AUTOSAR 4.4 Security Enhancements

Automotive Security Meets Functional Safety Symposium 2018
Overview

Security Extensions
Importance of cryptographic material
Vehicle key management != key storage
Challenges for standardization
Example: Initial keying at OEM for SECOC
Status of standardization
Summary
Goals of AUTOSAR 4.4 Security Extensions

With AUTOSAR 4.3 major improvements in the AUTOSAR security stack have been specified. Furthermore the SECOC module was improved for more flexible handling of the freshness value. However experience from projects shows that the following extensions to the current security modules are required.

- C1: Security Event Memory
- C2: Key Management / Key Distribution
- C3: Secure Boot Status (dropped)
- C4: Authentic Synchronized Time
- C5: Dynamic Rights Management for Diagnostic Access
- C6: Improved Certificate Handling (integrated in C2)
- C7: Abstract pre-definition of Crypto Items in System Template (improves AUTOSAR tooling support for security)
Overview

- **Security Extensions**
  - Importance of cryptographic material
  - Vehicle key management ≠ key storage
  - Challenges for standardization
  - Example: Initial keying at OEM for SECOC
  - Status of standardization
  - Summary
Goal:
The Security Event Memory (SEM) manages records that provide *documentary evidence* of security-relevant events.

Basic Functions and Key Aspects:
- Security-relevant events can be recorded together with *context data* such as event-type, event counters, time stamps and suspicious data.
- Optionally the SEM records can be protected by a *hardware trust anchor* to detect or prevent tampering.
C2: Key Management / Key Distribution

- **Goal:**
  - Simplifies typical and common key lifecycle management tasks.

- **Basic Functions and Key Aspects:**
  - Receives new *cryptographic material* (keys, certificates) via diagnostic routines.
  - Verifies authenticity, integrity and freshness of cryptographic material.
  - Provides callouts to integrate with business logic for different typical *key lifecycle phases* (production, initialization, update, repair, replacement).
  - Supports on board *derivation* of new keys.
  - Supports secure *distribution* of shared secret keys.
  - Logs security events to *security event memory (SEM)*.
Goal:
- Several security mechanisms require a trusted time source that is synchronized between several nodes

Basic Functions and Key Aspects:
- The Global Time Master receives a Global Time-Base start value from a trusted external source via diagnostic routines.
- All certificate users shall validate the expiration time of the current received certificate against the Global Time.
- Synchronizes the Local Time-Base reference of a Global Time-Base in a tamper-proof way between different in-vehicle nodes, for example for Freshness Value Management of Secure On-board Communication (SecOC).
- Provides authenticated Time-Bases for Security Event Memory (SEM) and Crypto Service Manager (CSM).
- Logs Global Time related security events to Security Event Memory (SEM), e.g. unauthorized access to secure Time-Bases.

C4: Authentic Synchronized Time
Goal:
Currently diagnostic access can be secured by statically defining security levels which are protected via a challenge response protocol. To achieve more flexibility, it shall be possible to dynamically define access rights for diagnostic access which are evaluated by the diagnostic policy manager (DPM).

Basic Functions and Key Aspects:
- Certificates shall be used for authentication of the diagnostic tester to the vehicle. Optionally bidirectional authentication shall be possible. For this purpose, the 0x29 service of the upcoming ISO-14229-1 shall be supported
- The certificates shall support the definition of user roles which gain predefined access rights
- Beyond role based access rights it shall be possible to define individual (“white list”) access rights via certificates
- Security events shall be reported to the SEM
C6: Improved Certificate Handling

- **Goal:**
  - Certificates play a major role in security concepts. Support for **certificate handling** by the AUTOSAR crypto stack shall be improved.

- **Basic Functions and Key Aspects:**
  - Provide interfaces to **retrieve basic information** stored in a certificate.
  - Verifying signatures of certificates against a **certificate chain**
  - Usage of a certificates public key and associated private key.
C7: Abstract pre-definition of Crypto Items in System Template

Goal:
- On design level (SysT, SWC) it is currently not possible to define key parameters and crypto services and jobs. This should be improved to allow crypto to be handled according to the AUTOSAR design process.

Basic Functions and Key Aspects:
- Allows to **pre-define jobs** and their parameters.
- Define key slots and parameters that can be assigned to jobs.
Overview
Security Extensions

- Importance of cryptographic material
  Vehicle key management ≠ key storage
  Challenges for standardization
  Example: Initial keying at OEM for SECOC
  Status of standardization
Summary
For security reasons **different keys** are used for different security related use cases, e.g.

- Secure flashing of ECUs (a.k.a code signing, secure reprogramming)
- Secure boot of ECUs
- Diagnostic access control
- Secured communication between the ECUs of a vehicle (e.g. via SECoC)
- Secure communication from the ECU to external services (e.g. via TLS)
- SW update over the air (SOTA)
- Remote feature activation
- Component theft protection
- Immobilizer
- Mobile online services
- ...

