Automotive Security

An Overview of Standardization in AUTOSAR

Dr. Marcel Wille

31. VDI/VW-Gemeinschaftstagung Automotive Security

21. Oktober 2015, Wolfsburg

Hacking threat to drivers

Wireless networks let cyber-criminals seize control of cars

THE TIMES

Hackers show how to seize control of a car at 70mph

EXCLUSIVE

Revealed: car key hacking scandal

USA TODAY

Hackers take over steering from smart car driver

NUR 15 EURO MATERIALKOSTEN

Dieses Gerät legt mit einem Klick Ihr Auto lahm!

... und schon haben Fremde Kontrolle über Bremse, Licht, Lenkung

News · World news · Mobile phones

Hackers control car using a mobile phone in eye-opening footage claiming to expose security flaws

Topics

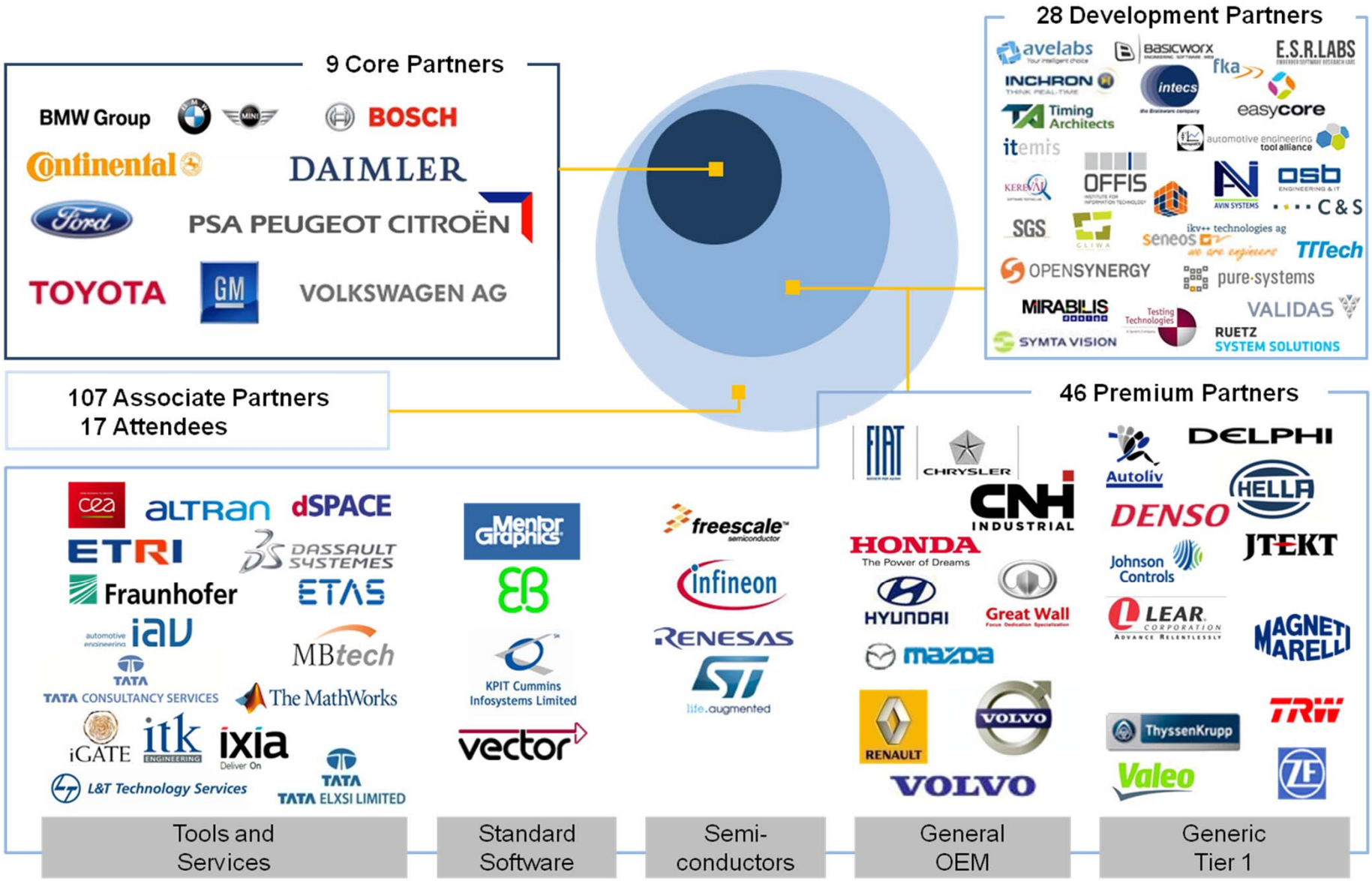
1. Status AUTOSAR
2. Security Features in AUTOSAR
   - Secure on-board communication
3. The AUTOSAR Security Work Package
4. Conclusion and outlook

