AUTOSAR™

WG-SEC Overview

Florin Anton

23 May 2024 User Group North America meeting

BMW BOSCH Continental Ford gm STELLANTIS TOYOTA VOLKSWAGEN GROUP

Agenda

- Introduction to WG-SEC
- Overview over AUTOSAR Security Features
- Adaptive Platform current main activities
- Classic Platform current main activities

Agenda

- Introduction to WG-SEC
- Overview over AUTOSAR Security Features
- Adaptive Platform current main activities
- Classic Platform current main activities

Introduction to WG-SEC

AUTOSAR goals

- Support the development of secure systems through the two standards (Classic & Adaptive)
- To provide layered automotive security approach, to define measures at specific layers:
  - Individual ECU
  - In vehicle network
  - E/E architecture
  - Connected vehicle
- Provide and support coexistence and interoperability of security measures between CP and AP

WG-SEC

- Maintain and improve Security features in Adaptive and Classic Platform
- Ensure interoperability between Adaptive and Classic Platform
- Coordinate security concepts and provide security expertise for cross functional topics

Agenda

- Introduction to WG-SEC

Overview over AUTOSAR Security Features

- Adaptive Platform current main activities
- Classic Platform current main activities

Overview over AUTOSAR Security Features

Layered Automotive Security Approach

E/E architecture

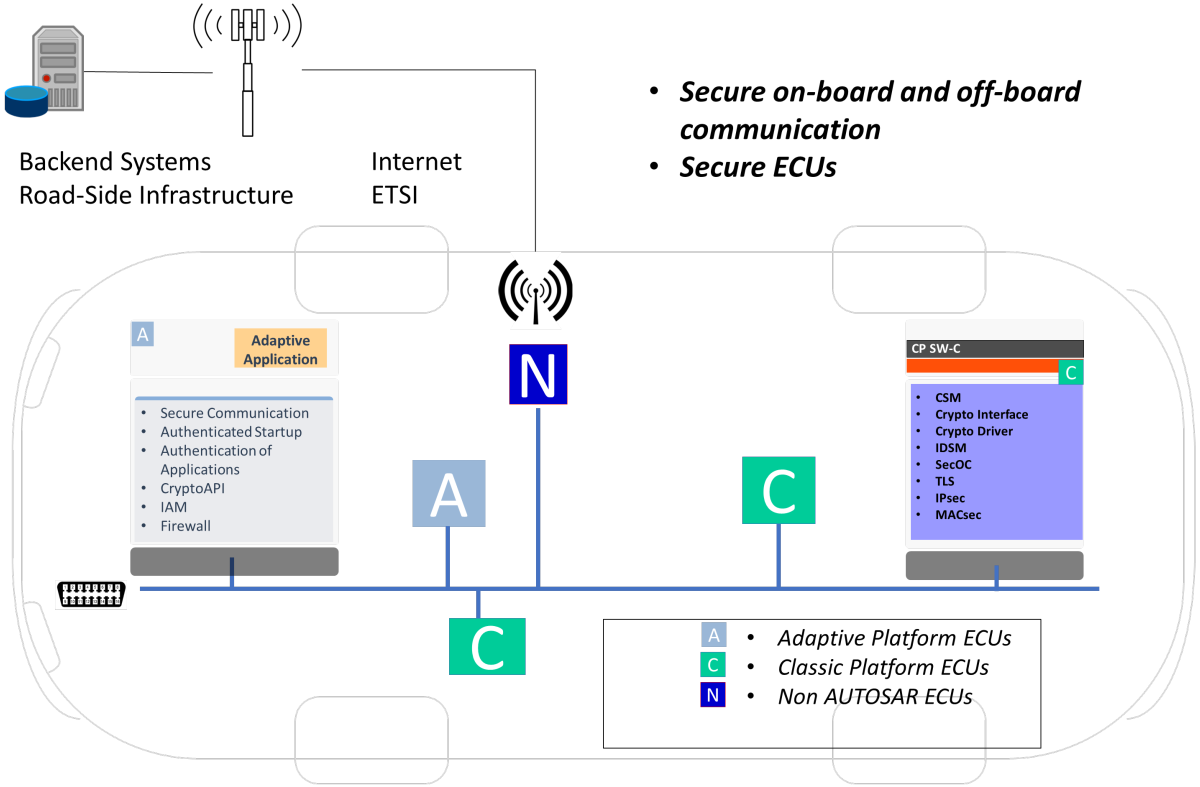
Intrusion Detection System, Firewall

In vehicle network

SecOC, (D)TLS, IPsec, MACsec

Individual ECU

Crypto API, Key Management, Identity and Access Management, Trusted Platform



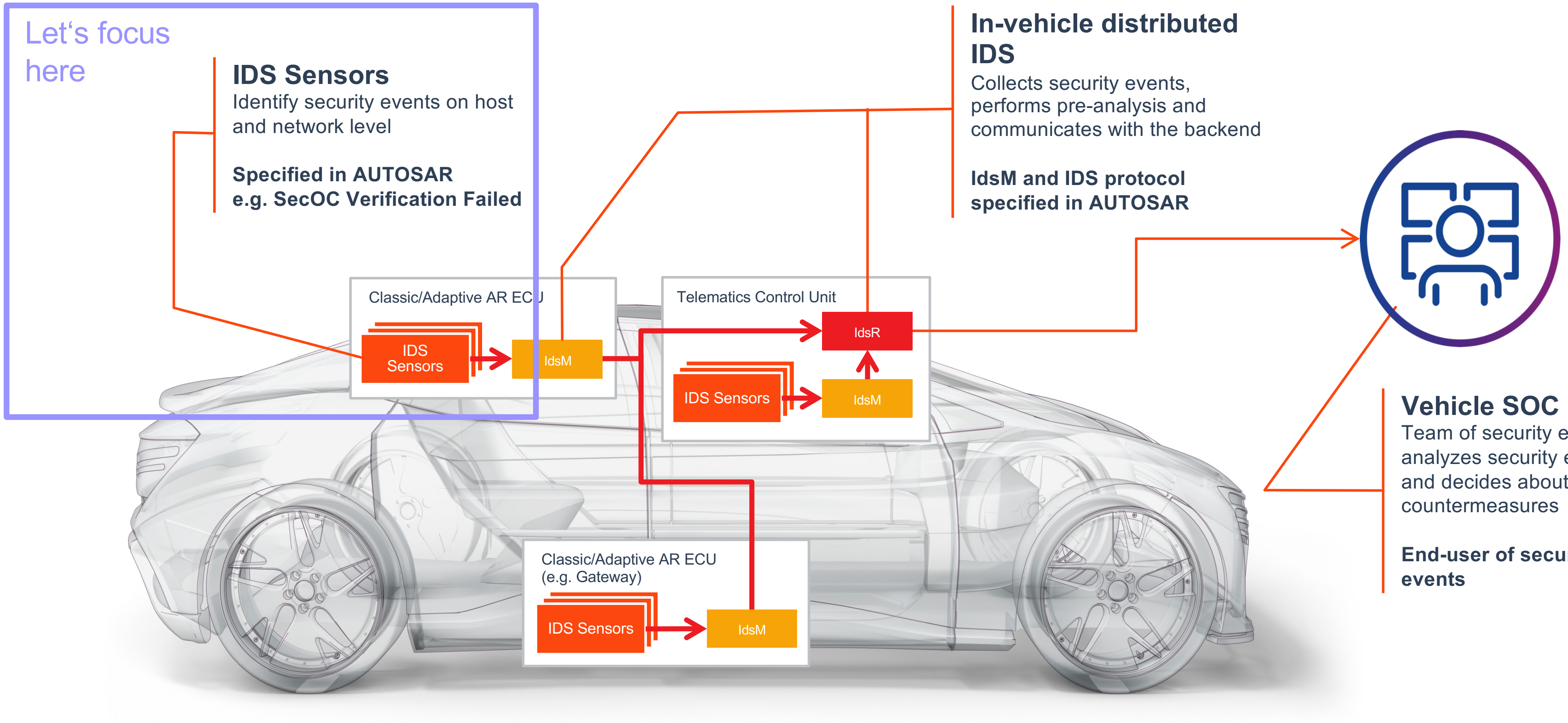
- ***Secure on-board and off-board communication***
- ***Secure ECUs***

Adaptive Platform current main activities

CONC727 Sev Extension & Improvement (AP & CP)

