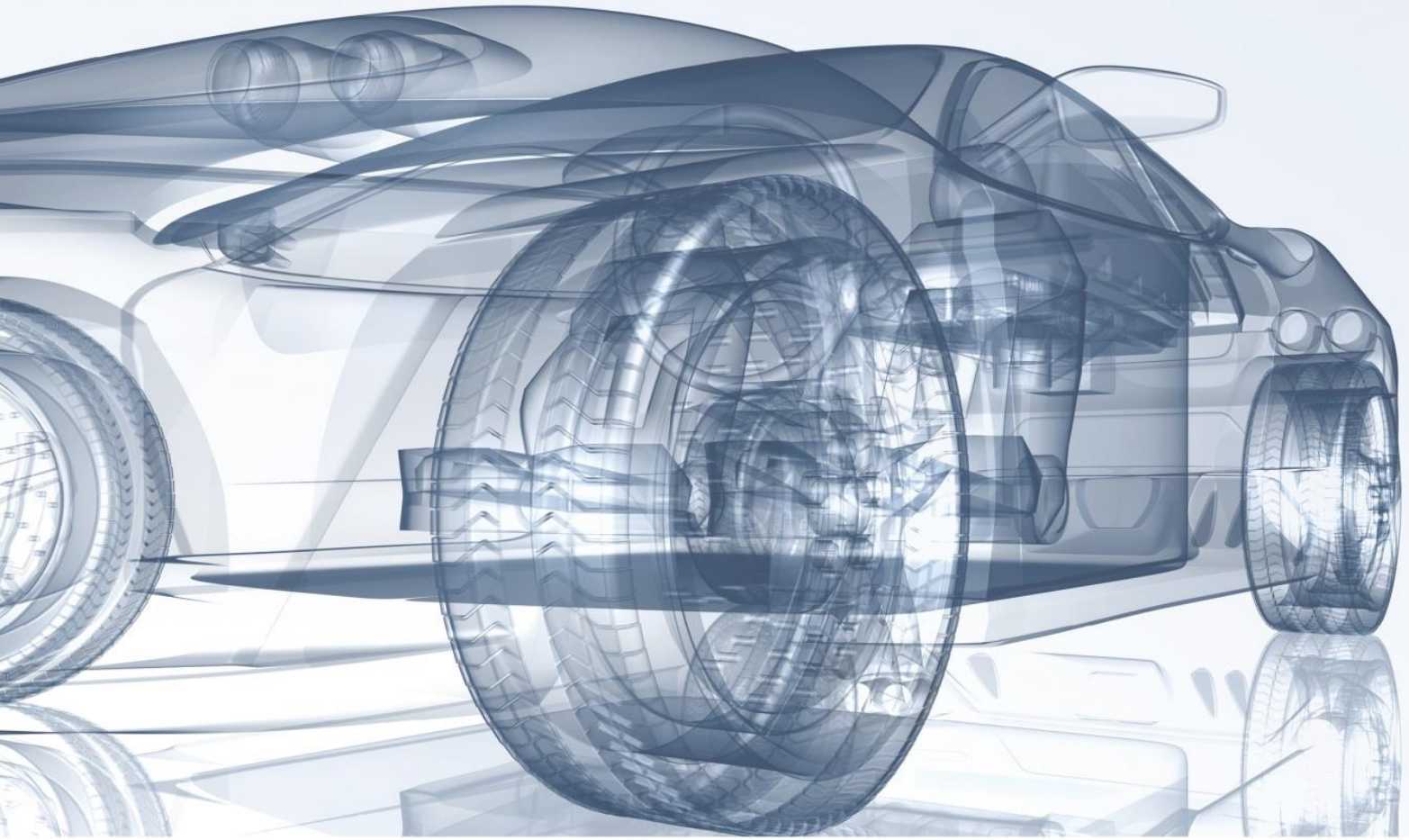
evs 30



The 30th International
Electric Vehicle
Symposium & Exhibition

October 9–11, 2017

Messe Stuttgart, Germany

www.evs30.org

Sponsored by

DAIMLER BOSCH Invented for life GROUPE RENAULT MAHLE EnBW PORSCHE swarco

VECTOR

Introducing Hardware Security Modules to Embedded Systems

for Smart Charging (ISO/IEC 15118)

