Document Title	SRS_Diagnostics: Complete Change Documentation 1.4.0 - 1.5.0
Document Owner	AUTOSAR
Document Responsibility	AUTOSAR
Document Identification No	885

Document Status	Final
Part of AUTOSAR Standard	Foundation
Part of Standard Release	1.5.0

Table of Contents

1 SRS_Diagnostics

1.1 Specification Item SRS_Diag_04230

Trace References:

RS_Main_00170

Content:

Type:	Valid
Description:	Diagnostics in AUTOSAR shall support the ISO 14229-1:2018 service 0x29 Authentication with sub-functions for "Authentication with PKI Certificate Exchange (APCE)" to grant access to diagnostic services. The service shall be implemented as internal service (in the BSW) without interaction with applications over middleware.
Rationale:	The authentication service provides a standardized way in authenticating a tester and ECU and grant access to diagnostic services depending on the certificate content.
AppliesTo:	CP, AP
Use Case:	A repair shop diagnostic tester authenticates with an ECU to gain access to diagnostic services that are explicitly allowed to be executed for a repair shop.
Supporting Material:	Concept 636 "Security Extensions" - C5, ISO14229-1:2018 Authentication Service 0x29

RfCs affecting this spec item between releases 1.4.0 and 1.5.0:

- Unknown reason for change.

1.2 Specification Item SRS_Diag_04231

Trace References:

RS_Main_00260

Content:

Type:	Valid
Description:	Diagnostics in AUTOSAR shall support the client certificate formats CVC and X.509 in service 0x29 diagnostic requests. The supported certificate type shall be configurable.
Rationale:	Only the subset of common known and used client certificate types shall be accepted by diagnostics in AUTOSAR. This allows a standardized handling and evaluation of certificates and content.
AppliesTo:	CP, AP
Use Case:	The OEM PKI issues a certificate for a repair shop diagnostic tester. The diagnostic tester and authenticates itself with the ECU.
Supporting Material:	Concept 636 "Security Extensions"

RfCs affecting this spec item between releases 1.4.0 and 1.5.0:

- Unknown reason for change.

1.3 Specification Item SRS_Diag_04232

Trace References:

RS_Main_00170

Content:

Type:	Valid
Description:	The client certificate extensions shall contain well-defined data with diagnostic access rights. The following access rights types shall be available:
Rationale:	Only well-defined client certificate shall be accepted by diagnostics in AUTOSAR that allows a standardized handling and evaluation of certificates and content.
AppliesTo:	CP, AP
Use Case:	The OEM PKI issues a certificate for a repair shop with role based or individual access rights for diagnostic services.
Supporting Material:	Concept 636 "Security Extensions"

RfCs affecting this spec item between releases 1.4.0 and 1.5.0:

- Unknown reason for change.

1.4 Specification Item SRS_Diag_04233

Trace References:

RS_Main_00170

Content:

Type:	Valid
Description:	Certificates provide role based and individual access rights definition. Diagnostics in AUTOSAR shall provide a diagnostic service access right by evaluation properties of services to be executed in the following order:
Rationale:	A definition is required how, the diagnostic service is identified to be executed. Especially the level of granularity is important to reduce the resource consumption to a minimum. The SID check is very coarse but efficient, for services with sub-function the sub-function can be taken into account. Further services with DIDs and RIDs are identified by this identifier only.
AppliesTo:	CP, AP
Use Case:	An authentication state allows to execute any ECU reset service, is restricted to extended session, allows 5 DIDs and one RID to be executed.
Supporting Material:	Concept 636 "Security Extensions"

RfCs affecting this spec item between releases 1.4.0 and 1.5.0:

- Unknown reason for change.

1.5 Specification Item SRS_Diag_04234

Trace References:

RS_Main_00170

Content:

Type:	Valid
Description:	Diagnostics in AUTOSAR shall specify the white list binary layout. This layout shall be compatible for all ECUs independent from the endianness in place.
Rationale:	A definition is required how a white list shall look like so it can be downloaded into any ECU software independent from the used implementation.
AppliesTo:	CP, AP
Use Case:	A certain binary layout for a white list shall define a well-defined set of diagnostic services that are allowed to be executed.
Supporting Material:	Concept 636 "Security Extensions"

RfCs affecting this spec item between releases 1.4.0 and 1.5.0:

- Unknown reason for change.