AUTOSAR – Where we are

- AUTOSAR is the global standard for Automotive SW Architecture.
  - Number of new developments and platforms adopting AUTOSAR is increasing fast
  - More than 200 partners worldwide (July 2015)

- AUTOSAR is on the road:
  - **Millions of ECUs already use AUTOSAR solutions today.**

AUTOSAR – Partners overview

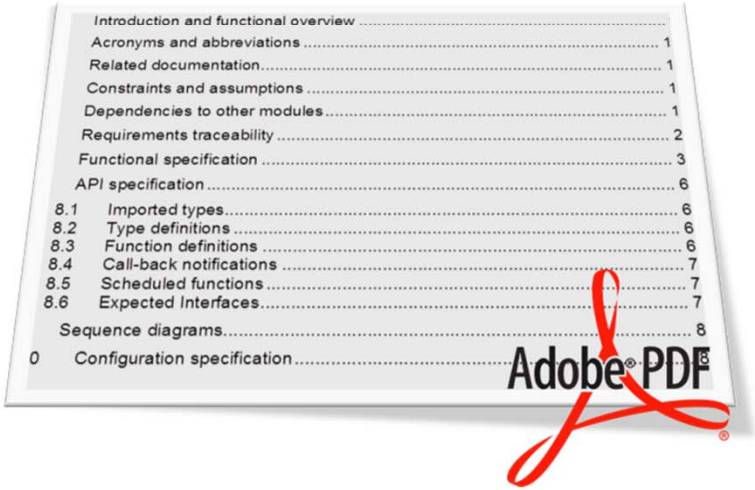


Status: July 2015

AUTOSAR – Some numbers

- **Partnership**
  - More than 250 persons active in technical workgroups
  - More than 70 companies active in the development of the standard

- **Release 4.2.2 size**
  - ~ 19.600 Pages
  - ~ 26.000 Requirements
  - 116 standard specifications
  - 102 auxiliary specifications



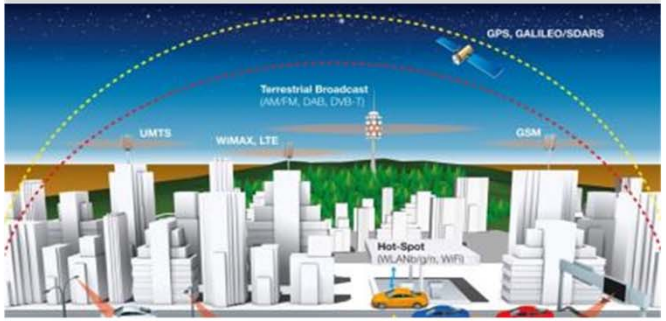
Topics

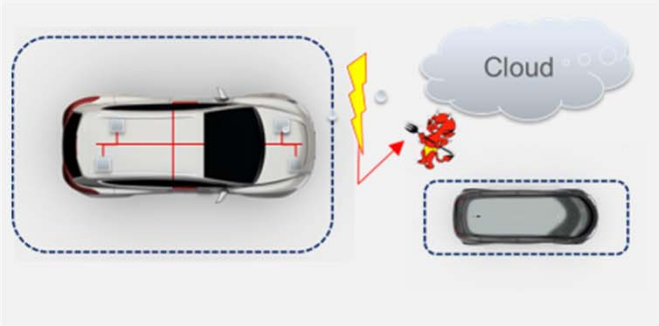
1. Status AUTOSAR
2. Security Features in AUTOSAR
   - Secure on-board communication
3. The AUTOSAR Security Work Package
4. Conclusion and outlook

