EB‘s security solutions

Roman Iseler
July 27, 2017

EB Tech Day 2017 - Farmington Hills

EB’s security track record

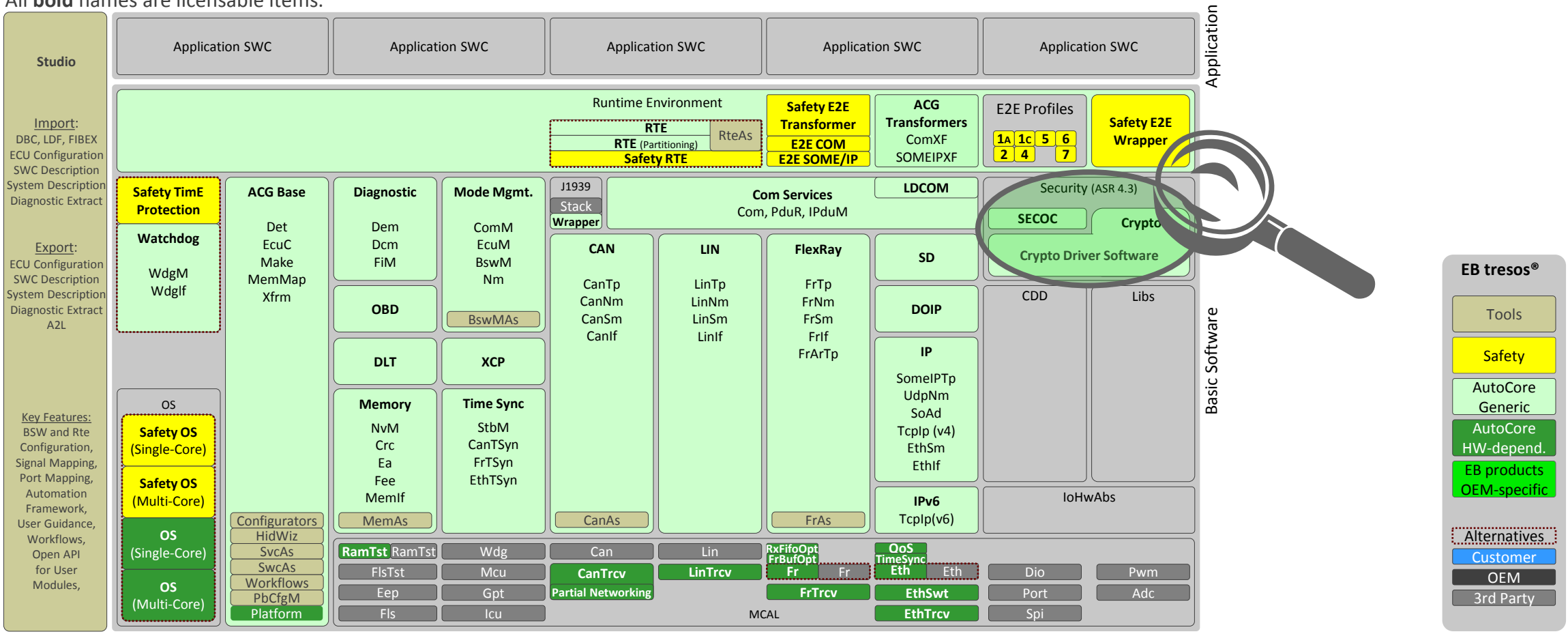
- Mass production approved implementations
- 15 years of experience in the field of embedded security
- EB’s security solutions are on the street in millions of cars
- EB delivered SSW security modules for BMW, Daimler, VW, Audi, Continental
- OEM consulting and project specific security solutions for GM, Renault, Volvo

EB’s security portfolio

- Secure separation
- Crypto
- Secure HW
- Security Consulting
- OTA
- Security applications
- Key management
- Secure Networks
- Testing & Certification
- Car2X
- Role & Rights management

