



DPC: 25 / 30459613 DC

BSI Group Headquarters

389 Chiswick High Road London W4 4AL

Tel: +44 (0)20 8996 9000

Fax: +44 (0)20 8996 7400

www.bsigroup.com

Date: 26 February 2025

Origin: International

Latest date for receipt of comments: 19 March 2025

Project No. 2022/01733

Responsible committee: GEL/65 Measurement and control

Interested committees:

Title: Draft BS EN 63278-3 Ed.1.0 Asset Administration Shell for Industrial Applications # Part 3: Security provisions for Asset Administration Shells

Please notify the secretary if you are aware of any keywords that might assist in classifying or identifying the standard or if the content of this standard

- i) has any issues related to 3rd party IPR, patent or copyright
- ii) affects other national standard(s)
- iii) requires additional national guidance or information

**WARNING: THIS IS A DRAFT AND MUST NOT BE REGARDED OR USED AS A BRITISH STANDARD.
THIS DRAFT IS NOT CURRENT BEYOND 19 March 2025**

This draft is issued to allow comments from interested parties; all comments will be given consideration prior to publication. No acknowledgement will normally be sent. **See overleaf for information on the submission of comments.**

No copying is allowed, in any form, without prior written permission from BSI except as permitted under the Copyright, Designs and Patent Act 1988 or for circulation within a nominating organization for briefing purposes. Electronic circulation is limited to dissemination by e-mail within such an organization by committee members.

Further copies of this draft may be purchased from BSI Shop <http://shop.bsigroup.com> or from BSI Customer Services, Tel: +44(0) 20 8996 9001 or email cservices@bsigroup.com. British, International and foreign standards are also available from BSI Customer Services.

Information on the co-operating organizations represented on the committees referenced above may be obtained from <http://standardsdevelopment.bsigroup.com>

Responsible Committee Secretary: Ms Charmaine Mukherjee (BSI)

Direct tel:

E-mail: charmaine.mukherjee@bsigroup.com

Introduction

This draft standard is based on national and international discussions. Your comments on this draft are invited and will assist in the preparation of the consequent standard.

For international standards, comments will be reviewed by the relevant UK national committee before sending the consensus UK vote and comments to the international committee, which will then decide appropriate action. If the international standard is approved, it is usual for the text to be published as a British Standard.

For national standards, comments will be reviewed by the relevant UK national committee and the resulting standards published as a British Standard.

UK Vote

Please indicate whether you consider the UK should submit a negative (with supporting technical reasons) or positive vote on this draft. Please indicate if you are aware of any reason why this draft standard should not be published as a British Standard.

Submission of Comments

- **Annotated drafts are not acceptable and will be rejected.**
- All comments should be submitted online at <https://standardsdevelopment.bsigroup.com/>. You will need to register in order to comment.

Template for comments and secretariat observations

Date: xx/xx/20xx	Document: ISO/DIS xxxx
------------------	------------------------

1	2	(3)	4	5	(6)	7
MB	Clause No./ Subclause No./Annex (e.g. 3.1)	Paragraph/Figure/ Table/Note	Type of comment	Commend (justification for change) by the MB	Proposed change by the MB	Secretariat observations on each comment submitted
	3.1	Definition 1	ed	Definition is ambiguous and needs clarifying.	Amend to read '...so that the mains connector to which no connection...'	
	6.4	Paragraph 2	te	The use of the UV photometer as an alternative cannot be supported as serious problems have been encountered in its use in the UK.	Delete reference to UV photometer.	



65/1119/CD

COMMITTEE DRAFT (CD)

PROJECT NUMBER:

IEC 63278-3 ED1

DATE OF CIRCULATION:

2025-02-21

CLOSING DATE FOR COMMENTS:

2025-04-18

SUPERSEDES DOCUMENTS:

65/916/NP, 65/938A/RVN

IEC TC 65 : INDUSTRIAL-PROCESS MEASUREMENT, CONTROL AND AUTOMATION

SECRETARIAT:

France

SECRETARY:

Mr Didier GIARRATANO

OF INTEREST TO THE FOLLOWING COMMITTEES:

SyC SM,SC 41

HORIZONTAL FUNCTION(S):

ASPECTS CONCERNED:

Digital content, Information security and data privacy

This document is still under study and subject to change. It should not be used for reference purposes.