Presenter: Fabian Eisele, Vector Informatik GmbH

V1.0 | 2017-10-10

Agenda

- **Hardware Trust Anchors - General Introduction**

  Hardware Trust Anchors - Utilization within AUTOSAR

  ISO/IEC 15118 - Certificate Usage

  ISO/IEC 15118 - Impact on Embedded Systems

  Outlook

General Introduction to Hardware Trust Anchors (HTA)

- Hardware Trust Anchors (HTA)
  - Protect sensitive data (e.g. crypto material) from unauthorized access
  - Provide crypto functions (e.g. ECDSA signature generation) to unburden the host controller

- Different standardized feature sets for HTAs
  - Secure Hardware Extension (SHE)
  - Hardware Security Module (HSM)
  - Trusted Platform Module (TPM)

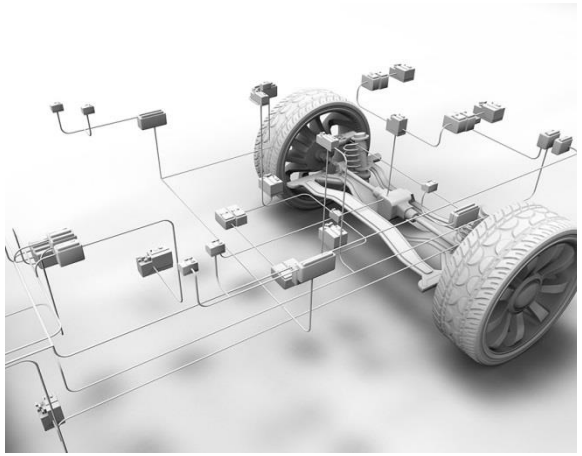
- Different brand names for HTA by different HW suppliers
  - Infineon: Aurix HSM / SHE+ driver
  - Renesas: Intelligent Cryptographic Unit (ICU)
  - Freescale: Crypto Service Engine (CSE)
  - ARM: Trust Zone

Hardware Security Module (HSM)

- History
  - Developed in EU-sponsored project EVITA
  - Consortium: Robert Bosch, BMW, Infineon, …
  - Specs available via the EVITA web site

- HSM design objectives
  - Harden ECUs against attacks
    - SW as well as selected HW attacks
  - Provide HW acceleration for crypto functions
    - By offloading the Application Core
  - Support ECU to ECU communication protection
    - To securely transport sensitive information

- EVITA HSM profiles
  - HSM full
    - Support strong authentication (e.g. via RSA, ECC)
    - Support complex block ciphers
    - High performance
  - HSM medium
    - Secure ECU 2 ECU communication
  - HSM small
    - Secure critical sensors / actuators
    - Simple block ciphers
    - Low cost modules



Comparison of SHE and HSM

	SHE ~ HSM (small)	HSM (medium)	HSM (full)
Integrity of Crypto Material	Yes	Yes	Yes
Secure storage of symmetric crypto material	Yes	Yes	Yes
Secure storage of asymmetric crypto material	No	Yes	Yes
Dedicated CPU	No	Yes	Yes
HW support for symmetric cryptography	Yes	Yes	Yes
HW support for asymmetric cryptography	No	No	Yes
Additional things to consider	+ Availability of HW	+ Allows Firmware Changes + SW security libraries can be executed in HSM	+ High Performance - Cost - Availability of HW
Summary	Cost effective when system doesn't require asymmetric cryptography and functionality doesn't need to be extended	Recommended when asymmetric cryptography is not required, but system shall be extendable	Recommended when high performance is required, i.e. for ISO/IEC 15118 PnC

