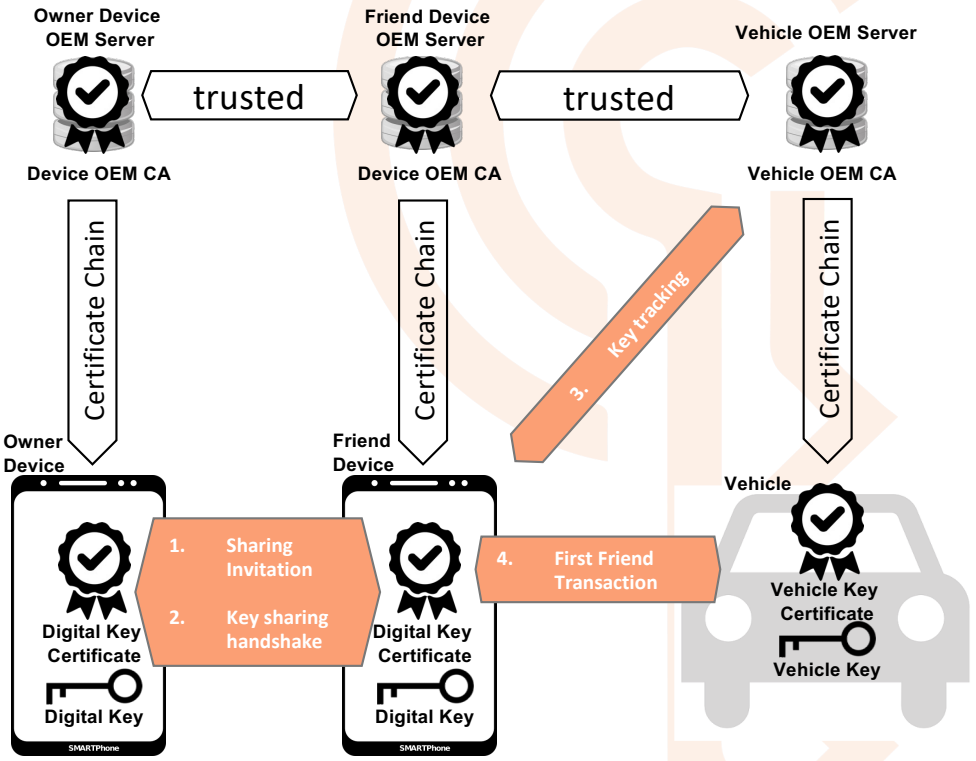
Security Concept Sharing

01. Owner reaches out to friend with a sharing invitation

02. Key sharing handshake

03. Track Key
- Vehicle OEM to verify and track the pairing

04. First Friend Transaction
- Verify Key Tracking
- Persist Friend Key in Vehicle



DK Applet PP – TOE Architecture

TOE type

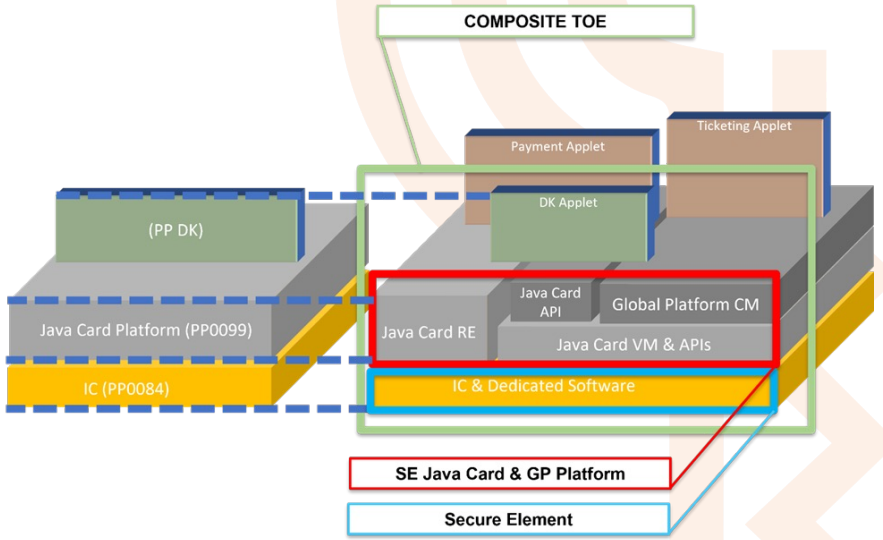
- Secure element composition on top of a
  - PP0084 certified IC and
  - PP0099 certified Java Card Platform