Recipients of this document are invited to submit, with their comments, notification of any relevant patent rights of which they are aware and to provide supporting documentation.

Recipients of this document are invited to submit, with their comments, notification of any local regulations or technical reasons that may exist and should be considered should this proposal proceed, recognizing that failure to address such requirements could result in the need for new or existing "In Some Countries" clauses. (SEE [AC/22/2007](#) OR [NEW GUIDANCE DOC](#)).

TITLE:

Asset Administration Shell for Industrial Applications – Part 3: Security provisions for Asset Administration Shells

NOTE FROM TC/SC OFFICERS:

Copyright © 2025 International Electrotechnical Commission, IEC. All rights reserved. It is permitted to download this electronic file, to make a copy and to print out the content for the sole purpose of preparing National Committee positions. You may not copy or "mirror" the file or printed version of the document, or any part of it, for any other purpose without permission in writing from IEC.

CONTENTS

1		
2		
3	FOREWORD	4
4	INTRODUCTION	6
5	1 Scope	7
6	2 Normative reference	7
7	3 Terms and definitions, abbreviated terms and acronyms, conventions	7
8	3.1 Terms and definitions	7
9	3.2 Abbreviated terms and acronyms	9
10	3.3 Conventions	9
11	4 Protection Goals	9
12	4.1 Integrity protection	9
13	4.2 Confidentiality protection	10
14	4.3 Availability of data	10
15	5 AAS Security requirements	10
16	5.1 General	10
17	5.2 Security requirements concerning the AAS structure and interface	11
18	5.2.1 Overview	11
19	5.2.2 Requirements regarding Authentication Control (FR1)	11
20	5.2.3 Requirements regarding Use Control (FR2)	13
21	5.2.4 Requirements regarding AAS Integrity (FR3)	14
22	5.2.5 Requirements regarding Data Confidentiality (FR4)	15
23	5.2.6 Requirements regarding restricted data flow (FR5)	15
24	5.2.7 Requirements regarding Timely Response to Events (FR6)	16
25	5.2.8 Requirements regarding Resource Availability (FR7)	16
26	6 AAS security provisions	17
27	6.1 General	17
28	6.2 Access control	17
29	6.2.1 General	17
30	6.2.2 Attribute based access control (ABAC)	17
31	6.2.3 Access tokens	18
32	6.2.4 Access rule model	19
33	6.3 Accountability for AAS Content and Digital Signatures	25
34	6.4 Secure Asset Binding	25
35	Annex A (informative)	27
36	A.1 Assessment of IEC 62443 requirements for AAS structure	27
37	Annex B – Access control rule grammar (normative)	31
38	Annex C – Access control rule examples (informative)	37
39	C.1 Allow READ access for ANONYMOUS to complete API	37
40	C.2 Allow READ access for ANONYMOUS to a list Submodels identified by their	
41	semanticIDs	37
42	C.3 Allow READ and UPDATE for specific authenticated users	37
43	C.4 Allow READ and UPDATE for specific Submodel "submodel1"	38
44	C.5 Use of pre-defines for access control lists, objects, and formula	38
45	C.6 Use of custom claim "BusinessPartnerNumber"	38

46	C.7	Allow READ for all authenticated users of a company for Submodels	
47		Nameplate and TechnicalData	39
48	C.8	Allow READ to Submodels Nameplate and TechnicalData having an ID	
49		starting with “https://example.com” all authenticated users of “company1-	
50		name” between 9:00 and 17:00 UTC	39
51	C.9	Use of FILTER	39
52	C.10	Allow READ access for ANONYMOUS to Submodel interface based on route	40
53		Bibliography	42
54			
55		Figure 1 – AAS security model	11
56		Figure 2 – Access control rules (UML)	19
57			
58		Table 1 – Security Events	13
59		Table 2 – Accountability Events	13
60		Table 3 – <AllAccessPermissionRules> pre-defines	20
61		Table 4 – <AccessPermissionRule>	21
62		Table 5 – <ACL>	21
63		Table 6 – <Right>	22
64		Table 7 – <Access>	22
65		Table 8 – <ClaimAttribute>, <GlobalAttribute>, <ReferenceAttribute>	23
66		Table 9 – <GlobalAttribute>	23
67		Table 10 – <SingleObject>	24
68		Table A.1 – Assessment of IEC 62443 FR1 Authentication Control requirements for	
69		AAS 27	
70		Table A.2 – Assessment of IEC 62443 FR2 Use Control requirements for AAS	28
71		Table A.3 – Assessment of IEC 62443 FR3 System Integrity requirements for AAS	28
72		Table A.4 – Assessment of IEC 62443 FR4 Data confidentiality requirements for AAS	29
73		Table A.5 – Assessment of IEC 62443 FR5 Restricted data flow requirements for AAS	29
74		Table A.6 – Assessment of IEC 62443 FR6 Timely response to events requirements for	
75		AAS 30	
76		Table A.7 – Assessment of IEC 62443 FR7 Resource Availability requirements for AAS	30
77			
78			
79			
80			
81			
82			