Agenda

Hardware Trust Anchors - General Introduction

- **Hardware Trust Anchors - Utilization within AUTOSAR**

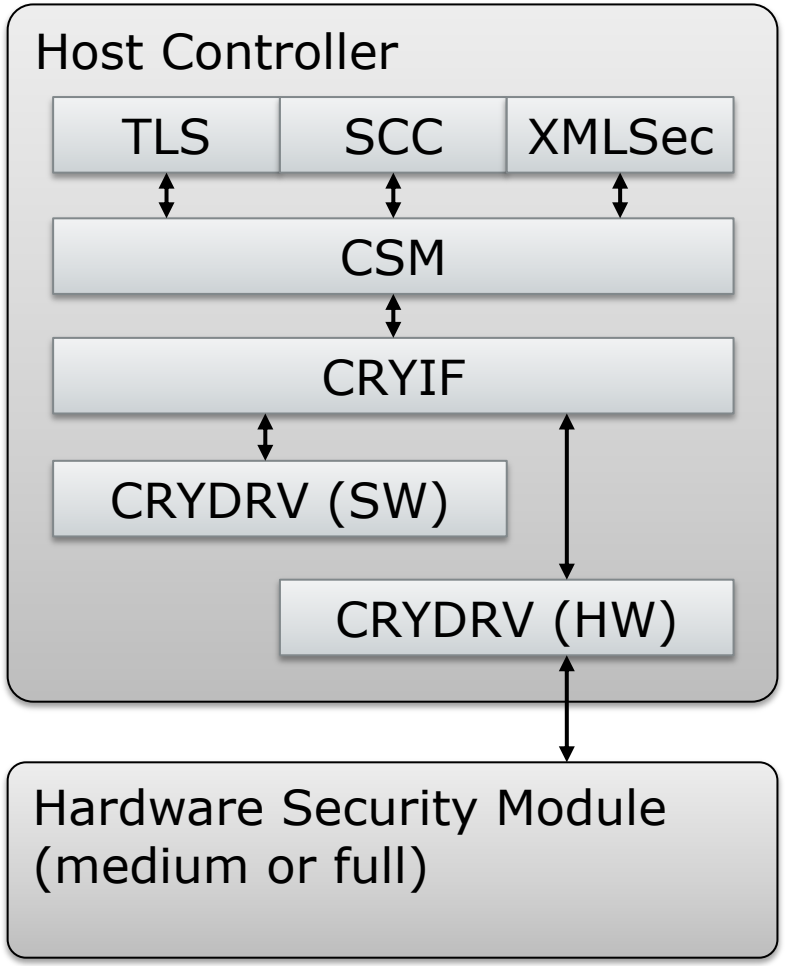
ISO/IEC 15118 - Certificate Usage

ISO/IEC 15118 - Impact on Embedded Systems

Outlook

AUTOSAR 4.3 Security Architecture

- Crypto Service Manager - CSM
  - SWCs use CSM through RTE
  - BSW/CDDs use CSM by inclusion
  - CSM provides job queueing
- Crypto Interface – CRYIF
  - Supports dispatching of security jobs to HW or SW crypto drivers
- Crypto Driver – CRYDRV
  - Implementation of cryptographic functions
  - Either in SW or HW (HTA)