› Current status of IAM

Introduction to security monitoring



IDS Sensors
Identify security events on host and network level

Specified in AUTOSAR e.g. SecOC Verification Failed

In-vehicle distributed IDS
Collects security events, performs pre-analysis and communicates with the backend

IdsM and IDS protocol specified in AUTOSAR

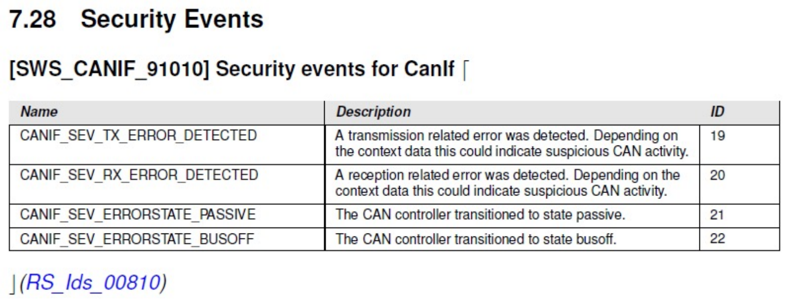
Vehicle SOC
Team of security experts analyzes security events and decides about countermeasures

End-user of security events

SEv specification in AUTOSAR

What indicates a well-defined SEv

Property	CanIf
Clear name	🟩
Clear description	🟩
Context Data available and useful	🟩
Trigger condition	🟩
Harmonization CP/AP	n/a

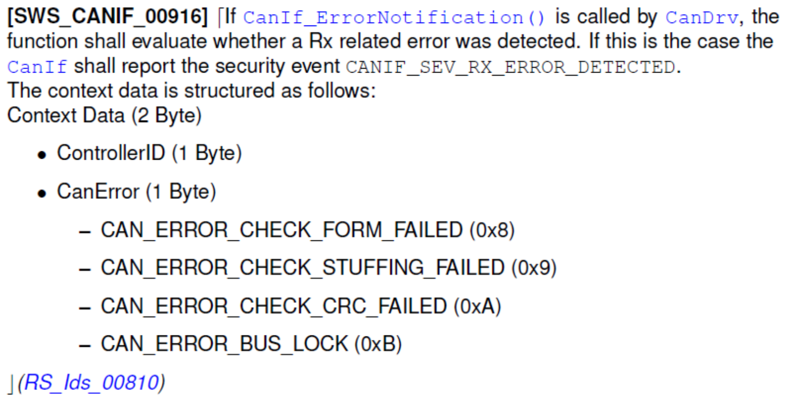


7.28 Security Events

[SWS_CANIF_91010] Security events for CanIf ⌈

Name	*Description*	*ID*
CANIF_SEV_TX_ERROR_DETECTED	A transmission related error was detected. Depending on the context data this could indicate suspicious CAN activity.	19
CANIF_SEV_RX_ERROR_DETECTED	A reception related error was detected. Depending on the context data this could indicate suspicious CAN activity.	20
CANIF_SEV_ERRORSTATE_PASSIVE	The CAN controller transitioned to state passive.	21
CANIF_SEV_ERRORSTATE_BUSOFF	The CAN controller transitioned to state busoff.	22

⌋*(RS_Ids_00810)*



[SWS_CANIF_00916] ⌈If `CanIf_ErrorNotification()` is called by `CanDrv`, the function shall evaluate whether a Rx related error was detected. If this is the case the `CanIf` shall report the security event `CANIF_SEV_RX_ERROR_DETECTED`.
The context data is structured as follows:
Context Data (2 Byte)

- ControllerID (1 Byte)
- CanError (1 Byte)
  - CAN_ERROR_CHECK_FORM_FAILED (0x8)
  - CAN_ERROR_CHECK_STUFFING_FAILED (0x9)
  - CAN_ERROR_CHECK_CRC_FAILED (0xA)
  - CAN_ERROR_BUS_LOCK (0xB)

