escrypt
SECURITY. TRUST. SUCCESS.

Security in Adaptive AUTOSAR

Author: Michael Schneider
Presenter: Hoyong Lee

Adaptive AUTOSAR Solution Open Seminar @ ETAS Korea, 10.07.2018

Outline

escrypt
SECURITY. TRUST. SUCCESS.

- Introduction
- Crypto-/Key-Management
- Secure Communication
- Identity & Access Management
- Trusted Platform
- Security beyond the specification
- Conclusion

© ESCRYPT 2018. All rights reserved.

escrypt
SECURITY. TRUST. SUCCESS.

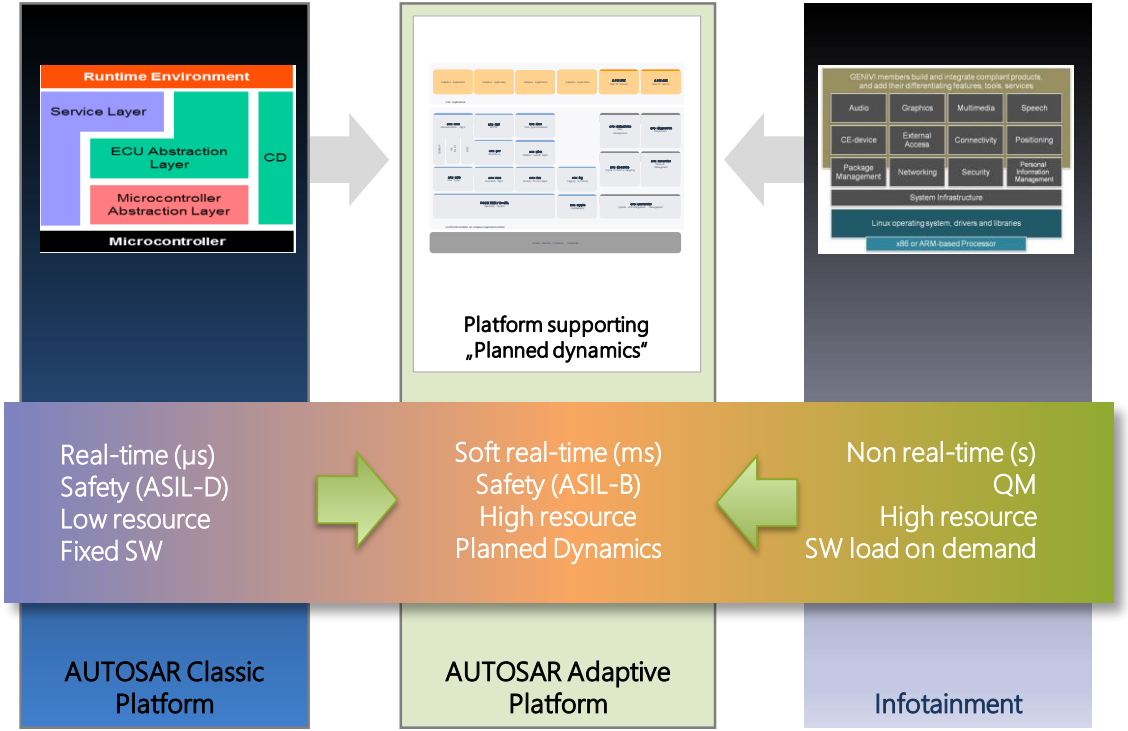
Introduction

© ESCRYPT 2018. All rights reserved.