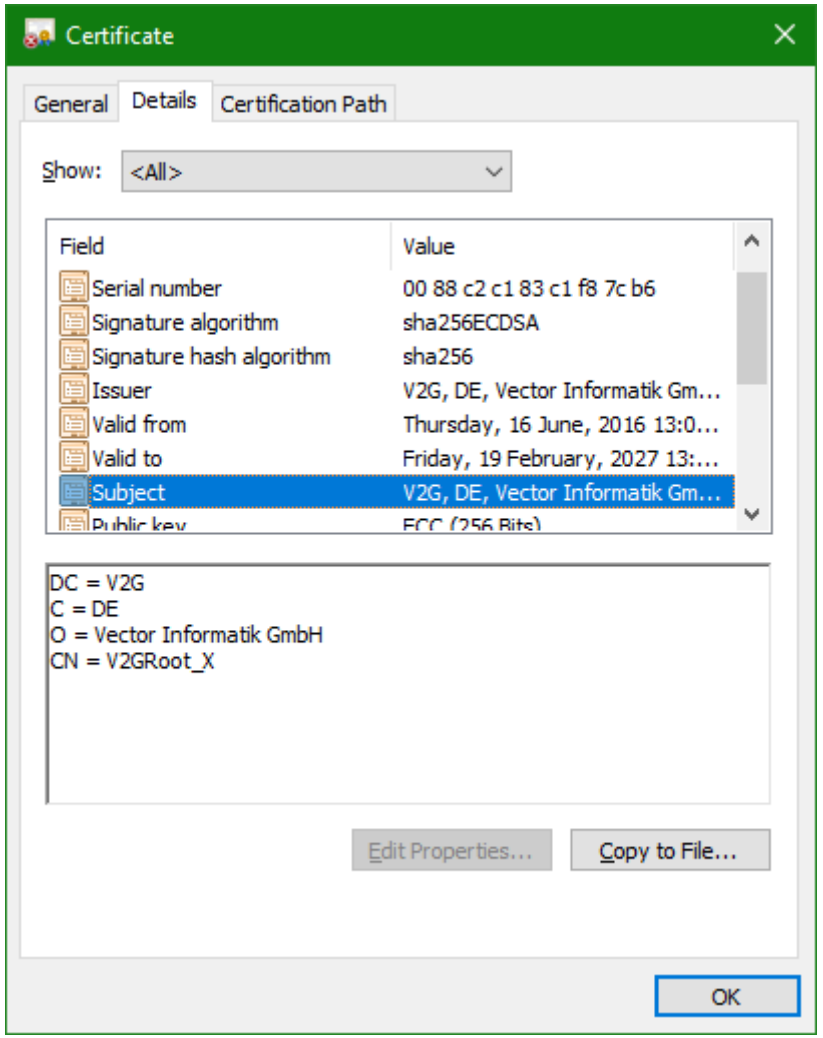


Agenda

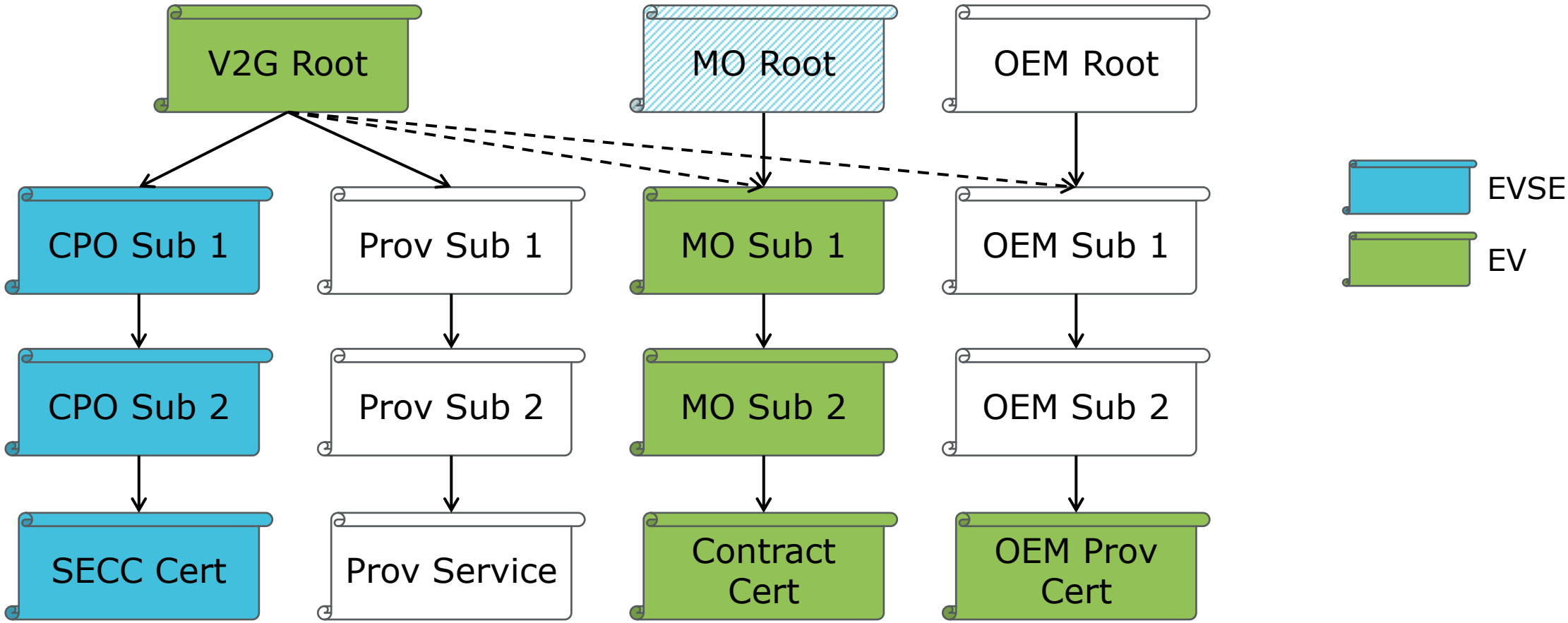
- Hardware Trust Anchors - General Introduction
- Hardware Trust Anchors - Utilization within AUTOSAR
- **ISO/IEC 15118 - Certificate Usage**
- ISO/IEC 15118 - Impact on Embedded Systems
- Outlook