⌋*(RS_Ids_00810)*

Quality shortcoming in AUTOSAR SEvs

We performed an analysis of all SEvs in R23-11

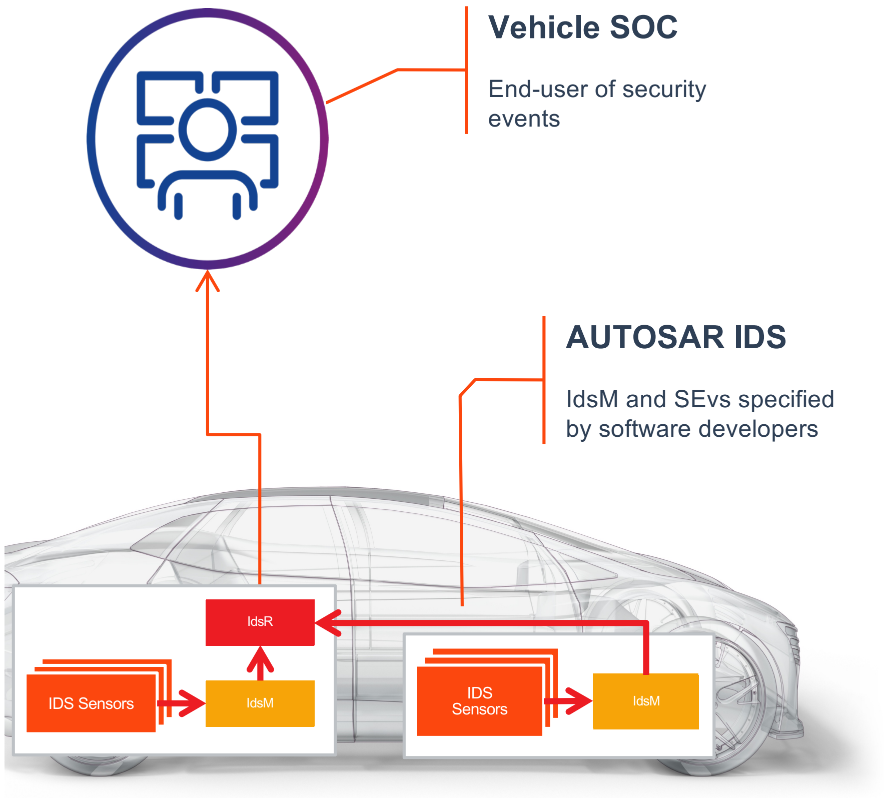
➔ **Many SEvs don‘t fulfill multiple quality criteria**

Shortcoming render incident analysis hard to impossible:

- Missing/underspecified context data
  - Missing data to perform thorough event analysis
- Undefined trigger conditions
  - No reliable source of SEv
- SEv Harmonization missing
  - SEvs only available either by Classic or Adaptive

SEV Name	Naming remarks	Description remarks	Context Data Remarks	Trigger conditions Quality	Harmonization
SEV_CERT_ROOT_INST_REQ	OK	OK	Improvement (see JIRA tickets)	Needed	Needed
SEV_CERT_ROOT_UPD_REQ	OK	OK	Improvement (see JIRA tickets)	Needed	Needed
SEV_CERT_INTERMEDIATE_INST_REQ	OK	OK	Improvement (see JIRA tickets)	Needed	Needed
SEV_CERT_INTERMEDIATE_UPD_REQ	OK	OK	Improvement (see JIRA tickets)	Needed	Needed
SEV_CERT_VERIF_FAILED	OK	OK	Improvement (see JIRA tickets)	Needed	Needed
SEV_IDSM_NO_EVENT_BUFFER_AVAILABLE	OK	OK	Needed	OK	Needed (AP does not define any SEV for IdsM)
SEV_IDSM_NO_CONTEXT_DATA_BUFFER_AVAILABLE	OK	OK	Needed	OK	Needed (AP does not define any SEV for IdsM)
SEV_IDSM_TRAFFIC_LIMITATION_EXCEEDED	OK	OK	Needed	Improvement (name of SEV in trigger condition does not match the SEV in the table)	Needed (AP does not define any SEV for IdsM)
SEV_IDSM_COMMUNICATION_ERROR	OK	OK	Needed	Needed	Needed (AP does not define any SEV for IdsM)
SEV_IDSM_NO_QUALIFIED_EVENT_BUFFER_AVAILABLE	OK	OK	Needed	OK	Needed (AP does not define any SEV for IdsM)

What‘s the reason for these shortcomings?