Selected drivers for security in E/E architectures

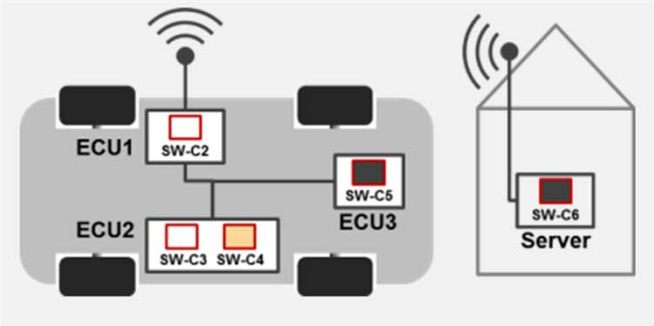
Highly automated driving

Car-2-X applications





Vehicle in the cloud

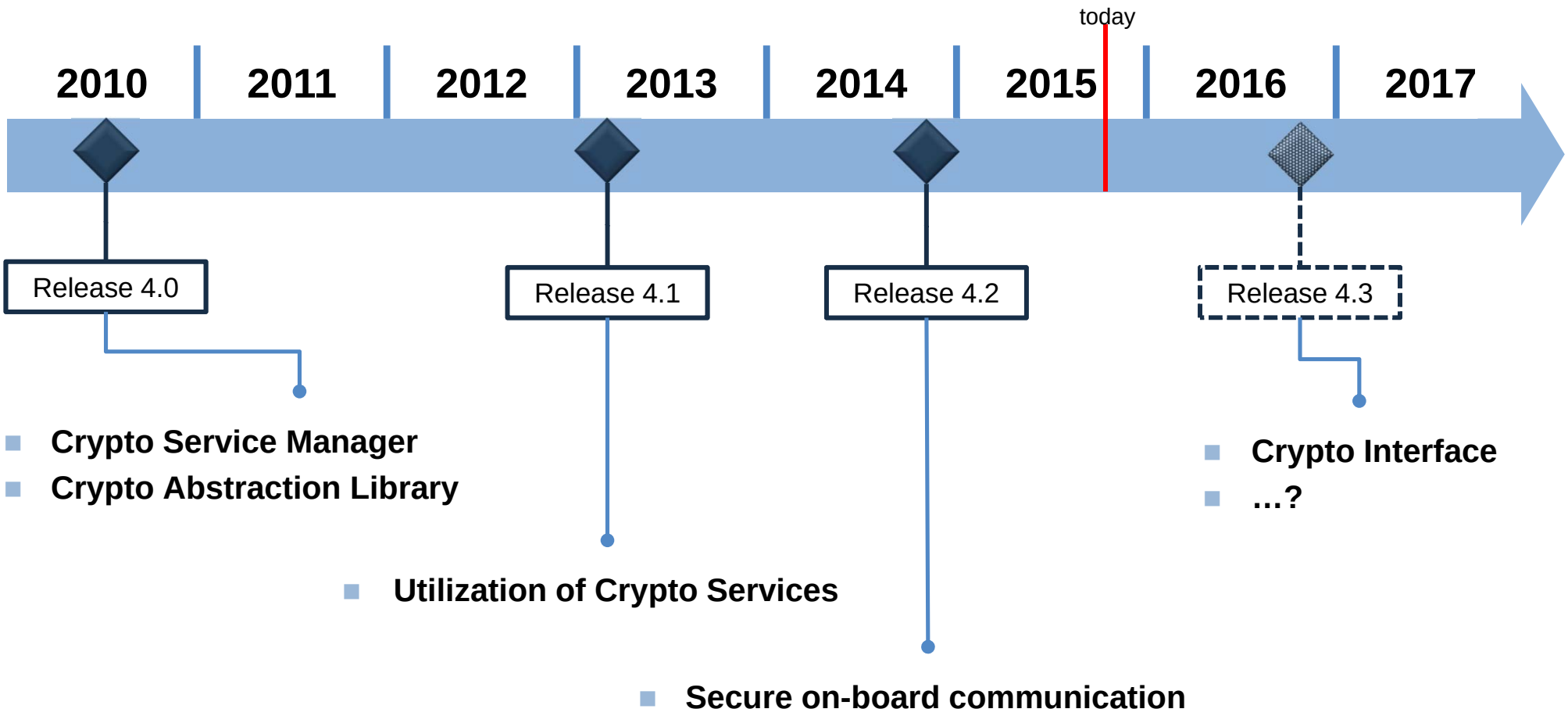


Increased connectivity

- Importance of security demonstrated by attacks on automotive communication systems
- Functionalities are more and more distributed over different ECUs within the car
- Growing need for communication of sensitive content inside the car and to the outside world (cars as part of the internet of things)