Introduction

- X.509 is an ITU-T standard for Public Key Infrastructures
- The following objects are part of the standard
  - Public Key Certificate (Digital Certificate)
    - Proves the ownership and provides information about the owner
    - Public Key belongs to Private Key only known by the owner
  - Attribute Certificate
    - Trustfully assigns additional attributes to the owner of a public key certificate
  - Certificate Revocation List
    - Allows to revoke certain certificates before they have expired
- X.509 certificates are widely used for electronic communication
  - Transport Layer Security (TLS) connections
    - In case the connection protects HTTP data, it's called HTTPS



Public Key Infrastructure



Transport Layer Security (TLS)

- Transport Layer Security (TLS) encrypts the communication between a client and a server

- TLS v1.2 is used with one of the two following cipher suites
  - TLS_ECDH_ECDSA_WITH_AES_128_CBC_SHA256
  - TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256

- Derived requirements to an HSM
  - Support Elliptic Curve Diffie Hellman (ECDH(E))
    - Secure exchange of asymmetric keys over an unprotected channel
  - Support Elliptic Curve Digital Signature Algorithm (ECDSA)
    - Signatures guarantee authenticity and integrity
  - Support Advanced Encryption Standard (AES128)
    - Encrypts the transmitted data using a symmetric key
  - Support Secure Hash Algorithm 2 (SHA256)
    - Hash arbitrary amount of data to fixed length

Installation and Update of Certificates

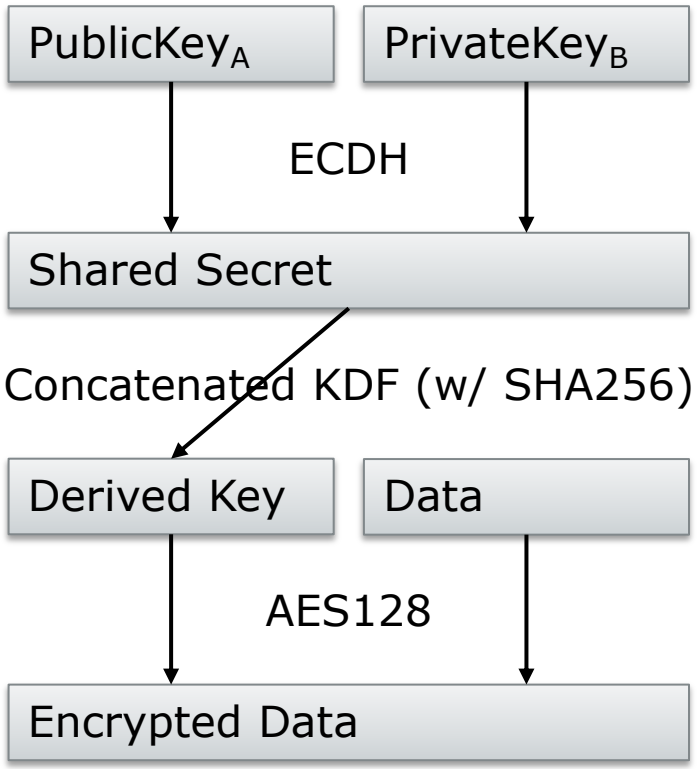
- Certificates installed during production, possibly without using cryptographic operations
  - V2G Root Certificate(s)
  - Provisioning Certificate, incl. its Private Key
- Certificates installed in public space need to be protected using cryptographic operations
  - Contract Certificate(s), incl. Private Key(s)
  - Contract Sub Certificates