INTERNATIONAL ELECTROTECHNICAL COMMISSION

ASSET ADMINISTRATION SHELL FOR INDUSTRIAL APPLICATIONS

Part 3: Security provisions for Asset Administration Shells

FOREWORD

- 1) The International Electrotechnical Commission (IEC) is a worldwide organization for standardization comprising all national electrotechnical committees (IEC National Committees). The object of IEC is to promote international co-operation on all questions concerning standardization in the electrical and electronic fields. To this end and in addition to other activities, IEC publishes International Standards, Technical Specifications, Technical Reports, Publicly Available Specifications (PAS) and Guides (hereafter referred to as "IEC Publication(s)"). Their preparation is entrusted to technical committees; any IEC National Committee interested in the subject dealt with may participate in this preparatory work. International, governmental and non-governmental organizations liaising with the IEC also participate in this preparation. IEC collaborates closely with the International Organization for Standardization (ISO) in accordance with conditions determined by agreement between the two organizations.
- 2) The formal decisions or agreements of IEC on technical matters express, as nearly as possible, an international consensus of opinion on the relevant subjects since each technical committee has representation from all interested IEC National Committees.
- 3) IEC Publications have the form of recommendations for international use and are accepted by IEC National Committees in that sense. While all reasonable efforts are made to ensure that the technical content of IEC Publications is accurate, IEC cannot be held responsible for the way in which they are used or for any misinterpretation by any end user.
- 4) In order to promote international uniformity, IEC National Committees undertake to apply IEC Publications transparently to the maximum extent possible in their national and regional publications. Any divergence between any IEC Publication and the corresponding national or regional publication shall be clearly indicated in the latter.
- 5) IEC itself does not provide any attestation of conformity. Independent certification bodies provide conformity assessment services and, in some areas, access to IEC marks of conformity. IEC is not responsible for any services carried out by independent certification bodies.
- 6) All users should ensure that they have the latest edition of this publication.
- 7) No liability shall attach to IEC or its directors, employees, servants or agents including individual experts and members of its technical committees and IEC National Committees for any personal injury, property damage or other damage of any nature whatsoever, whether direct or indirect, or for costs (including legal fees) and expenses arising out of the publication, use of, or reliance upon, this IEC Publication or any other IEC Publications.
- 8) Attention is drawn to the Normative references cited in this publication. Use of the referenced publications is indispensable for the correct application of this publication.
- 9) IEC draw attention to the possibility that the implementation of this document may involve the use of (a) patent(s). IEC take no position concerning the evidence, validity or applicability of any claimed patent rights in respect thereof. As of the date of publication of this document, IEC had not received notice of (a) patent(s), which may be required to implement this document. However, implementers are cautioned that this may not represent the latest information, which may be obtained from the patent database available at <https://patents.iec.ch>. IEC shall not be held responsible for identifying any or all such patent rights.

IEC 63278-3 has been prepared by IEC technical committee 65: INDUSTRIAL-PROCESS MEASUREMENT, CONTROL AND AUTOMATION. It is an International Standard.

The text of this International Standard is based on the following documents:

Draft	Report on voting
XX/XX/FDIS	XX/XX/RVD

Full information on the voting for its approval can be found in the report on voting indicated in the above table.

The language used for the development of this International Standard is English.

