Document Title	Requirements on Identity and Access Management
Document Owner	AUTOSAR
Document Responsibility	AUTOSAR
Document Identification No	899

Document Status	Final
Part of AUTOSAR Standard	Adaptive Platform
Part of Standard Release	18-03

Document Change History			
Date	**Release**	**Changed by**	**Description**
2018-03-29	18-03	AUTOSAR Release Management	• Initial release

Disclaimer

Table of Contents

1 Scope of Document

This document specifies the requirements of Identity and Access Management to the AUTOSAR Adaptive Platform. The motivation is to provide standardized and portable security in Adaptive Applications.

2 Acronyms and abbreviations

The glossary below includes acronyms and abbreviations relevant to Identity and Access Management that are not included in the AUTOSAR Glossary [1].

Abbreviation / Acronym:	Description:
Identity and Access Management (IAM)	IAM is about managing access rights of Adaptive Applications to interfaces of the Adaptive Platform Foundation and Services.
Policy Decision Point (PDP)	The PDP represents the logic in which the access control decision is made. It determines if the application is allowed to perform the requested task.
Policy Enforcement Point (PEP)	The PEP represents the logic in which the Access Control Decision is enforced. It communicates directly with the corresponding PDP to receive the Access Control Decision.
Access control Policy	Access Control Policies are bound to the targets of calls (i.e. Service interfaces) and are used to express what Identity Information are necessary to access those interfaces.
Access Control Decision	The Access Control Decision is a Boolean value indicating if the requested operation is permitted or not. It is based on the identity of the caller and the Access Control Policy.
Identity	Information represents properties of the Adaptive Applications the access control is decided / enforced upon.
AUTOSAR Resource	The term AUTOSAR Resource covers interfaces that are under the scope of IAM, i.e. Service Interfaces.
Application ID / Application Instance ID	Application ID is a unique identifier for Adaptive Applications. In order to enable multiple instances of Applications with different Startup-Configurations Application Instance IDs might be defined. Both terms may change in future releases.
Capability	A capability is a property of an Adaptive Application. Access to an AUTOSAR resource is granted if a requesting AA possesses all capabilities that are necessary for that specific AUTOSAR Resource.

Table 2.1: Acronyms and Abbreviations

3 Requirements Specification

3.1 Functional Overview

Identity and Access Management provides services for Adaptive Applications and other clusters in the AUTOSAR Adaptive Platform.

3.2 Functional Requirements

[RS_IAM_00001] Limit Adaptive Application access to the `Adaptive Platform Foundation` and Services. ⌈

Type:	draft
Description:	An Adaptive Platform Instance shall provide means to limit access from Adaptive Applications to interfaces of the Adaptive Platform Foundation and Services.
Rationale:	–
Dependencies:	RS_IAM_00010
Use Case:	–
Supporting Material:	–

⌋(*RS_Main_00514*)

[RS_IAM_00002] Enforcement of access control shall happen within `Adaptive Platform Foundation` ⌈

Type:	draft
Description:	Access control shall be enforced by the `Adaptive Platform Foundation` and not by the application.
Rationale:	Applications are considered to potentially being compromised.
Dependencies:	RS_SEC_03004
Use Case:	–
Supporting Material:	–

⌋(*RS_Main_00514*)

[RS_IAM_00003] Applications shall be prevented from taking control over the AUTOSAR PEP ⌈

Type:	draft
Description:	The `Adaptive Platform Foundation` shall prevent Applications from taking control over the AUTOSAR PEP that is part of the AUTOSAR Runtime for Adaptive Applications.
Rationale:	Enforcement to AUTOSAR Resources should happen within the `Adaptive Platform Foundation`.
Dependencies:	RS_SEC_5019, RS_SEC_5018
Use Case:	–

Supporting Material:	–

⌋(*RS_Main_00514*)

[RS_IAM_00004] Circumvention of AUTOSAR PEP interfaces by Applications shall be prevented. ⌈