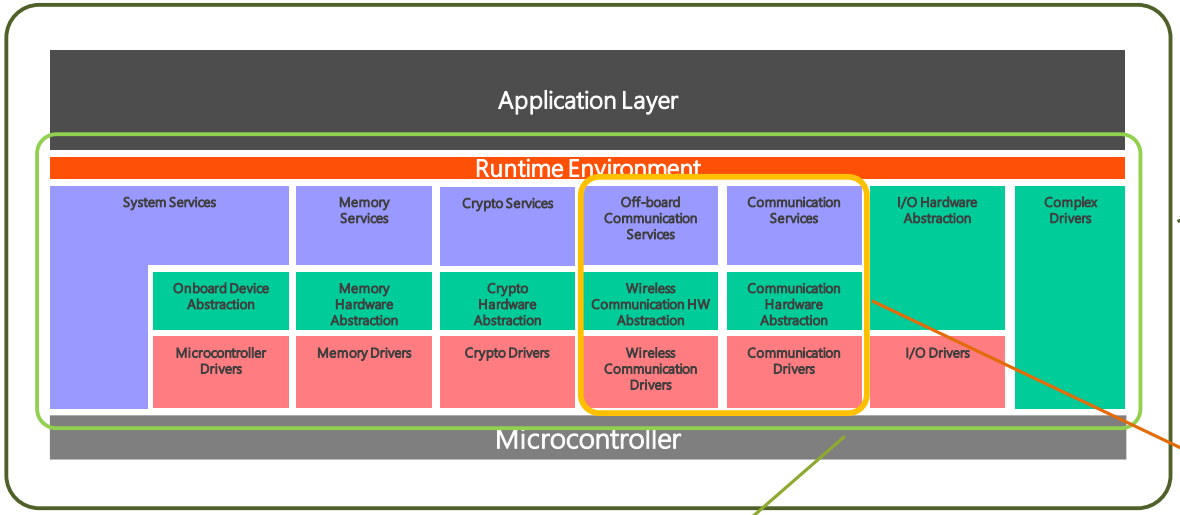
escrypt
SECURITY. TRUST. SUCCESS.

Why adaptive?

- New Application Domains
  - ADAS, V2X, …
- New requirements
  - Open access to the vehicle
  - High performance computing
  - High bandwidth communication
- Planned dynamics includes…
  - Pre-determination of service discovery
  - Dynamic memory allocation in startup phase only
  - Fixed allocation of processes to cores
  - Access to only pre-existing files
  - API usage restrictions



escrypt
SECURITY. TRUST. SUCCESS.



Monolithic:
All components are compiled to one binary which can only be changed as an entire block

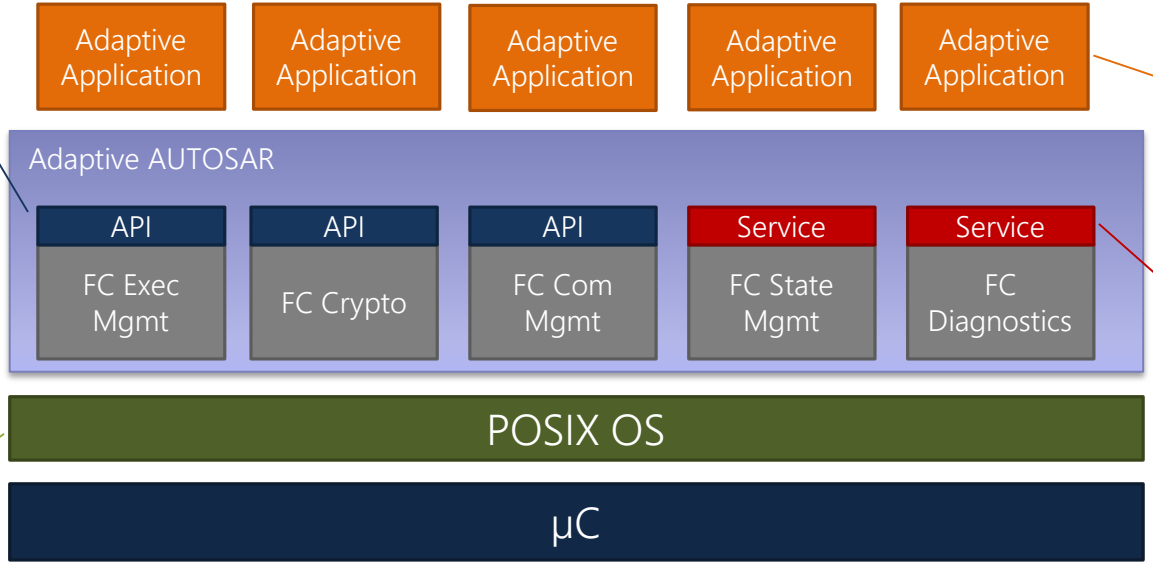
Signal-based communication:
Communication & partners are predefined

HW abstraction:
Classic AUTOSAR abstracts directly the µC and provides predefined ports to Applications via the RTE

© ESCRYPT 2018. All rights reserved.

escrypt
SECURITY. TRUST. SUCCESS.