1.6 Specification Item SRS_Diag_04235

Trace References:

RS_Main_00170

Content:

Type:	Valid
Description:	Diagnostics in AUTOSAR shall evaluate the client certificates validity period and refuse expired our not yet valid certificates.
Rationale:	Control the certificate lifetime and limit the potential of outdated certificates.
AppliesTo:	CP, AP
Use Case:	The OEM PKI issues a certificate (e.g. for a repair shop) for a defined period.
Supporting Material:	Concept 636 "Security Extensions"

RfCs affecting this spec item between releases 1.4.0 and 1.5.0:

- Unknown reason for change.

1.7 Specification Item SRS_Diag_04236

Trace References:

RS_Main_00170

Content:

Type:	Valid
Description:	Diagnostics in AUTOSAR shall provide standardized means for target identification. A target can be identified by OEM defined criteria such as VIN, vehicle line or ECU type.
Rationale:	Control the certificates validity on defined targets only.
AppliesTo:	CP, AP
Use Case:	The OEM PKI issues a certificate for a vehicle with a certain VIN or an only for one type of ECU.
Supporting Material:	Concept 636 "Security Extensions"

RfCs affecting this spec item between releases 1.4.0 and 1.5.0:

- Unknown reason for change.

1.8 Specification Item SRS_Diag_04237

Trace References:

RS_Main_00170

Content:

Type:	Valid
Description:	Diagnostics in AUTOSAR shall use the diagnostic policy manager to evaluate client certificates from service 0x29 requests. The result of a certificate evaluation is the decision if the certificate is valid and which diagnostic services are allowed for execution. Based on the active certificate it grants access for received diagnostic requests.

▽

△

Rationale:	AUTOSAR shall define the semantics for the certificate payload. This allows to have a standardized check for certificate validities and evaluation of contained access rights.
AppliesTo:	CP, AP
Use Case:	A repair shop diagnostic tester initiates an authentication by sending its certificate. A set of diagnostic services is available to the diagnostic tester after authentication.
Supporting Material:	Concept 636 "Security Extensions"

RfCs affecting this spec item between releases 1.4.0 and 1.5.0:

- Unknown reason for change.

1.9 Specification Item SRS_Diag_04238

Trace References:

RS_Main_00170

Content:

Type:	Valid
Description:	The diagnostic policy manager shall report a security event every time a certificate is passed for evaluation. The event data shall contain at least the result of the certificate evaluation.
Rationale:	Forensic analysis and interested parties require information which kind of access was requested and granted to diagnostic testers.
AppliesTo:	CP, AP
Use Case:	A certificated with extended access rights is provided by the diagnostic tester. A security event provides information about that specific certificate was provided to the ECU.
Supporting Material:	Concept 636 "Security Extensions"

RfCs affecting this spec item between releases 1.4.0 and 1.5.0:

- Unknown reason for change.

1.10 Specification Item SRS_Diag_04239

Trace References:

RS_Main_00170

Content:

Type:	Valid
Description:	Diagnostics in AUTOSAR shall have a configuration to allow execution of dedicated diagnostic services in deauthenticated state.
Rationale:	At least the services to authenticate the tester, shall be available in all authentication states.
AppliesTo:	CP, AP
Use Case:	Sending a service 0x29 in deauthenticated state to reach an authentication state.
Supporting Material:	Concept 636 "Security Extensions"

RfCs affecting this spec item between releases 1.4.0 and 1.5.0:

- Unknown reason for change.

1.11 Specification Item SRS_Diag_04240

Trace References:

RS_Main_00170

Content:

Type:	Valid
Description:	Diagnostics in AUTOSAR shall provide means to applications to change the authentication state of unauthenticated connections.
Rationale:	An individual authentication with each ECU in the vehicle might be take too much time some for some applications.
AppliesTo:	CP, AP

▽

△

Use Case:	An application based centralized authentication broadcast is required to gain access to a set of diagnostic services.
Supporting Material:	Concept 636 "Security Extensions"

RfCs affecting this spec item between releases 1.4.0 and 1.5.0:

- Unknown reason for change.