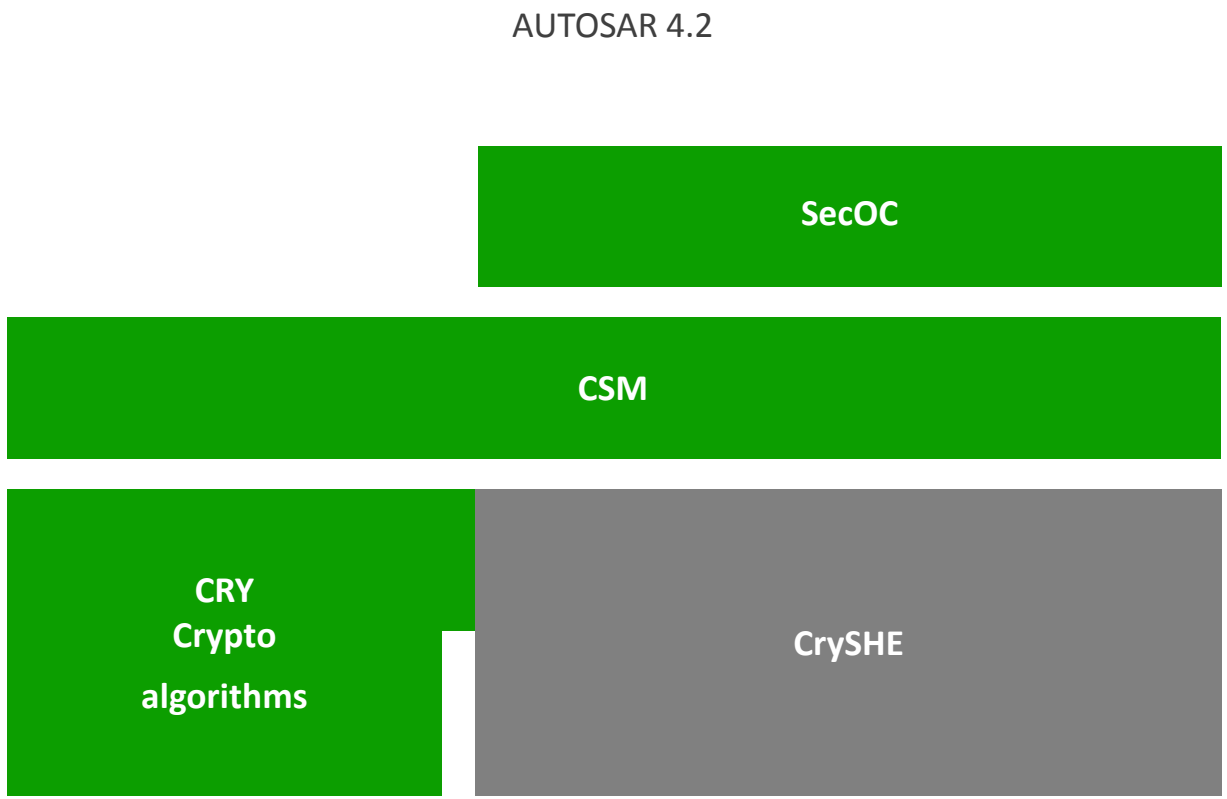
AUTOSAR Architecture – Focus on Security

All **bold** names are licensable items.



New AUTOSAR 4.3 security stack

- **New modules (SecOC, CSM, CryIf, CryptoDrivers)**
- Flexible SecOC freshness value handling on application level
- Optimized support for SecOC
- Single call API (synchronous/asynchronous)
- Added support for cryptographic key handling
- Official support for (multiple) software and hardware drivers
- Parallel job processing in hardware if supported
- Job queueing and priority handling