Communication & access to the car must be protected against manipulation & must ensure authenticity and message freshness to ensure the trust in new features

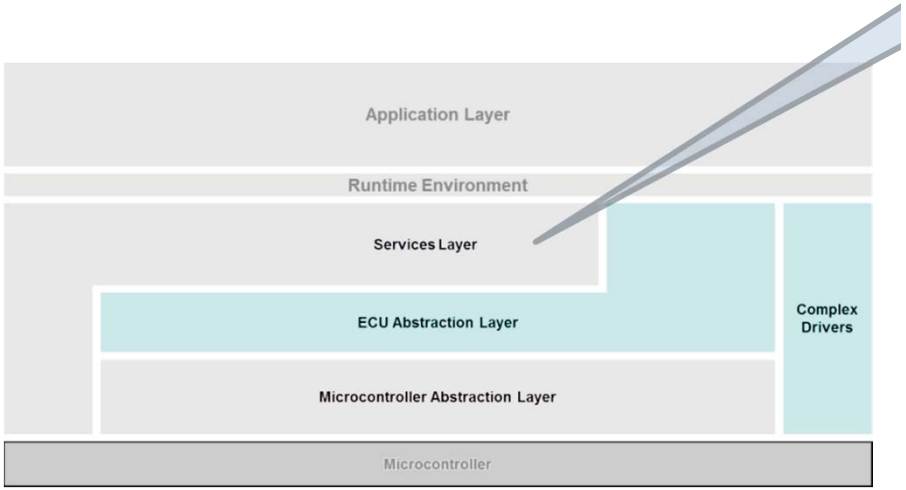
Supported security features by AUTOSAR

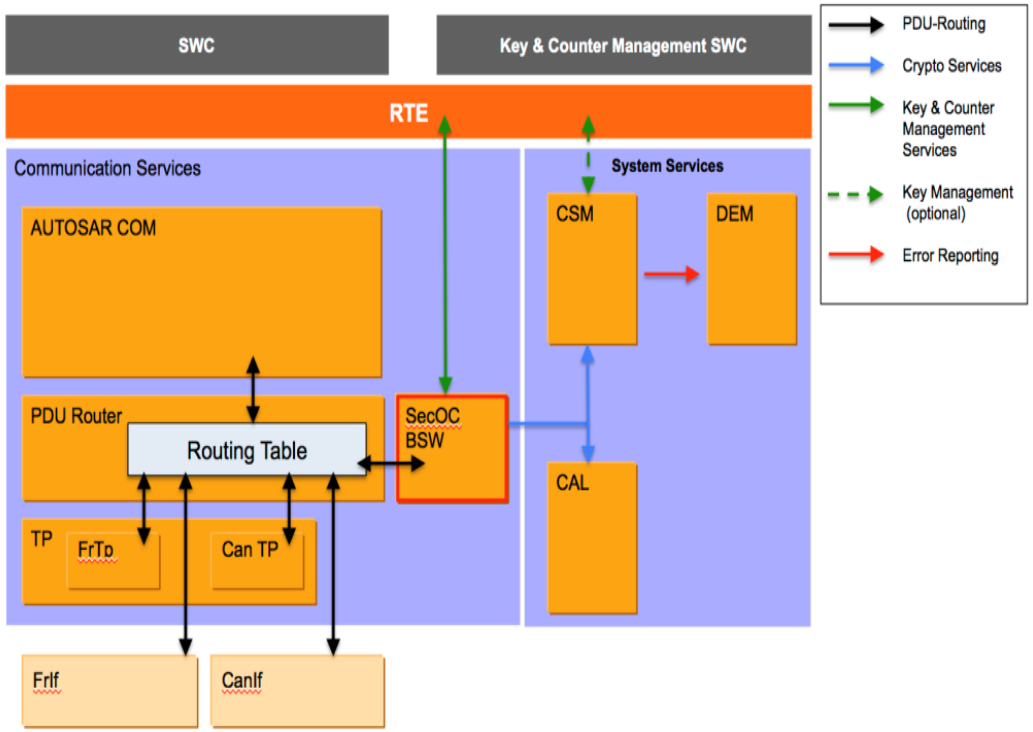


The standard defines procedures and interfaces to secure on-board communication while secrets, calculation algorithms and configuration of the AUTOSAR security software modules remains in the responsibility of the OEM