FCs offer APIs which can be consumed by applications like a library



Modular: Applications are handled as processes and can be updated individually

Service-oriented communication: Applications can subscribe dynamically to services (also remote)

POSIX OS abstracts µC from Adaptive AUTOSAR

escrypt
SECURITY. TRUST. SUCCESS.

Adaptive AUTOSAR is based on a fundamentally different architecture than Classic AUTOSAR

- Existing security concepts in Classic AUTOSAR have to be adapted
- New security concepts are needed for securing the platform

escrypt
SECURITY. TRUST. SUCCESS.

Crypto- & Key-Management

© ESCRYPT 2018. All rights reserved.

escrypt
SECURITY. TRUST. SUCCESS.

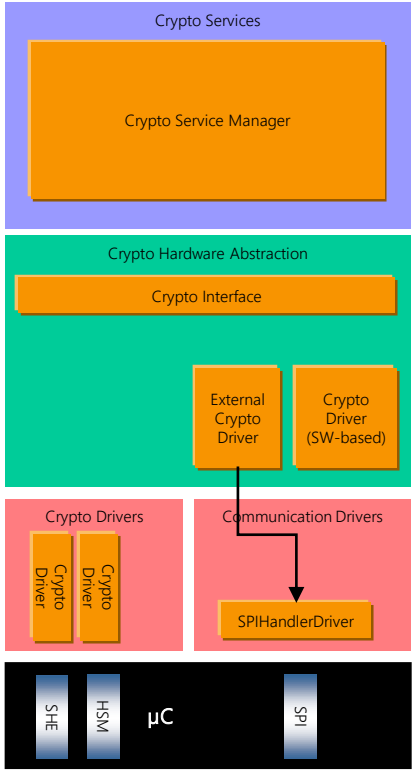
Classic AUTOSAR

Cryptostack: CSM, CryIf, Crypto Driver

Functionality:

- CryptoJobs: Used to access algorithms, linked to keys
- Keyslots are preconfigured
- Certificates: Only parsing and verifying available

The configuration is statically configured during the development of the ECU!

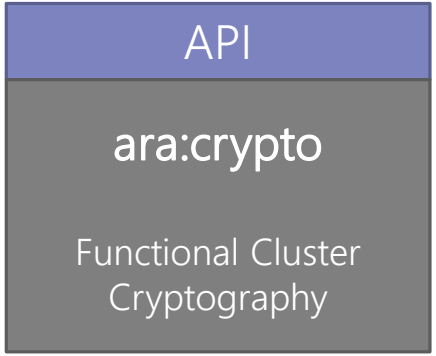


escrypt
SECURITY. TRUST. SUCCESS.

Adaptive AUTOSAR

Realized as Functional Cluster Cryptography

- Crypto operations are **not** offered as a service
- API can be consumed by applications like a library



