Vector Cyber Security Solution – vHSM Firmware

MICROSAR.HSM – Optimized and Flexible Software for Hardware Security Modules
Agenda

- Overview
  - Cryptographic Solutions
  - MICROSAR.HSM - Features
  - MICROSAR.HSM - Architecture
  - MICROSAR.HSM - Integration and Workflow
  - Summary
Cyber Security in Automotive

Cyber security gains increasing importance in automotive industry due to highly connected vehicles and accessible customer interfaces. Vehicles become a part of the internet of things. Therefore, highly complex algorithms have to be executed efficiently in an isolated portion within the ECUs. A secure storage for cryptographic secrets is needed as well.

At this, a hardware security module including its software is used to provide necessary performance and isolation with appropriate small footprints.
Layered Security Concept – Defense in Depth

Overview

Secure External Communication
- Intrusion detection mechanisms
- Firewalls
- Key Infrastructure / Vehicle PKI
- Synchronized secure time
- Secure communication to services outside the vehicle via TLS

Secure Gateways
- Message authentication codes (MAC)
- Freshness to ensure integrity of messages
- Encryption to ensure confidentiality of messages

Secure In-Vehicle Communication
- Secure key storage
- Secure boot and secure flash
- Crypto algorithm library
- HW trust anchor (HTA)
  - E.g. Hardware Security Modules (HSM)

Secure Platform
Overview

Security Mechanisms allocated in Example Architecture
MICROSAR.HSM: vHSM – What it actually is and does.

- Cryptographical services on secure core with isolated memory
- Large library of crypto algorithms
  - Crypto Basic functions (hash, random numbers)
  - Message authentication code (HMAC, CMAC)
  - Symmetric and asymmetric crypto algorithms
- Providing secure key storage, update and handling
- Supporting signature generation and verification
- Providing secure boot protocol
- Supporting hardware acceleration for better performance

- Modular architecture with extensive configuration space
- Adaptable HSM firmware to match use case requirements and footprint
- Comprehensive configuration tool DaVinci Configurator

vHSM is an efficient and flexible firmware for hardware security modules that is adaptable to your use case in order to improve cybersecurity.
Agenda

Overview

- **Cryptographic Solutions**
  - MICROSAR.HSM - Features
  - MICROSAR.HSM - Architecture
  - MICROSAR.HSM - Integration and Workflow
  - Summary
Cryptographic Solutions

Pure Software Approach

- Executing cryptographic algorithms in software
- No hardware support / acceleration possible
- No isolated secure core or memory available
- May occupy many CPU resources (CPU time)
- Code size and speed highly depends on the microcontroller
Cryptographic Solutions

Based on Crypto Peripheral

- Accelerating cryptographic algorithms in crypto peripheral
- Hardware support / acceleration possible
- No isolated secure core or memory available
- Secrets and application data in same memory
- No updates of crypto hardware are possible
Cryptographic Solutions

Hardware security module (HSM)

- HSM design objectives
  - Harden ECUs against SW and selected HW attacks
  - Provide HW acceleration for crypto functions

- EVITA HSM profiles
  - HSM full:
    > Support strong authentication (e.g. via RSA, ECC)
    > Support complex block ciphers
    > High performance, updateable
  - HSM medium:
    > Secure ECU 2 ECU communication
    > updateable
  - HSM small:
    > Secure critical sensors / actuators
    > Simple block ciphers
    > Low cost modules, not updateable
Agenda

Overview

Cryptographic Solutions

- **MICROSAR.HSM - Features**
  - MICROSAR.HSM - Architecture
  - MICROSAR.HSM - Integration and Workflow
  - Summary
MICROSAR.HSM - Features

Overview vHSM Product Features

Core Features

- (HW accelerated*) Cryptographic basic functions and algorithms
- Streaming of crypto jobs
- Isolated secure key storage
- Secure error log
- Development error handling and debugging
- Customization and extension support

Featured use cases:

- Secure software download and code signing support
- Secure communication support
  - On board (e.g. SecOC)
  - Off board (e.g. V2G)
- Secure boot support

*Depending on available accelerators in HW
Supported Basic Functions and Cryptographic Algorithms

- Basic functions and symmetric crypto algorithms
  - Hash (SHA-256, ...)
  - Random number generation
  - MAC Generate and Verify
    - CMAC
    - HMAC
  - Cipher
    - AES in the modes ECB, CBC, GCM
- Asymmetric crypto algorithms
  - RSA (Generation and Verification of Signatures)
    - PKCS #1 V1.5, PKCS #1 V2.2
  - RSA (Encryption and Decryption)
  - ECDSA (Generation and Verification of Signatures)
    - Ed25519, NIST/ANSI P256 R1, SEC P256 R1, ...
- Key derivation functions (KDF) and key exchange
  - KDF in counter mode
  - Concatenation KDF
  - Key exchange protocol EC-DHE

Example: Encryption and decryption

Example: HMAC for flash programming
Key Storage

- Any Keys can be passed in plaintext and stored inside the HSM
  - Includes symmetric/asymmetric keys and certificates
  - Any other security relevant data (e.g. mileage) can be stored as well in secure storage!