Security in the current AUTOSAR software architecture

CSM = Crypto Service Manager
CAL = Crypto Abstraction Library
SecOC = Secure On-board Communication

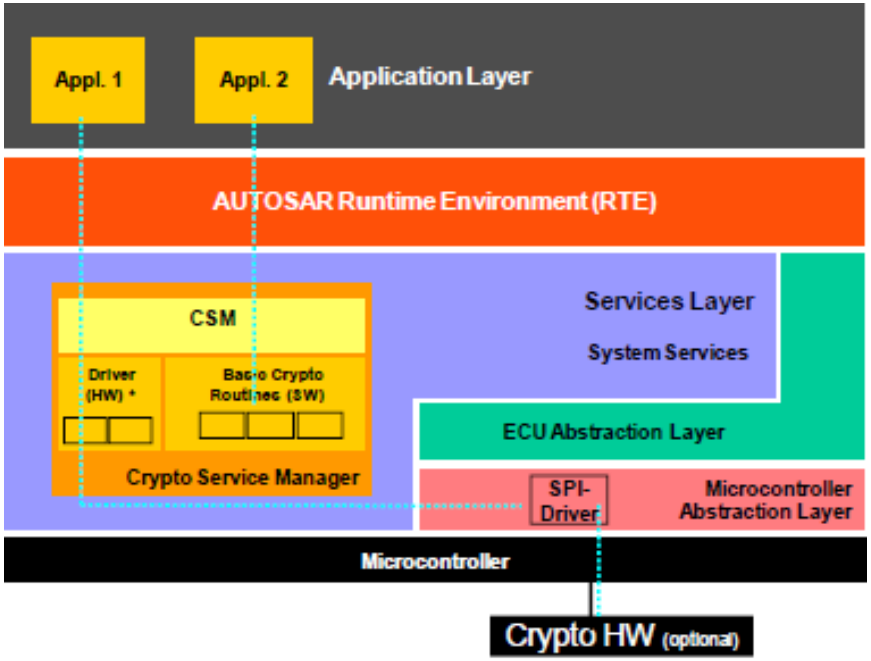




- Standardized interface for cryptographic services
- CSM and CAL define the same cryptographic functionality
- Support for hardware security modules
- Secure on-board communication by using APIs provided by CSM or CAL

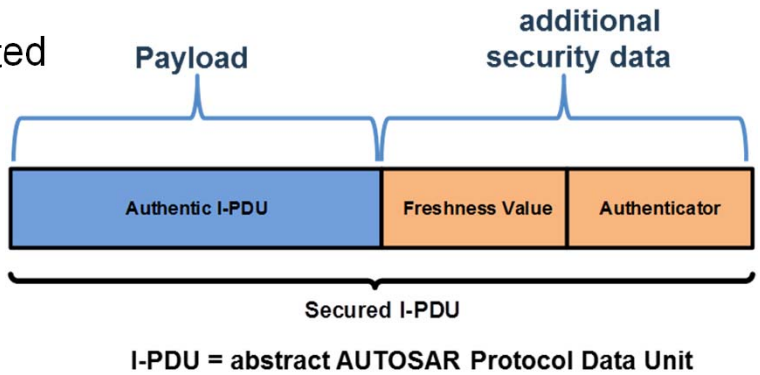
Crypto Service Manager (CSM)

- CSM provides access to cryptography services, based on a software library and/or a hardware module (“crypto library”)
- parallel access to different services possible
- incorporated crypto libraries provides the implementation of cryptographic routines, e.g. MD5, SHA-1, RSA, AES, …
- Supported cryptographic services:
  - Hash calculation
  - Random number generation
  - Generation and verification of message authentication codes
  - Encryption and decryption using symmetrical algorithms
  - Generation and verification of digital signature
  - Key management operations