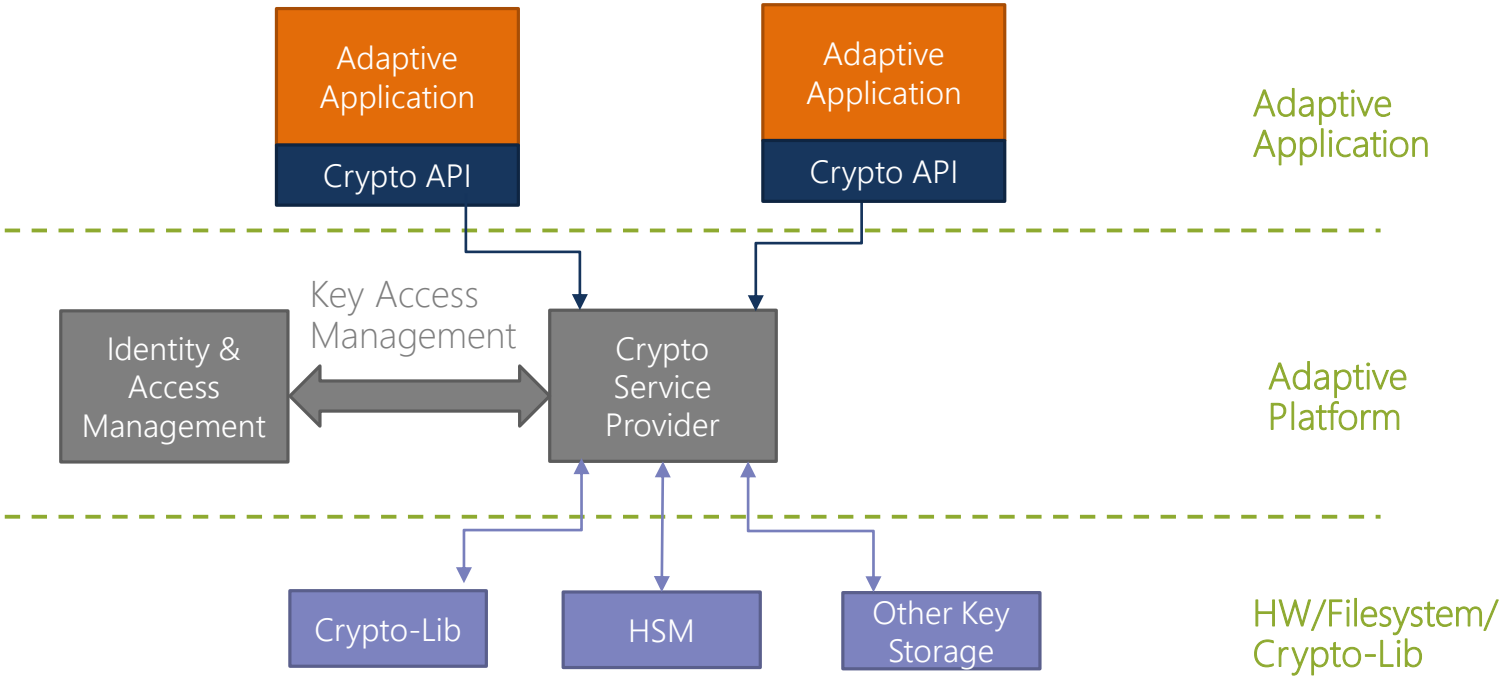
Functionality

- Access to Crypto-Algorithms (**dynamically configurable by Application**)
- Key-Management (**including e.g. session key derivation**)
- Certificate management

Will be included in the 18-10 release

Crypto- & Key-Management

escrypt
SECURITY. TRUST. SUCCESS.



escrypt
SECURITY. TRUST. SUCCESS.

Secure Communication

© ESCRYPT 2018. All rights reserved.

escrypt
SECURITY. TRUST. SUCCESS.

Classic AUTOSAR

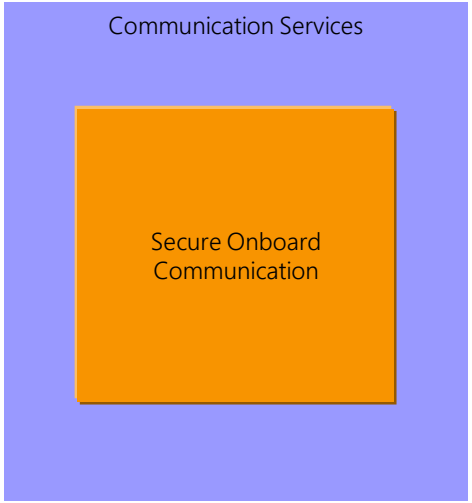
Constraints

- Signal-based communication (service-oriented is coming)
- No constraints with regards to busses

SecOC module

Authenticating communication with MAC-Tags

- Specific to AUTOSAR
- Focus on (but not limited to) CAN-Bus
- Supports multicast communication



escrypt
SECURITY. TRUST. SUCCESS.