Conformance

- Strict

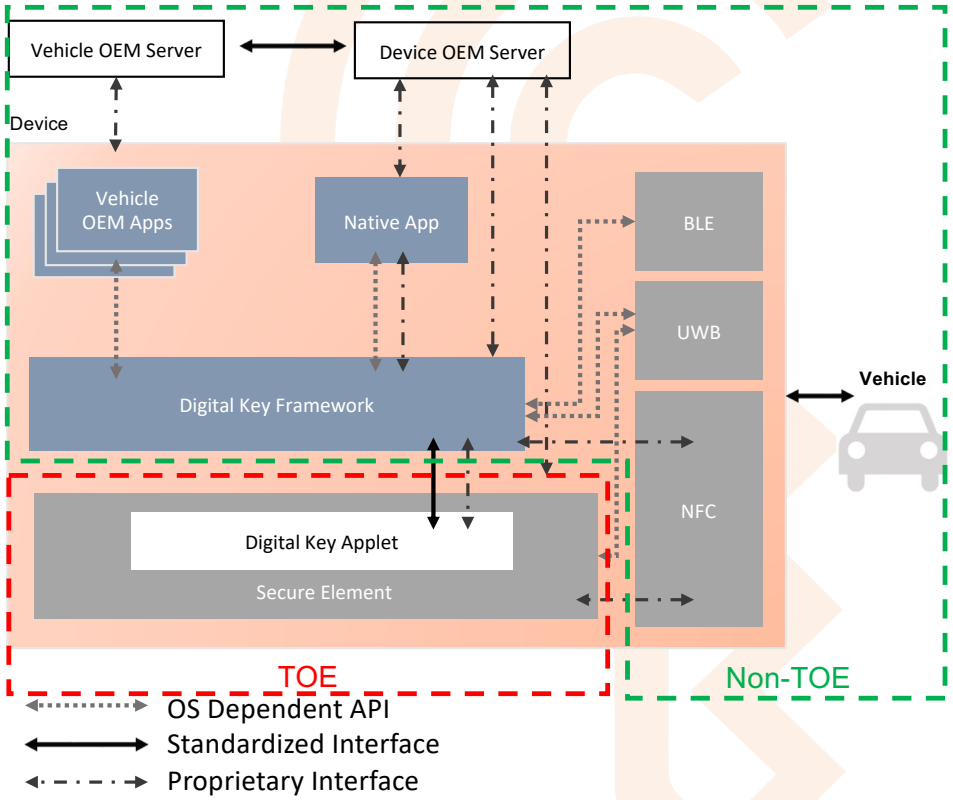
Assurance

- EAL4 augmented with ALC_DVS.2 and AVA_VAN.5



DK Applet PP – TOE Security Features

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



DK Applet PP - Acknowledgements

PP Author – Roland Atoui, Red Alert Labs

CARCONNECTIVITY consortium®

Reviewers – All CCC members contributing to the PP

ITSEF – SRC

Certification Body – BSI Germany

CCC Digital Key: Dedicated to cross-industry collaboration

- The Car Connectivity Consortium (CCC) is dedicated to cross-industry collaboration in developing global standards and solutions for smartphone and in-vehicle connectivity.
- The organization's 100 plus members represent a large portion of the global automotive and smartphone market.
- The Board of Directors of CCC include individuals from the following Charter Member Companies.

Apple Inc, BMW, Ford, General Motors, Google, Honda, Hyundai, Mercedes Benz, NXP, Panasonic, Samsung, Thales, Volkswagen, Xiaomi

Car Connectivity Consortium – Consensus based, contribution driven.