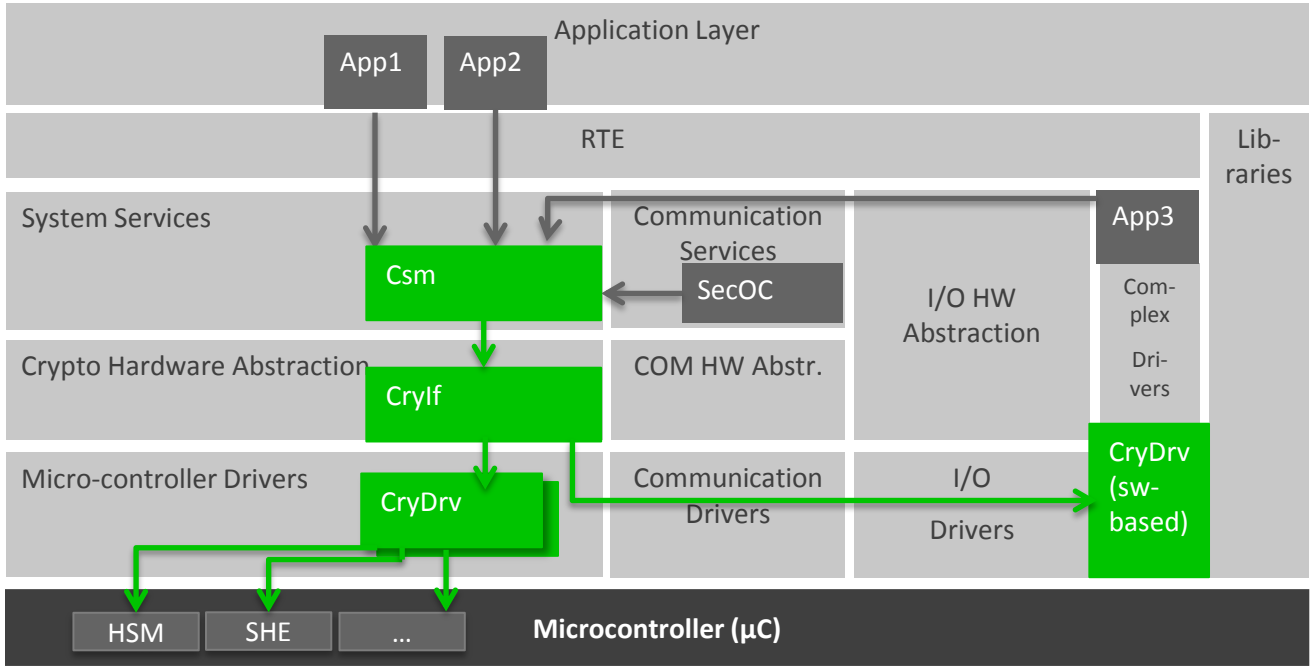
Csm/CryIf/CryDrv

CSM:

- data path is separated from the key management to be able to change the crypto algorithm without modifying the data paths in the application.
- user-concept. multiple independent jobs can be processed in parallel within the CSM.
- prioritized queues to improve performance

Crypto Interface:

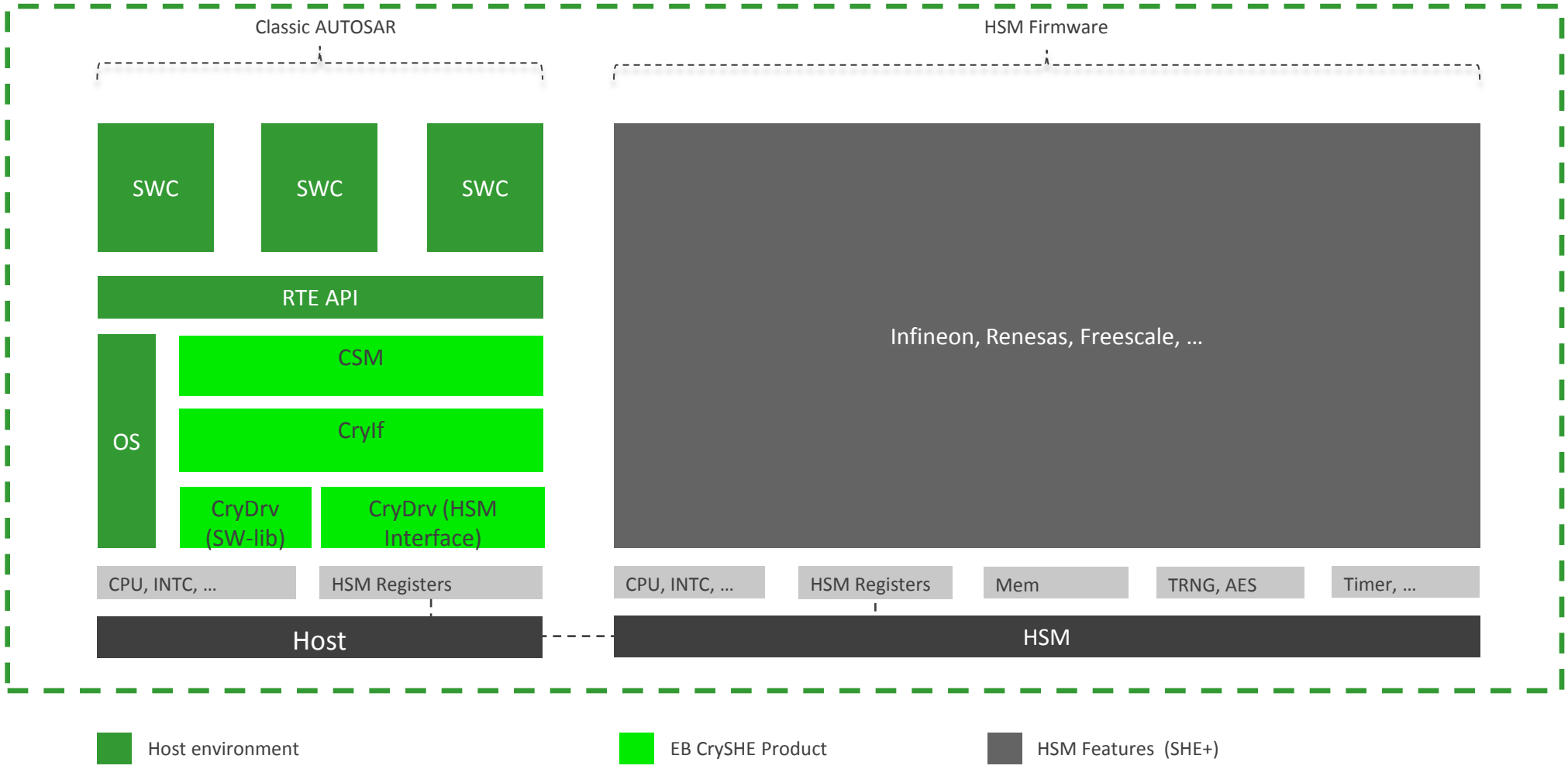
- mapping to a concrete hardware unit or a software library.