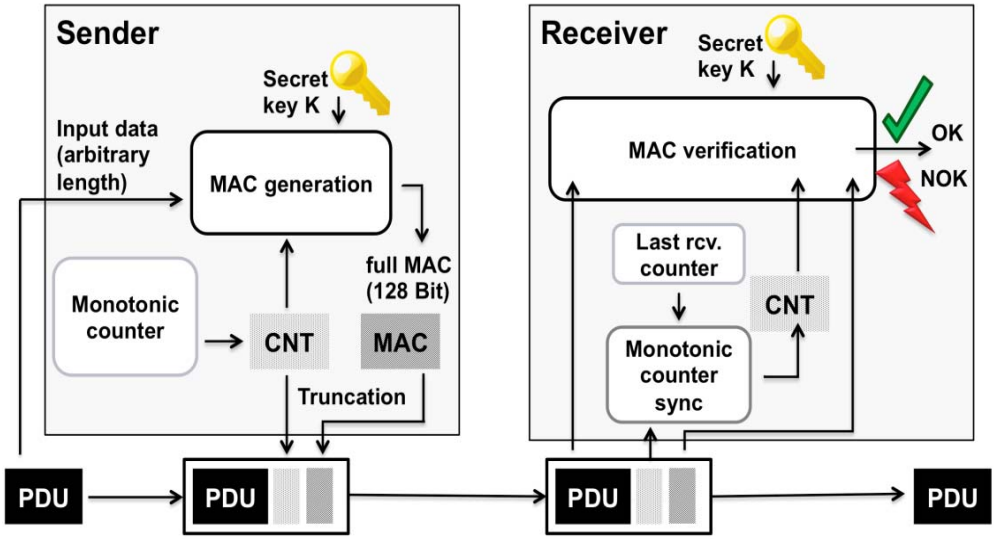


Secure On-board Communication
Technical solution

- Security data will be added to the payload:
  - Authentication code to protect the payload - can be truncated
  - Freshness value – truncated, transmission is optional



- **Authentication code** is created by using payload freshness value and secret key
  - can be generated by symmetric or asymmetric cryptographic algorithms
- **Freshness value** is part of the authentication code calculation and prevents replay attacks
  - can either be a simple counter or a time value



- Freshness value must be synchronized between sender and receiver in a secure way (not part of the standard)
- Freshness value must never overflow except after the secret keys have been replaced

- AUTOSAR considers validation as part of concept development process

  - **Validation by proof of concept implementation (prototype implementation)**
    - Performed by subcontracted BSW vendor
    - Validation covered message authentication (transmission of full and truncated MAC with counter value of different length); Freshness-Counter usage; Propagation of the verification status

  - **Security Assessment**
    - Performed by independent security experts
    - In scope: cryptographically strong integrity, authentication and anti-replay
    - Out of scope: Key management, attacks on cryptographic algorithms
    - The specified protection mechanisms follow acknowledged best practices regarding the replay-protected authentication of messages

  - **Conclusion**:
    - “Secure On-board Communication” features will safeguard against injection, altering, and replay of secure I-PDUs

Topics

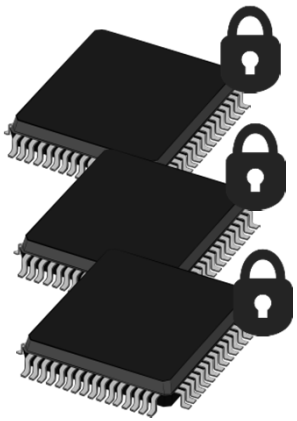
1. Status AUTOSAR
2. Security Features in AUTOSAR
   - Secure on-board communication
3. The AUTOSAR Security Work Package
4. Conclusion and outlook

AUTOSAR Work Package for Security (WP-X-SEC)

- WP-X-SEC started in November 2014
- Comprehensive representation of automotive security experts from vehicle manufacturers, suppliers, software stack vendors and semiconductor vendors
- Motivation
  - Connected vehicle is exposed to security threats
  - Automotive industry must prove itself trustworthy
  - Security is no competitive differentiating feature
  - Higher quality of the security solution when examined and designed by more experts
  - Cost efficiency and improved interoperability between different ECU manufactures
- Mission
  - Maintain existing standard
  - Identify and incorporate new security measures into AUTOSAR
  - Holistic approach on a secure heterogeneous automotive SW architecture

AUTOSAR Work Package for Security (WP-X-SEC)
Working Topics

- Crypto Interface concept
  - standardization of cryptographic primitives as well as access to security hardware
  - planned to be released with Rel. 4.3
- Policy Manager concept
  - Mechanisms, protocols and standardized format to define, configure, update security policies
- SOTA (Software Over The Air) subgroup
  - security analysis of SOTA use cases
- Key Management subgroup
  - analysis of all requirements relevant to key management on vehicle side
- Adaptive AUTOSAR security subgroup
  - security analysis of use cases to be supported with Adaptive AUTOSAR
- …