Vehicle SOC
End-user of security events
AUTOSAR IDS
IdsM and SEvs specified by software developers
IdsR
IDS Sensors
IdsM
IDS Sensors
IdsM

- ➢ Timing: Vehicle SOCs were not established when IdsM was introduced
- ➢ SEv specification from developers perspective – „What does my SW module offer that might be a sensible SEv?“
- ➢ End-user perspective (VSOC) was not taken into account

➔ **Vehicle SOCs are now established, IDS specifications available**

➔ **SEvs should be defined in top-down approach instead of bottom-up**

How to address these shortcomings?

Challenges for SEv improvement

- Distributed SWS specification
  → How to manage improvement?
- No quality criteria established and enforced
- End-user (VSOC) not participating in AUTOSAR

➔ Concept group established to address all of these challenges

CONC727 is no concept any longer

- Concept work is handled within CRs/Bugs (see list here)
- After discussion with QA: No concept, rather CR/Bug umbrella
- We keep the concept as a vehicle for organizing our work
- No milestone reviews by working groups required

Concept goals

SEv specification improvement

- Identify SEv gaps and prioritize them
- R24-11 priorities
  - **SW Update → WG-UCM**
  - UDS → WG-DIA
  - Secure Boot → WG-SEC, WG-EMO

- Define and establish SEv quality criteria for high-quality SEv specification

SEv specification as open-source

- Use-case: End-user (VSOC) wants to have uniform SEvs from the vehicle
  ➔ Non-AUTOSAR ECUs shall raise the same SEVs as AUTOSAR ECUs

- Concept goals
  - Context data focusing on underlying technology
  - **Publication of SEv specification in new open-source document**
    → Enables usage of AUTOSAR SEv specification by non-AUTOSAR ECUs

Take away messages

- The CONC727 concept group is **improving the AUTOSAR SEv specification**

- Sooner or later, the **concept group will approach your working group** to discuss SEvs

- If you are currently working on SEvs, **please reach out to the concept group**

Adaptive Platform current main activities

- CONC727 Sev Extension & Improvement
- Current status of IAM

Current status of IAM

What is IAM?

Identity & Access Management provides access control to sensible resources on AP

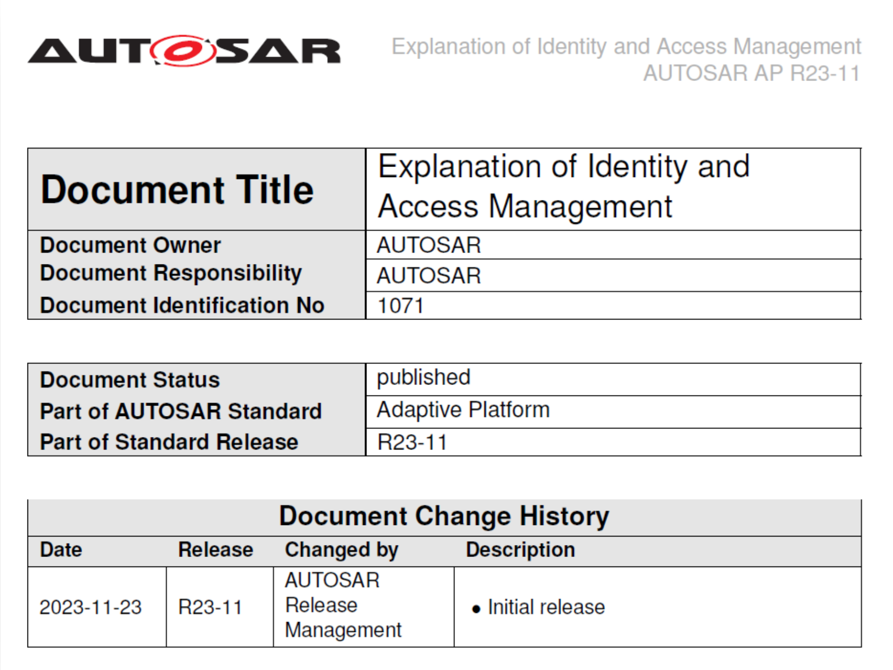
What‘s new?

- SWS_IAM discontinued in R23-11
- Functional IAM specification in respective FCs
- EXP_IAM introduced in R23-11

Why this presentation?