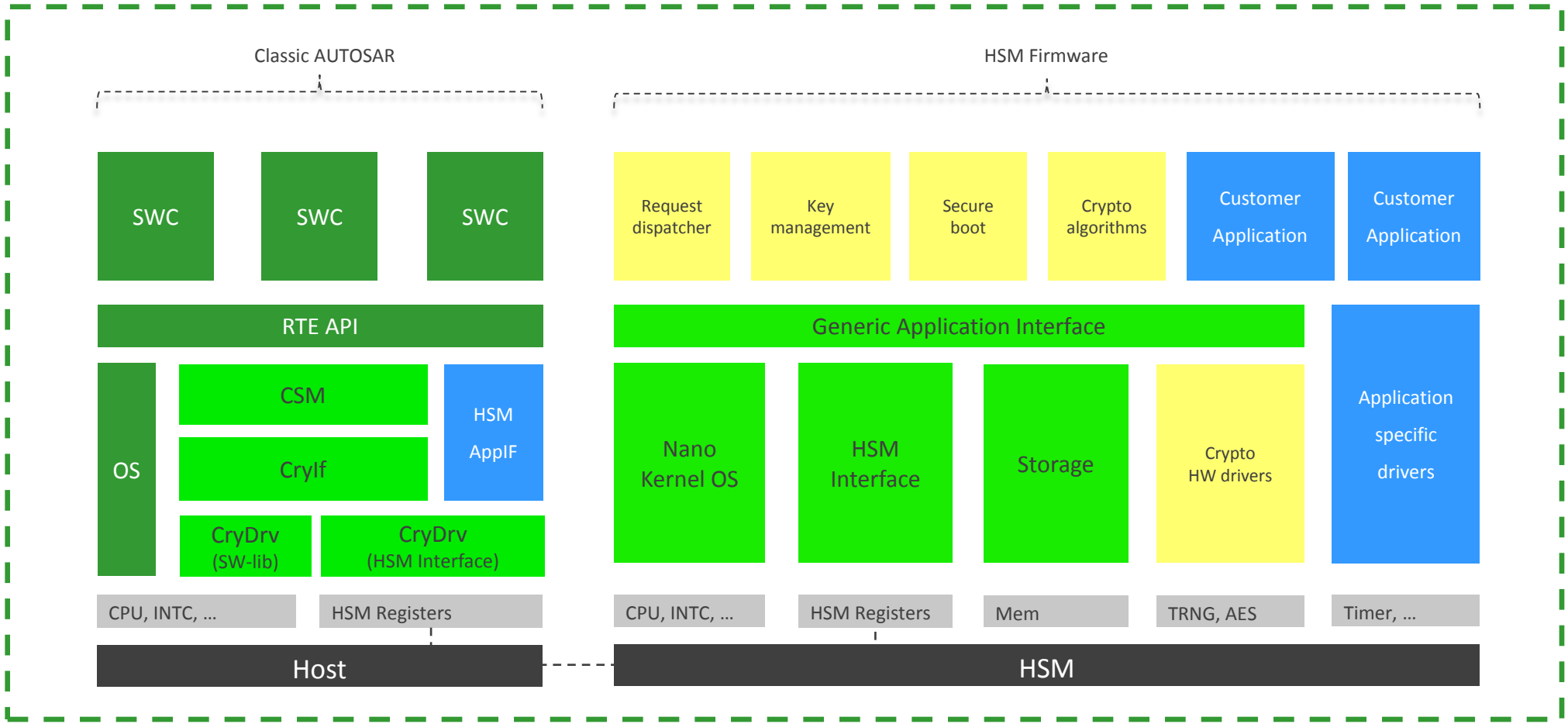
Crypto Driver:

- MCAL BSWMD contains the algorithms supported by the driver/hardware.
- Especially for the HSM features for higher utilization or more deterministic response times.