Type:	draft
Description:	`Adaptive Platform Foundation` shall prevent Applications from circumventing AUTOSAR PEPs by using other APIs than the AUTOSAR defined APIs.
Rationale:	If IAM access control is utilized the PEP has to ensure that the APIs are exclusive to IAM.
Dependencies:	RS_SEC_5019, RS_SEC_5018
Use Case:	–
Supporting Material:	–

⌋(*RS_Main_00514*)

[RS_IAM_00005] `Adaptive Platform Foundation` shall enforce that only Applications that are configured accordingly are able to gain information about the permissions of other applications ⌈

Type:	draft
Description:	The `Adaptive Platform Foundation` must prevent applications from gaining information about the permissions of other applications unless explicitly configured to be allowed to access this information, i.e. for implementing a PDP in this specific Application.
Rationale:	–
Dependencies:	–
Use Case:	–
Supporting Material:	–

⌋(*RS_Main_00514*)

[RS_IAM_00006] Access control policies shall be available to the PDP ⌈

Type:	draft
Description:	Access control policies shall be available to the PDP.
Rationale:	–
Dependencies:	–
Use Case:	–
Supporting Material:	–

⌋(*RS_Main_00514*)

[RS_IAM_00007] The `Adaptive Platform Foundation` shall provide access control decisions ⌈

Type:	draft

Description:	The adaptive `Adaptive Platform Foundation` shall provide access control decisions based on access control policies and capabilities that are stored in the corresponding manifests.
Rationale:	–
Dependencies:	–
Use Case:	–
Supporting Material:	–

⌋(*RS_Main_00514*)

[RS_IAM_00009] An `Adaptive Application` may provide access control decisions ⌈

Type:	draft
Description:	The adaptive `Adaptive Platform Foundation` shall provide an interface to `Adaptive Application` to facilitate access control decisions based on access control policies and capabilities that are stored in the corresponding manifests.
Rationale:	–
Dependencies:	–
Use Case:	–
Supporting Material:	–

⌋(*RS_Main_00514*)

[RS_IAM_00008] Access control decisions must be denied by the PEP if the corresponding PDP is not available ⌈

Type:	draft
Description:	Access control decisions must be denied by the PEP if the corresponding PDP is not available.
Rationale:	Applications that depend on access control during startup have to be covered by IAM. Therefore IAM should be available as soon as possible.
Dependencies:	–
Use Case:	–
Supporting Material:	–

⌋(*RS_Main_00514*)

[RS_IAM_00010] Adaptive applications shall only be able to use AUTOSAR Resources when authorized ⌈

Type:	draft
Description:	The `Adaptive Platform Foundation` must ensure that adaptive applications shall only be able use a AUTOSAR Resource if an existing policy authorizes them to do so.
Rationale:	–
Dependencies:	RS_SEC_00001
Use Case:	–

Supporting Material:	–

⌋(*RS_Main_00060*, *RS_Main_00514*)

[RS_IAM_00011] Policies shall be enforced by the local `Adaptive Platform Foundation` ⌈

Type:	draft
Description:	Policies shall be enforced by the local `Adaptive Platform Foundation`, i.e., that `Adaptive Platform Foundation` that runs on the machine of the requesting application.
Rationale:	–
Dependencies:	–
Use Case:	–
Supporting Material:	–

⌋(*RS_Main_00514*)

[RS_IAM_00012] For each AUTOSAR Resource an access control policy shall be specifiable ⌈

Type:	draft
Description:	For each AUTOSAR Resource an access control policy shall be specifiable which describes what is needed to use that interface.
Rationale:	–
Dependencies:	–
Use Case:	–
Supporting Material:	–

⌋(*RS_Main_00514*)

[RS_IAM_00013] The manifest shall provide a way to state the policy for each AUTOSAR Resource ⌈

Type:	draft
Description:	The manifest shall provide a way to state the policy for each AUTOSAR Resource defining necessary capabilities for access. The `Adaptive Platform Foundation` shall deny access to the AUTOSAR Resource, if the application's capability does not match the policy of the AUTOSAR Resource.
Rationale:	–
Dependencies:	RS_IAM_00013
Use Case:	–
Supporting Material:	–

⌋(*RS_Main_00514*)

[RS_IAM_00014] Unique Adaptive Application ID ⌈

Type:	draft
Description:	An Adaptive Application ID shall be unique regarding the local machine.