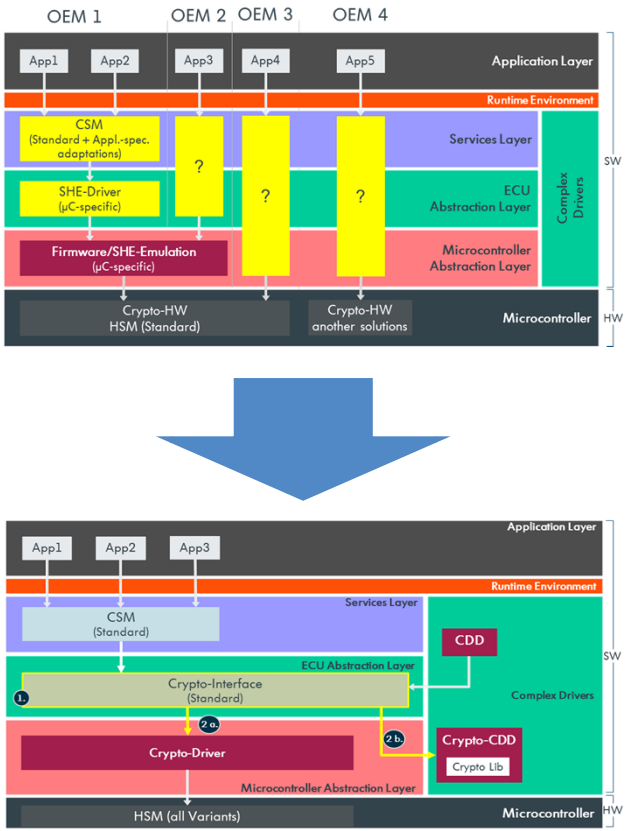


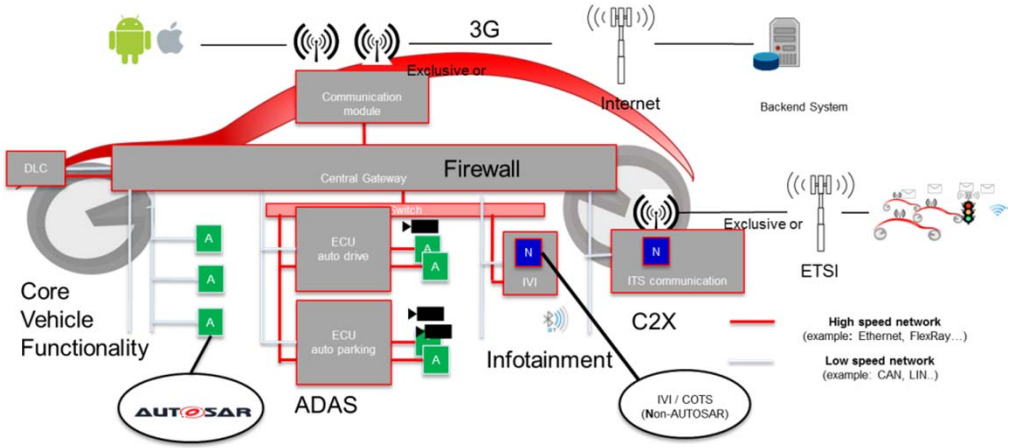
Topics

1. Status AUTOSAR
2. Security Features in AUTOSAR
   - Secure on-board communication
3. The AUTOSAR Security Work Package
4. Conclusion and outlook

Making the car more secure
Towards a secure automotive software architecture

- Enhance security software architecture e.g. by Crypto Interface concept
  - technology trends like Car-2-X require cryptographic protection by security hardware as well as security software
  - heterogeneous solutions with different proprietary drivers for diverse microcontroller lead to high costs
  - → Standardized interface to security hardware and software
- Security policies
- Key management
- Certificate handling
- …