- Key Installation of symmetric keys according SHE 1.1
  - Support of counter handling
  - UID can be read out

- Extensive configuration options:
  - Free choice if a key is stored in flash or only in RAM
  - Keys can be stored redundantly and reset safe
  - Keys are pre-loaded / cached on startup to avoid loading with every use
  - Number of keys only limited by available RAM and data flash of platform
  - Keys can be locked until secure boot has finished
  - Keys can be configured as write once
  - Keys can be persisted immediately or delayed to be able to persist multiple keys at once

Example: Secure key, mileage and SecOC freshness value storage
vHSM Error Log

- vHSM provides an error log, which can be used to log error events which occur on the HSM
- Errors can be written to secure data flash and read out by application
- The maximum number of log entries is configurable
MICROSAR.HSM - Features

Development Error Handling and Debugging

- Reporting of Det Errors on vHSM
  - Can be treated as error and logged
  - Can be forwarded to application
  - Det of vHSM works as proxy of the host DET
    - Errors are forwarded and reported on the host

- For some compilers (e.g. Greenhills / MULTI), trace messages are displayed on the console window if enabled

- Due to source code delivery, vHSM is fully debuggable
Example Use Case: Secure Boot

- Prevent execution of tampered ECU software by means of a chain of trust
- Integrity check is performed at ECU startup
- Each software unit involved in the boot process validates the integrity of the subsequent software unit, forming a chain of trust
- Validation can be done via checking signature / MAC
- Keys and MAC must be stored in a secure area

vHSM supports Secure Boot in:
- Secure key and MAC storage
- Signature / MAC verification
- 1..n secure boot slots with
  - Configurable keys
  - Configurable sanctions
- Configurable performance improvement options
  - Sequential or parallel secure boot
- Isolation of host and secure domains
Agenda

Overview
Cryptographic Solutions
MICROSAR.HSM - Features

MICROSAR.HSM - Architecture
MICROSAR.HSM - Integration and Workflow
Summary
Internal Architecture of the vHSM

- The vHSM firmware consists of vHSM dedicated and Vector standard modules
- Modular and configurable architecture
  - In analogy to AUTOSAR Crypto stack
    - CryIf channels
    - CryDrv driver objects
    - Crypto primitives
    - Keys, key types and key elements
- Communication between host and vHSM is done by IPC / shared memory
- Synchronous and asynchronous job processing supported
- Notification about job completion by polling or interrupts on host side
Internal Architecture of the vHSM

- AUTOSAR 4.3 BSW
- SWC / Application
  - RTE
  - SYS
  - COM
  - OS
- MCAL
- Crypto(vHSM)

Microcontroller
- Flash Bootloader
- RAM
  - HSM Channel
  - HSM Channel
  - HSM Channel
  - HSM Channel

vHSM
- vHSM KeyM
- vHSM Crypto
- vHSM Custom
- vHSM Secure
- vHSM Job Processor
- vHSM Hardware Accelerator
- vHSM Secure Boot and Update Support

Application core subsystem
- Shared memory
- HSM subsystem

Vectors
Agenda

Overview
Cryptographic Solutions
MICROSAR.HSM - Features
MICROSAR.HSM - Architecture

MICROSAR.HSM - Integration and Workflow

Summary
MICROSAR.HSM - Integration and Workflow

Configuration of vHSM: Synchronization

- Comprehensive configuration with DaVinci Configurator Pro
- DaVinci Configurator Pro provides pre-config file to sync vHSM configuration with MICROSAR configuration including:
  - Available primitives
  - Available and configured keys

![Diagram showing configuration process]

Generate pre-config file as output

Input as Additional Definitions

*.arxml

- Available primitives
- Available and configured keys
Agenda

Overview
Cryptographic Solutions
MICROSAR.HSM - Features
MICROSAR.HSM - Architecture
MICROSAR.HSM - Integration and Workflow

Summary
MICROSAR.HSM – vHSM Solution

**Summary**

**MICROSAR.HSM – Functionality**

- Cryptographical services on secure core with isolated memory
- Large library of crypto algorithms
  - Crypto Basic functions (hash, random numbers)
  - Message authentication code (HMAC, CMAC)
  - Symmetric and asymmetric crypto algorithms
- Providing secure key storage, update and handling
- Supporting signature generation and verification
- Providing secure boot protocol
- Supporting hardware acceleration for better performance

**MICROSAR.HSM – Configuration**

- Modular architecture with extensive configuration space
- Adaptable HSM firmware to match customer requirements and footprint
- Comprehensive configuration tool DaVinci Configurator

**MICROSAR.HSM – Use Cases**

- Secure boot in combination with flash bootloader
- Secure software update and code signing
- Secure OnBoard Communication (SecOC)

**vHSM** is Vectors solution to improve security by providing an efficient firmware for hardware security modules that is adaptable to your use case.
For more information about Vector and our products please visit

www.vector.com

Author:
Dr.-Ing. Falco Bapp
Dr. Eduard Metzker
Vector Germany