EB crypto driver for existing 3rd party HSM firmware

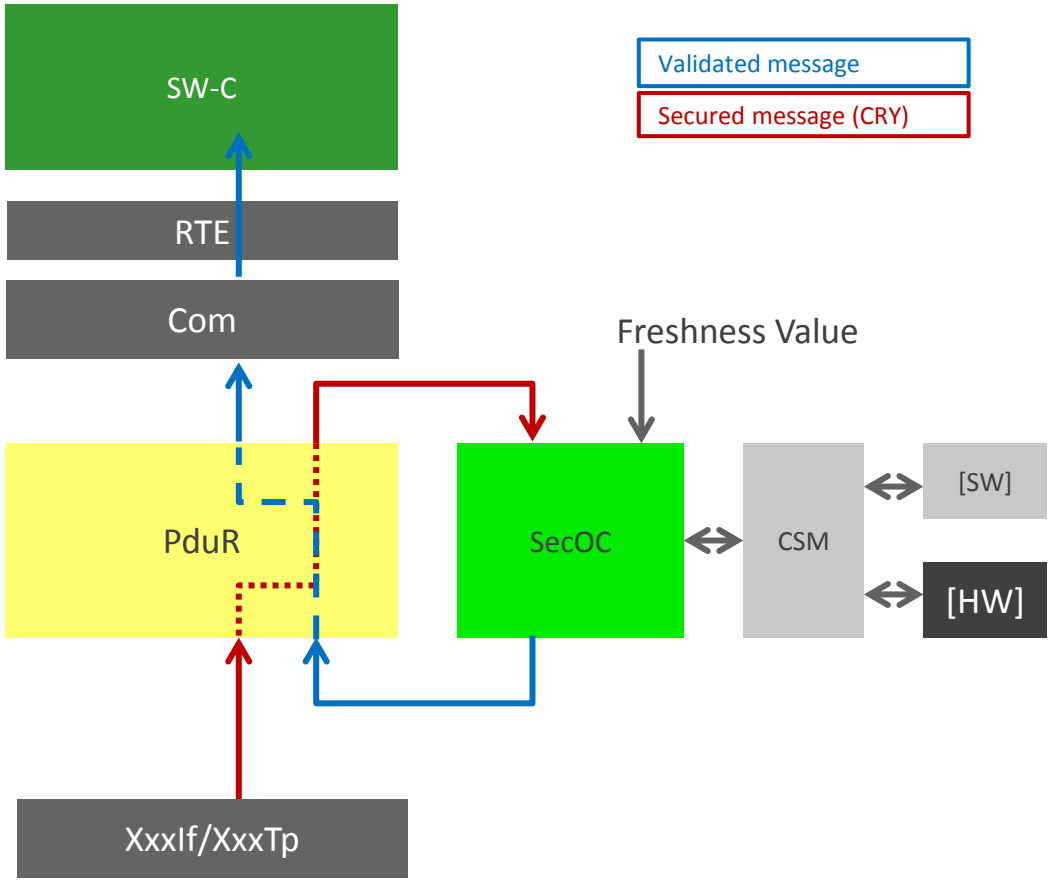


EB trusted HSM software platform architecture



Use case examples – Secure Onboard Communication

- EB is an active member of the AUTOSAR concept group “Secure Onboard Communication - SecOC“
- The concept is part since AUTOSAR 4.2.1
- Main characteristics:
  - Security protection on bus level
  - CMAC with freshness value
  - Protection/Verification on PduR level
  - Independent from Bus or protocol
- Integration with AUTOSAR cryptographic module (e.g. Csm)
- Easy tool driven configuration
- *Latest Evolution – AUTOSAR 4.3:*
  - *Concepts for Freshness Management*
  - *Performance optimizations*
  - *…*



Secure boot

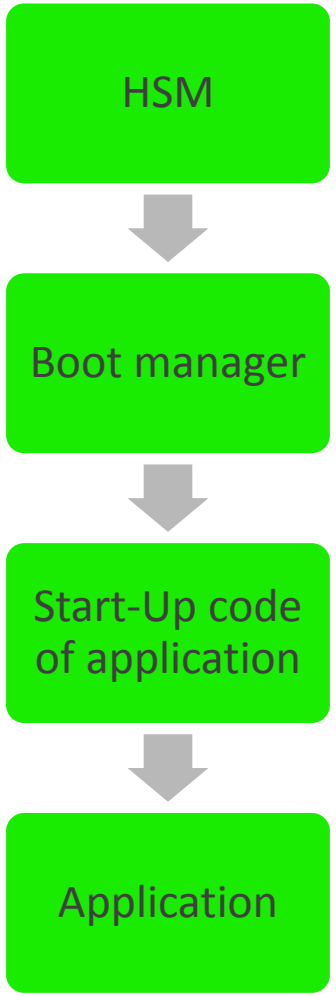
Idea: Verify all SW before it is executed

- Actual sequence depends on your boot strategy

Example: “Secure Boot” component with the following parts

- HSM application to verify the boot manager
- Boot Manager: To verify flash loader and application
- Flash loader verification
- Application verification and error handling (e.g. shutdown)

Cryptography via HSM driver needed for all parts



Secure boot

The big question:

How much boot time do you have left nowadays?

