

Defining Common Requirements for Automotive Key Management

Theo Van Dam
Stellantis

Agenda

Why does the OEM care

OEM Objectives

Areas for Commonality

Areas for Diversity

Future Opportunities

Why Does the OEM Care

Name on the vehicle

- People will call the vehicle brand first for support and blame that brand for any issue.

Better cryptography is generally not a competitive advantage

- Customers don't care as long as the vehicle is secure
- The most benefit is generally gained by keeping vehicles secure and cryptographic costs cheap

OEM Objectives

- Secure for the production and warranty time (can be 20+ years)
 - 10 years in production plus another 10 years in warranty
- Maintain the vehicle for the whole life of the vehicle
- Be able to establish OEM based trust
- Cryptography can't be turned off

Areas for Commonality

Allow for keys and cryptography to be updated

- Based on long security life

Allow for keys unique to SN ECU

- Based on long security life
- Solve problem by making keys not valuable targets

Have a significant key store

- Based on need to limit the trust of any individual key

The ability to query key/certificate store and sanction list

- Needed to properly debug and maintain vehicle

Areas for Diversity

How trust is established and maintained

- Can push or pull based on OEM and function needs
- May want different key characteristics for different applications

How keys are handled for different communication protocols

- How keys are used and the administration around them is tied to the communication protocol used
- Can standardize within a protocol

Future Opportunities

Post Quantum Cryptography uses mathematical capabilities useful for other vehicle features

ML-DSA, ML-KEM, and FN-DSA use vector math which is also useful for graphics, autonomous driving, and artificial intelligence.

FN-DSA also uses floating point and Fast Fourier Transform, which is useful for sensor signal processing.

Having the ability to use computational resources for both secure cryptographic calculations and also other functions is a useful selling point.



**Global
Platform[®]**

Securing the digital future

→ globalplatform.org