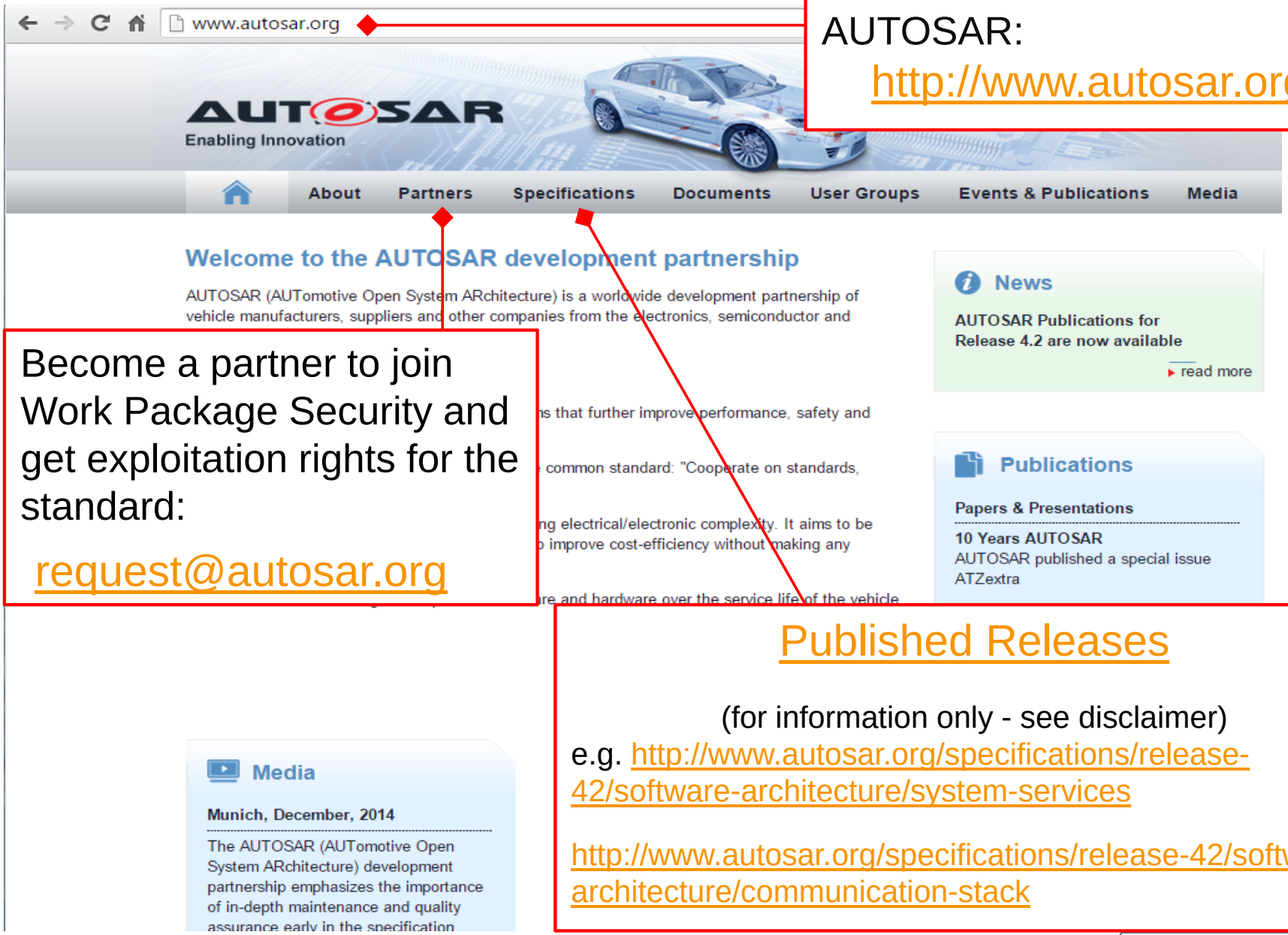
Conclusion

- AUTOSAR already supports fundamental security mechanisms since Release 4.0
- With the latest Release 4.2 the vehicle-internal communication can be protected
- AUTOSAR Work Package Security is in place …
- … to further enhance security features like secure storage of keys or certificate handling in upcoming AUTOSAR releases in order to fully support future trends like Car-2-X or highly automated driving

Thank you for your attention!

More Information about AUTOSAR:

http://www.autosar.org



Become a partner to join Work Package Security and get exploitation rights for the standard:

request@autosar.org

Published Releases

(for information only - see disclaimer)

e.g. http://www.autosar.org/specifications/release-42/software-architecture/system-services

http://www.autosar.org/specifications/release-42/software-architecture/communication-stack