Everyone is welcome - Please join and support to make smartphone-based connected-car solutions even more secure and customer centric.

For further information about CCC projects and to get involved,

please visit

- www.carconnectivity.org

or email to

- admin@carconnectivity.org.

Follow us on LinkedIn

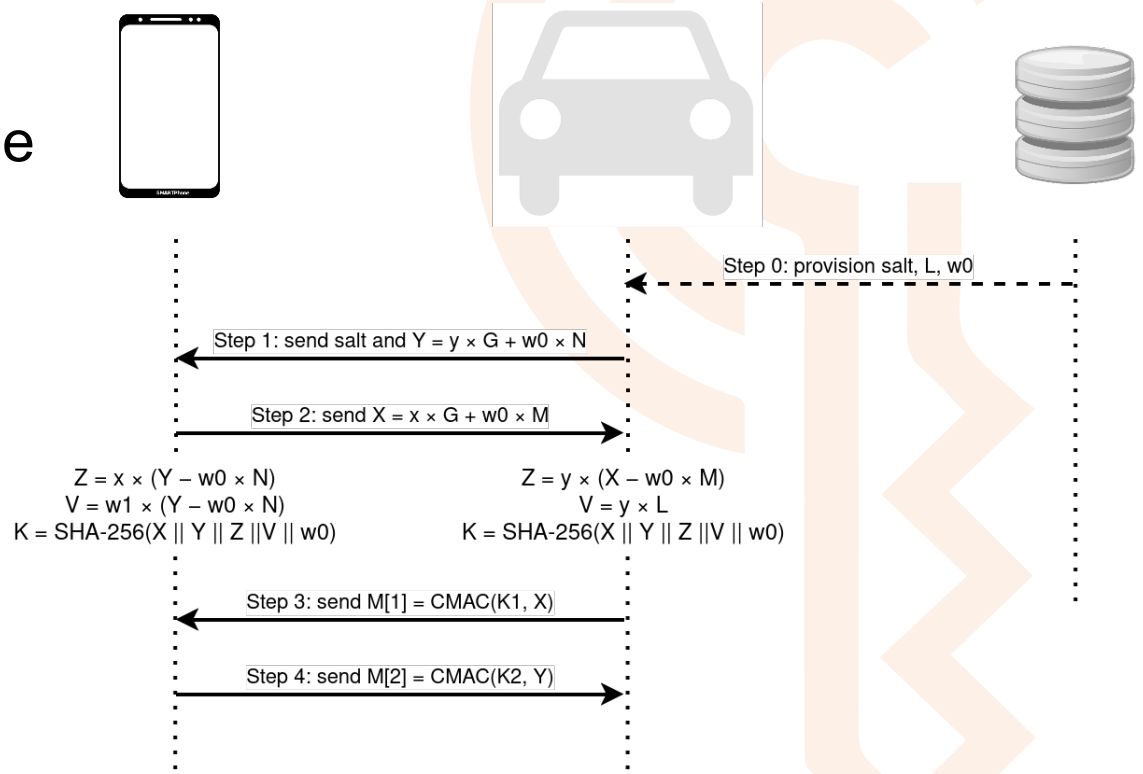
- https://www.linkedin.com/company/car-connectivity-consortium-ccc/

CCC Digital Key and FIPS

FIPS authentication requirements	• Level 2: role-based authentication • Level 3: identity-based authentication • Level 4: multi-factor identity-based authentication
Authentication in Digital Key	• Initial pairing: pre-provisioned password (PAKE) • Subsequent connections: ephemeral key pairs signed by device/vehicle public keys + signed challenge/response
Corresponding NIST SP 800-63b authentication types	• Memorized secret • Single-factor cryptographic software

SPAKE2+

- Symmetric Password-Authenticated Key Exchange
- Cryptographic Primitives:
  - scrypt
  - ECC with P-256
  - SHA-256
  - HKDF
  - CMAC-AES-128



THANK YOU