- IAM has low visibility, but big impact

➔ **Get everybody on the same page w.r.t. IAM**



Explanation of Identity and Access Management
AUTOSAR AP R23-11

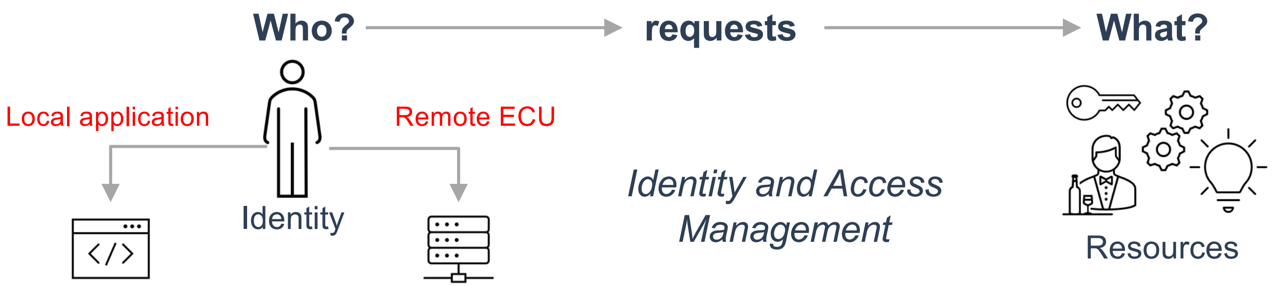
Document Title	Explanation of Identity and Access Management
Document Owner	AUTOSAR
Document Responsibility	AUTOSAR
Document Identification No	1071

Document Status	published
Part of AUTOSAR Standard	Adaptive Platform
Part of Standard Release	R23-11

Document Change History

Date	Release	Changed by	Description
2023-11-23	R23-11	AUTOSAR Release Management	• Initial release

IAM? Available and Stable for ara::com!



Identity and Access Management

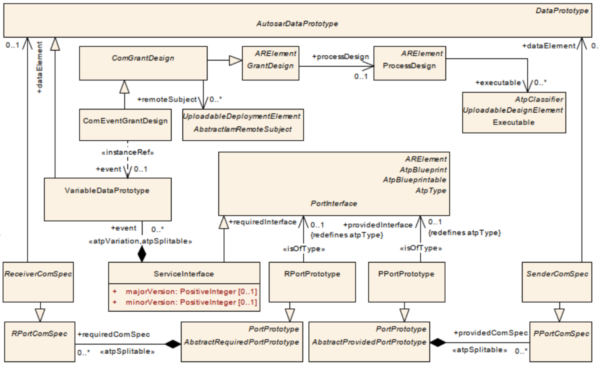
AP Foundation APIs, Services
Applications‘ capabilities

ara::com design …

I the **application designer** want to …

- Offer a **service**
- Use a **field**
- Access an **event**
- Invoke a **method**

and my application will be running on the local machine or a remote machine



DataPrototype
AutosarDataPrototype
ComGrantDesign
ARElement GrantDesign
ARElement ProcessDesign
ComEventGrantDesign
UploadableDeploymentElement AbstractIamRemoteSubject
AtpClassifier UploadableDesignElement Executable
VariableDataPrototype
ARElement AtpBlueprint AtpBlueprintable AtpType PortInterface
ReceiverComSpec
ServiceInterface
RPortPrototype
PPortPrototype
SenderComSpec
RPortComSpec
PortPrototype AbstractRequiredPortPrototype
PortPrototype AbstractProvidedPortPrototype
PPortComSpec

Figure 3.86: Modeling of grant designs for `event`

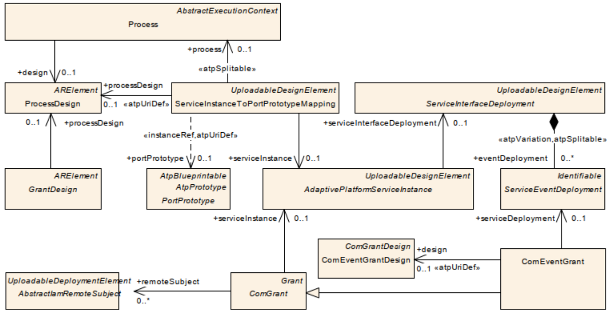
(TPS_ManifestSpecification chapter 3.6.1)

… to deployment

I the **platform integrator** grant access to …

an application running on the local machine or a remote machine to

- Offer a **service**
- Use a **field**
- Access an **event**
- Invoke a **method**