Adaptive AUTOSAR

Constraints

- Service-Oriented communication
- Limited to Ethernet

Communication Paradigms:

- SOME/IP (Scalable service-Oriented MiddlewarE over IP)
- DDS (Data Distribution Service)

Applications can discover and subscribe to services by using the Functional Cluster Communication Management

escrypt
SECURITY. TRUST. SUCCESS.

Adaptive AUTOSAR

- (D)TLS
  - Authentication & Encryption
  - In Scope for first final Release 18-10
  - Classic AUTOSAR will be extended to support TLS, too
- IPSec
  - Authentication & Encryption
  - In Scope for first final Release 18-10
  - Classic AUTOSAR will be extended to support IPSec, too
- SecOC
  - Only Authentication
  - Not in scope for Release 18-10
  - Currently not compatible with Classic AUTOSAR
  - Only mechanism that supports multicast

For an application, all provided methods are transparent

escrypt
SECURITY. TRUST. SUCCESS.

Identity & Access Management (IAM)

© ESCRYPT 2018. All rights reserved.

escrypt
SECURITY. TRUST. SUCCESS.

NEW concept in Adaptive AUTOSAR

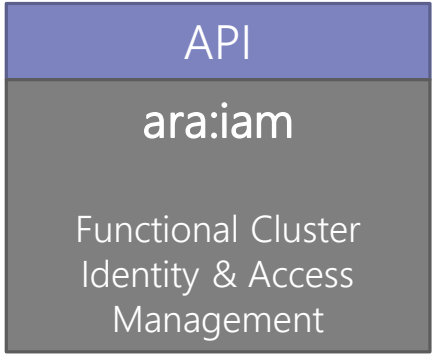
Reason:

- Applications can be dynamically updated
- Applications have more freedom in communication by subscribing to services

Access control is needed

Realization:

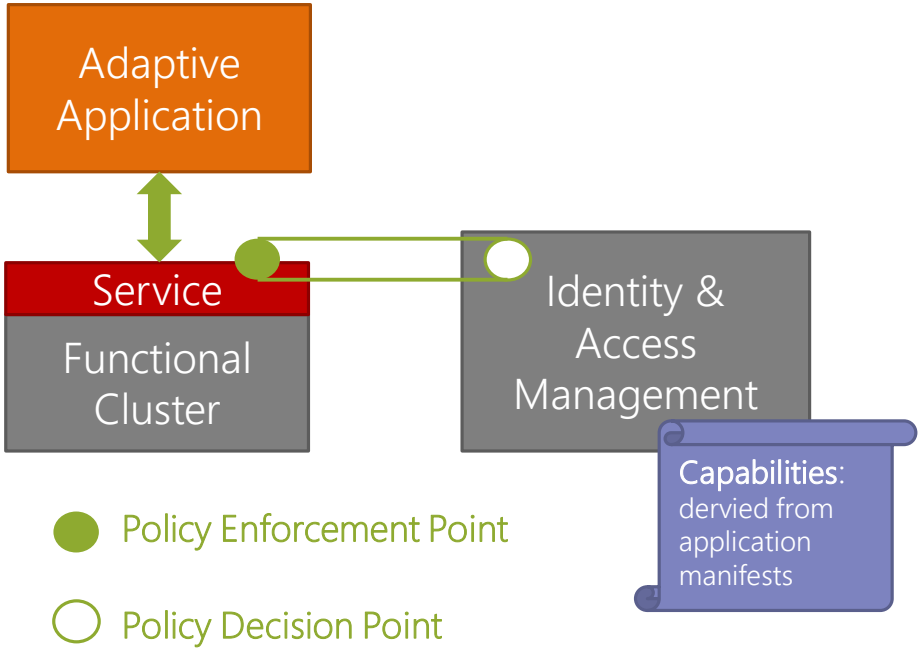
Functional Cluster Identity & Access Management



Identity & Access Management

escrypt
SECURITY. TRUST. SUCCESS.