The affected ECUs require a **considerable number of cryptographic keys**
Overview
Security Extensions
Importance of cryptographic material

- **Vehicle key management != key storage**

Challenges for standardization
Example: Initial keying at OEM for SECOC
Status of standardization
Summary
Vehicle key management != key storage

Vehicle key management in a layered security concept

Security concepts

- Secure communication to services outside the vehicle
- Intrusion detection mechanisms
- Diagnostic Policy Manager
  - **Vehicle Key Management**
  - Security Event Memory
  - Authentic synchronized time
- Authenticity of messages
- Integrity and freshness of messages
- Confidentiality of messages
- **Key storage**
  - Secure boot and secure flash
  - Crypto library
  - HW trust anchor (HTA)
Vehicle key management != key storage

**Key storage**

- **Goal:**
  - Securely store cryptographic keys

- **Basic Functions and Key Aspects:**
  - Take a cryptographic key from the application
  - Securely store it in NVM or hardware trust anchor of ECU

- **Supported by the crypto stack (CSM, CRYIF, CRYPTO)**
  - Configuration of key structures via key elements
Overview
Security Extensions
Importance of cryptographic material
Vehicle key management != key storage

**Challenges for standardization**
Example: Initial keying at OEM for SECOC
Status of standardization
Summary
Challenges for standardization

Key lifecycle phases

Production of the ECU
- Insertion of initial keys

End of line programming
- Replacement of initial keys by OEM specific master keys
- Insertion of additional keys
- On board derivation of further keys
- Secure distribution of keys in the vehicle network

Aftersales
- Keys can be replaced if they have become compromised
- Keys can be renewed after a certain time to improve security
- Additional keys can be inserted for new use cases
- Replaced ECUs can get appropriate keys to participate in secure vehicle communication
Challenges for standardization

Variation points for technical solution

- Development-, production-, after sales **processes @ Tier1 & OEM**
- Existing **backend** key management processes and IT infrastructure (e.g. PKI)
- Security goals (based on assumptions about the security of the development / production / service environment)
- Performance goals (based on end of line programming requirements)
- Vehicle **security architecture** / vehicle key management paradigm
  - Central key security manager: derives / generates and distributes keys
  - No central key security manager: Keys are mostly generated in the backend and inserted on the ECUs

→ Current situation: Vector provides **proprietary solutions** to support a large number of different OEMs

Goal for standardization: find right level of abstraction
- to provide added value compared to proprietary solutions
- Support known OEM specifics via configuration and extension interfaces
Overview
Security Extensions
Importance of cryptographic material
Vehicle key management \(\neq\) key storage
Challenges for standardization

- **Example: Initial keying at OEM for SECOC**

  Status of standardization

Summary
Scenario 1: Offboard (Backend) key derivation

- Diagnostic Tester provides backend generated keys to each node
- Key managers are limited to validating backend generated SEOC keys (e.g. via SHE update protocol)
Scenario 2: On-board key derivation with coordinator

Example: Initial keying at OEM for SECOC

- Diagnostic Tester triggers SECOC keying
- Server creates and stores vehicle specific secret
- Coordinates secure distribution of secret to client
- Clients use secret and key derivation function to securely derive SECOC keys
Scenario 3: On-board key generation without coordinator

Example: Initial keying at OEM for SECOC

- Diagnostic Tester triggers SECOC keying
- No dedicated server which coordinates key negotiation
- All nodes participate in negotiation of a shared secret from which SecOC keys are derived
Agenda

Overview
Security Extensions
Importance of cryptographic material
Vehicle key management ≠ key storage
Challenges for standardization
Example: Initial keying at OEM for SECOC

- Status of standardization

Summary
Vehicle key management in a layered security concept

**Security Concepts**

- Secure communication to services outside the vehicle (TLS)
- Intrusion detection mechanisms
- Diagnostic Policy Manager
- Vehicle Key Management
- Security Event Memory
- Authentic synchronized time
- Authenticity of messages
- Integrity and freshness of messages
- Confidentiality of messages
- Key storage
- Secure boot and secure flash
- Crypto library
- HW trust anchor (HTA)

**Standard**

- AUTOSAR4.4
- Security Extensions AUTOSAR4.4
- SECOC
- CSM / CRYIF / CRYPTO
- SHE, HSM, TPM, TEE,...
Status of standardization

Timeline 2018

**MS2 Criteria**
- Features, use cases and technical approach are agreed among all stakeholders
- Solution is described on requirement level
- Impact analysis completed

**MS3a Criteria**
- Technical solution is detailed out on specification level (C&P readiness)
- Validator, doc owner and WP review findings are considered in the concept

**MS3b Criteria**
- Technical solution is validated
- Validation results are considered in Concept
- Concept is ready for incorporation

**MS4 Criteria**
- Concept is incorporated
- Successful incorporation is confirmed by Lead-WPs and concept owner

**Timeline**
- **Conc. Review**
  - Call for Review MS3a
- **Valid. Review**
  - MS3a
- **Validation**
  - MS3b
- **Incorporation**
  - MS4 Release 4.4
Summary

Key Points

- **Standardization** has a lot of potential for cost saving but **is challenging due to OEM specifics**
- AUTOSAR is adapting to new security needs
- **Vehicle key management != key storage**
- Secure management of cryptographic keys in all lifecycle phases adds an important **layer of security**

Outlook:

- Security Extensions will be continued in **AUTOSAR 4.5**
For more information about Vector and our products please visit

www.vector.com

Authors:
Dr. Eduard Metzker, Jason Learst
Vector Germany, Vector North America