Typical answer:

None

Solution:

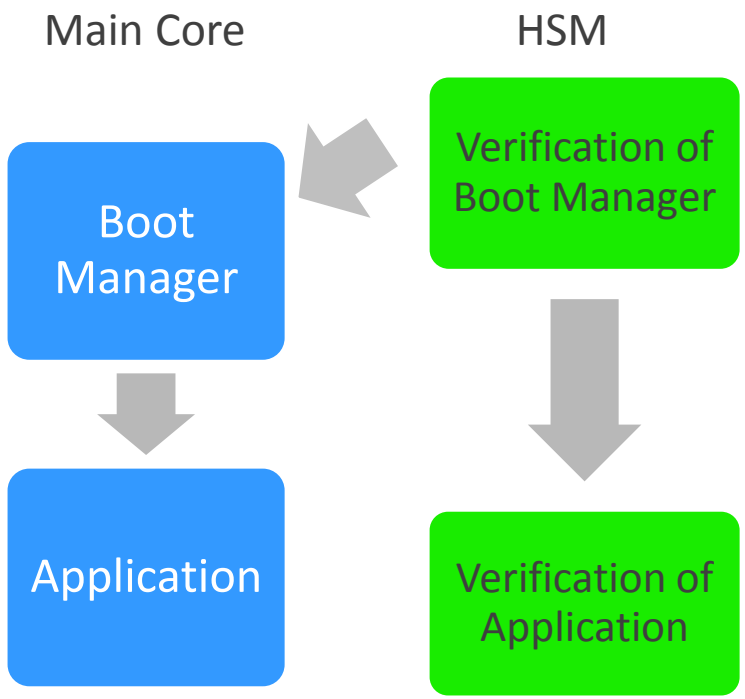
So called parallel or authenticated boot

Boot up your ECU the normal way and do a time shifted verification of the booted SW

Parallel secure boot

This is just one possible sequence:

- “Secure Boot” verification of Boot Manager and Flashloader
- Start of application
- HSM verifies application in parallel
- HSM persistently stores information about previous verification result
- On the next start, HSM inhibits start of application if signature is invalid ➔ Sequential Secure Boot



Cryptography via HSM driver needed for all parts

EB security portfolio

Secure separation
- Hypervisor
- Virtualization

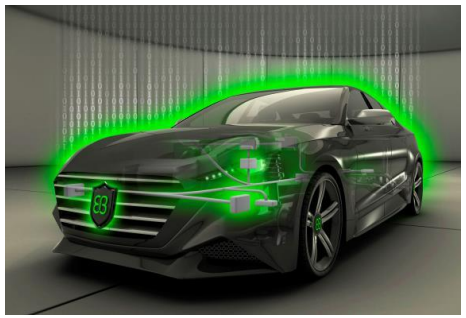
Crypto
- Algorithms
- SHE drivers
- HSM drivers
- Security Processes

Secure HW
- HSM firmware
- Security architecture
- Future Security HW

Security Consulting
- Architecture
- Solutions
- How-To

OTA
- Secure Connection
- Update strategies
- Implementation
- Backend

Role & Rights management
- Identity
- Role
- Rights



Security applications
- Unlock / Download
- SW as Product
- Secure Com

Key management
- Sym/Asym
- Key Derivation
- Initial / Update

Secure Networks
- Firewall
- ADS/IDS/IPS
- Secure network elements (SDN

Testing & Certification
- Functional
- Pen Testing
- FIPS / Com. Criteria

Car2X
- Consulting
- Implementation
- Testing

Thank you.
Get in touch!

Roman.Iseler@elektrobit.com
Product Manager Security
Martin.Boehner@elektrobit.com
Program Manager Security
elektrobit.com/security