- Access policy is derived from **capabilities**, which are shipped with the applications manifest.
- The capabilities are enforced at the **Policy Enforcement Point** (PEP), when the application tries to access a resource (e.g. service).
- The FC Identity & Access Management provides a **Policy Decision Point** (PDP), where the access is granted or forbidden.
- OEM IAM implementation and remote access to services are also supported



escrypt
SECURITY. TRUST. SUCCESS.

Trusted Platform

© ESCRYPT 2018. All rights reserved.

Trusted Platform

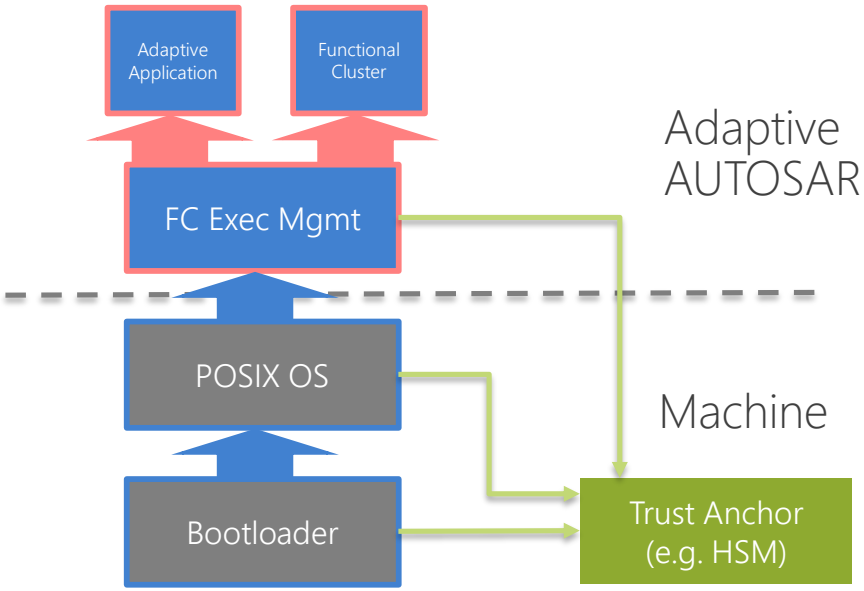
escrypt
SECURITY. TRUST. SUCCESS.

NEW concept in Adaptive AUTOSAR

Goal: Application Authenticity (Startup, Execution, Update)

Classic AUTOSAR could be authenticated as a block, due to its monolithic architecture

Adaptive Applications are separate executables which have to be checked individually



escrypt
SECURITY. TRUST. SUCCESS.

Security beyond the specification

© ESCRYPT 2018. All rights reserved.

Security beyond the specification

escrypt
SECURITY. TRUST. SUCCESS.

- POSIX OS
  - Security issues can arise depending on the POSIX OS used (e.g. lib poisoning)

  OS has to be hardened

- Programming language
  - C in Classic vs. C++ in Adaptive
  - C++ offers more standardized interfaces as C

  C++ makes it harder to follow bad coding habits

  AUTOSAR offers a collection of C++ Coding Guidelines

© ESCRYPT 2018. All rights reserved.

escrypt
SECURITY. TRUST. SUCCESS.

Conclusion

© ESCRYPT 2018. All rights reserved.

Conclusion

escrypt
SECURITY. TRUST. SUCCESS.

- Adaptive AUTOSAR is more dynamic and has a non-monolithic architecture in contrast to Classic AUTOSAR
- Crypto-Management: Both standards support the usage of crypto algorithms, but in Adaptive it is more dynamic with regards to the application
- Secure Communication: Adaptive only supports Service-oriented communication with Ethernet. The current focus is on TLS and IPSec
- IAM: Protects against unauthorized access of AUTOSAR resources
- Trusted Platform: Secure start, execution & update of applications
- Security beyond the specification: OS vulnerabilities are inherited, C++ coding guidelines

© ESCRYPT 2018. All rights reserved.