- Contract Certificate Chain may be installed by mechanism defined in ISO/IEC 15118
  - Certificate Installation
    - EV uses OEM Provisioning Certificate to receive new Contract Certificate Chain
  - Certificate Update
    - EV uses current Contract Certificate Chain to receive new Contract Certificate Chain

Certificate Installation

- Public Key of A together with Private Key of B leads to same secret as Public Key of B together with Private Key of A
- Concatenated Key Derivation Function (KDF) reduces risk of brute force attacks
- Derived Key is used to encrypt provided data (Private Key of Contract Certificate) with AES128

- Derived requirements to an HTA (additional to TLS)
  - Support Concatenated Key Derivation Function
  - Accept externally created Private Keys
    - Being provided in an encrypted format



Agenda

- Hardware Trust Anchors - General Introduction
- Hardware Trust Anchors - Utilization within AUTOSAR
- ISO/IEC 15118 - Certificate Usage
- **ISO/IEC 15118 - Impact on Embedded Systems**
- Outlook

Runtime

- Without an HTA, cryptographic operations need to be calculated with SW library
  - In case SW library is synchronous, ECU will block for the time the operation takes

- ECDSA signature generation on an MPC5668G@116Mhz
  - 204ms without cache and jump prediction
  - 102ms with cache and jump prediction

- Typical task periods are 5 to 20 milliseconds
  - Issues with watchdog will occur
  - CAN may not work properly without proper prioritization and preemption in OS

- Problems can be avoided by using an HSM (full)
  - ECDSA signatures can be generated/validated on HSM's own core
  - HSM may not be faster, but host controller can continue its execution normally
    - HSM processes cryptographic operations asynchronously and reports back when done

Storage of Certificates

- Certificates and their Private Keys have to be stored non-volatile
- Cars parking in public space could be accessed by attackers
  - ➜ Attacker readouts Certificate and Private Key and charges “for free”

- HTAs protect memory, so only authorized persons can access Certificates and Private Keys

Agenda

- Hardware Trust Anchors - General Introduction
- Hardware Trust Anchors - Utilization within AUTOSAR
- ISO/IEC 15118 - Certificate Usage
- ISO/IEC 15118 - Impact on Embedded Systems
- **Outlook**

VECTOR

Current Situation and Future Developments

- Demands on the security increases
  - Cars are opening up to the outside world and are vulnerable for attacks
  - Stronger security requires more powerful hardware, such as HSM (full)

- Availability of HSM (full) is currently low
  - Use cases like ISO/IEC 15118 or Firmware Over-the-Air (FOTA) drive the demand
  - Availability of HSM (full) will increase in the near future

- Working PKI of ISO/IEC 15118 doesn’t exist yet
  - Architecture of a possible PKI is currently being developed
  - Introduction of inductively charging vehicles speeds up the process
  - PKI for ISO/IEC 15118 should be available in the near future

- Testing of Implementation possible during Testing Symposium events
  - http://testing-symposium.net/

Your questions are welcome!

Visit us at our stand @ G61

Author:
Eisele, Fabian
Vector Germany

Certificate Installation

- Vehicle sends its OEM Provisioning Certificate to Charging Station incl. a list of the installed root certificates.
- Charging Station forwards this information to a Secondary Actor (SA) which then provides a Contract Certificate chain incl. private key
- The parameters are validated using the SAProvisioningCertChain
- The private key of the new Contract Certificate is decrypted using the private key of the Provisioning Certificate.