AbstractExecutionContext Process
ARElement ProcessDesign
UploadableDesignElement ServiceInstanceToPortPrototypeMapping
UploadableDesignElement ServiceInterfaceDeployment
ARElement GrantDesign
AtpBlueprintable AtpPrototype PortPrototype
UploadableDesignElement AdaptivePlatformServiceInstance
Identifiable ServiceEventDeployment
ComGrantDesign ComEventGrantDesign
UploadableDeploymentElement AbstractIamRemoteSubject
Grant ComGrant
ComEventGrant

Figure 10.39: Modeling of the `ComEventGrant`

(TPS_ManifestSpecification chapter 10.9.1.3)

IAM status in AP Functional Clusters

Access control of service interfaces

- ➢ Works out of the box, no additional specification needed

Access control of APIs

- ➢ Additional specification required
- ➢ Specification patterns available!

How to handle failed access attempts?

- SEv specification ongoing → AR-122319
- Heterogeneous return to application
  → Arc Rollout coming soon

FC	Resource	Status
PHM	ReportCheckpoint	**OK**
Crypto	CryptoKeySlot	**OK**
	Write Certificate	**In progress**
IdsM	SecurityEvent TimestampProvider ContextDataProvider	**OK**
Firewall	StateSwitchInterface	**In progress**
State Mgmt		**In Analysis**
Diag		**In Analysis**

Patterns

1. Explicit Modelling (ara::com)

Design : GRANT-DESIGN
Deployment : GRANT

2. Implicit Modelling

FC : FunctionClusterInteractsWithFunctionClusterMapping

- Modelled Element (resource)
- FC (identity)

AA : <Model-Element>ToPortPrototypeMapping links

- Modelled Process (identity)
- Modelled Element (resource)

3. Functional specification

[SWS_*<FC>*_XXX1] [*<FC>* shall grant a runtime process *<read/write/other access> <CppResource>*, if a *<ResourceToModel-Element>*Mapping exists that links

- The *<Model-Resource>* representing the *<CppResource>* resource to be accessed.
- The modelled Process, which was used to start this runtime process.]

[SWS_*<FC>*_XXX2] [The interface *<API-interface>* shall *<do-something>* that represents the *<Model-Resource>* identified by the provided ara::core::InstanceSpecifier, or *<return-error / drop-request / raise-SEv>*, if SWS_*<FC>*_XXX1 is not fulfilled.]

4. Failed Access

A failed access shall always raise a Security Event! This SEv is specific to the use case and optionally contains specific context data.

Take away messages

- SWS_IAM was replaced by EXP_IAM in R23-11. IAM was not removed from the specification, but is still part of AUTOSAR

- WG-SEC has developed specification patterns for use in FCs that require access control

- If your group is planning to work on access control specification, please consult with WG-SEC!

Classic Platform current main activities

Crypto refactoring

- KeyM

Crypto redesign

- AR-85630 -> [CSM] How to configure primitive specific parameters?
  - Handling of queues
  - Algo-Fam/Mode handling
  - Key wrap/unrap
  - PQC support

- If your group is planning to provide feedback and shape the future specification version on this topic, please check the Proposed Solution available in Jira and let‘s discuss!

Classic Platform current main activities

› Crypto refactoring

KeyM

Key Manager main topics

- Custom handling for certificates
  - Issues in "custom service and function profile 1“
  - Mapping table for Csm_CustomService
  - Mapping table for Csm_CustomSync
- Missing configuration for security events
- Context data for security events

How to contribute?

- **Weekly meeting dates**
  - CP call: Monday 3pm-5pm CET
    - Crypto subgroup call: Wednesday 3pm-4pm CET
  - AP call: Tuesday 10am-12am CET
    - SeV Extensions call: Monday 2pm-3pm CET
- **Monthly F2F meetings**
  - Every first Tuesday and Wednesday of the month
- **Requirements on participants**
  - Solid background in security, knowledge/experience in AUTOSAR, interest in topics for AUTOSAR security (e.g. CP Crypto Stack, IdsM, …) to make onboarding easier
- **Contact Persons:**
  - Michael Schneider: MichaelPeter.Schneider@etas.com
  - Florin Anton: florin.anton@continental.com

Thank you for your attention!