Rationale:	Adaptive Applications shall be linked to and held responsible for their actions.
Dependencies:	RS_IAM_00012
Use Case:	The IAM framework uses the application ID of Adaptive Applications to verify requests and grant access to certain AUTOSAR Resources based on the defined polices.
Supporting Material:	–

⌋(*RS_Main_00510*, *RS_Main_00514*)

[RS_IAM_00015] Unique Application Instance ID ⌈

Type:	draft
Description:	An Application Instance ID shall be unique regarding the local machine.
Rationale:	Applications shall be linked to and held responsible for their actions.
Dependencies:	–
Use Case:	The IAM framework uses the application ID to verify requests and grant access to certain AUTOSAR Resources based on the defined polices.
Supporting Material:	–

⌋(*RS_Main_00510*, *RS_Main_00514*)

[RS_IAM_00017] Identity information shall be stored and handled tamper-proof throughout its lifecycle. ⌈

Type:	draft
Description:	The generation, transmission and storage of the Application ID and Application Instance ID must be handled tamper-proof throughout the life cycle.
Rationale:	Application identity integrity is a fundamental component for enforcing access controls.
Dependencies:	–
Use Case:	–
Supporting Material:	–

⌋(*RS_Main_00510*, *RS_Main_00514*)

[RS_IAM_00018] Set of capabilities shall be provided in the corresponding manifest ⌈

Type:	draft
Description:	The set of capabilities of an Adaptive Application shall be provided in the corresponding manifest.
Rationale:	Capabilities defined for an Adaptive Application shall be determined by the corresponding manifest. If an Adaptive Application is compromised, we need the manifest with the capabilities to actually enforce the restrictions implied by the capabilities. We cannot solely rely on the correct behavior of each Adaptive Application. `Adaptive Platform Foundation` shall not provide any interface that allows applications to change its capabilites defined in the manifest during runtime.
Dependencies:	–
Use Case:	–

Supporting Material:	–

⌋(*RS_Main_00514*)

[RS_IAM_00019] Capabilities of an Adaptive Application shall be authentically linked to the manifest ⌈

Type:	draft
Description:	The set of capabilities of an Adaptive Application shall be authentically linked to the Adaptive Application in the corresponding application manifest.
Rationale:	An Adaptive Application is provided with a set of capabilities. It shall not be possible to extend or restrict this set. The Adaptive Application should always possess the same capabilities as originally intended.
Dependencies:	–
Use Case:	–
Supporting Material:	–

⌋(*RS_Main_00514*)

[RS_IAM_00020] `Adaptive Platform Foundation` **stack must allow to specify a superset manifest file of capabilities** ⌈

Type:	draft
Description:	`Adaptive Platform Foundation` must allow to specify a superset manifest file of capabilities.
Rationale:	–
Dependencies:	–
Use Case:	–
Supporting Material:	–

⌋(*RS_Main_00514*)

4 Requirements Tracing

The following table references the features specified in [2] and links to the fulfillments of these.

Feature	Description	Satisfied by
[RS_Main_00060]	AUTOSAR shall provide a standardized software interface for communication between Applications	[RS_IAM_00010]
[RS_Main_00510]	AUTOSAR shall support secure onboard communication	[RS_IAM_00014] [RS_IAM_00015] [RS_IAM_00017]
[RS_Main_00514]	AUTOSAR shall support the development of secure systems	[RS_IAM_00001] [RS_IAM_00002] [RS_IAM_00003] [RS_IAM_00004] [RS_IAM_00005] [RS_IAM_00006] [RS_IAM_00007] [RS_IAM_00008] [RS_IAM_00009] [RS_IAM_00010] [RS_IAM_00011] [RS_IAM_00012] [RS_IAM_00013] [RS_IAM_00014] [RS_IAM_00015] [RS_IAM_00017] [RS_IAM_00018] [RS_IAM_00019] [RS_IAM_00020]

5 References

[1] Glossary
AUTOSAR_TR_Glossary

[2] Main Requirements
AUTOSAR_RS_Main