136 This document was drafted in accordance with ISO/IEC Directives, Part 2, and developed in
137 accordance with ISO/IEC Directives, Part 1 and ISO/IEC Directives, IEC Supplement, available
138 at https://www.iec.ch/members_experts/refdocs. The main document types developed by IEC
139 are described in greater detail at <https://www.iec.ch/standardsdev/publications>.

140 The committee has decided that the contents of this document will remain unchanged until the
141 stability date indicated on the IEC website under webstore.iec.ch in the data related to the
142 specific document. At this date, the document will be

143 reconfirmed,
144 withdrawn,
145 replaced by a revised edition, or
146 amended.

147

148

INTRODUCTION

149 This document is the third part of the series "Asset Administration Shell for Industrial
150 Applications". The Asset Administration Shell (AAS) is seen as one interoperable manifestation
151 of a digital twin in manufacturing that facilitates tighter integration within and across the three
152 dimensions of smart manufacturing ecosystems, production system, product and supply chain.
153 The multiple parts of the series will detail on structure, information models, definition of services,
154 and online interfaces, required security aspects and communication languages including
155 mapping contents of OPC UA and AutomationML models.

156 The current planning foresees parts covering the following topics:

- 157 • Asset Administration Shell structure [IEC 63278-1].
- 158 • Information meta model [IEC 63278-2].
- 159 • Security provisions for Asset Administration Shells (this document).
- 160 • Online interfaces to Asset Administration Shells [IEC 63278-5].
- 161 • Communication language among sets of Asset Administration Shells.
- 162 • Specification of content of Asset Administration Shells for various domains.

163 One important goal of the design for the AAS security information model is to provide a well-
164 defined integration with the overall AAS information model. On the one hand smooth and close
165 interoperation between part 2, 3, and part 5 is essential. On the other hand reducing the
166 interdependencies to a minimum will facilitate both the development of the standards and its
167 application. The security model needs to allow easy adaptation of new security technologies to
168 the AAS as they become available. However, features introduced by the AAS security
169 information model shall not break the overall AAS information model and vice versa.
170

ASSET ADMINISTRATION SHELL FOR INDUSTRIAL APPLICATIONS

Part 3: Security provisions for Asset Administration Shells

1 Scope

This part of IEC 63278 specifies the security provisions for the Asset Administration Shell. AAS security controls the exposure of data provided by the AAS to the AAS User Application and the accountability for data the AAS User Application receives from the AAS.

2 Normative reference

The following documents are referred to in the text in such a way that some or all of their content constitutes requirements of this document. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

IEC 62443 (all series), *Industrial communication networks - IT security for networks and systems*

IEC 63278-1:2023, *Asset Administration Shell for industrial applications – Part 1: Asset Administration Shell structure*

IEC 63278-2, *Asset Administration Shell for industrial applications – Part 2: Information meta model*

IEC 63278-5, *Asset Administration Shell for industrial applications – Part 5: Interface*

3 Terms and definitions, abbreviated terms and acronyms, conventions

3.1 Terms and definitions

For the purposes of this document, the terms and definitions given in IEC TR 63283-1, IEC 63278-1, and the following apply.

ISO and IEC maintain terminological databases for use in standardization at the following addresses:

IEC Electropedia: available at <https://www.electropedia.org/>

ISO Online browsing platform: available at <https://www.iso.org/obp>

3.1.1

AAS class attribute

attribute of a Submodel or SubmodelElement

3.1.2

AAS object

structural part of an AAS according to [IEC 63278-2] or fragment thereof that can be uniquely addressed by an AAS query [IEC 63278-5]

Note 1 to entry: Every Referable is an AAS object.

Note 2 to entry: Especially Submodel and SubmodelElements and addressable fragments thereof are AAS objects.

3.1.3**ABAC attribute**

attribute used as basis for attribute-based access control

3.1.4**accountability**

property of a system (including all of its system resources) that ensures the actions of a system entity may be traced uniquely to that entity, which can be held responsible for its actions

[SOURCE: IEC 62443-1-1:2009, 3.2.3]

3.1.5**authenticate**

verify the identity of a user, user device, or other entity, or the integrity of data stored, transmitted, or otherwise exposed to unauthorized modification in an information system, or to establish the validity of a transmission

[SOURCE: IEC 62443-1-1:2009, 3.2.12]

3.1.6**authentication**

security measure designed to establish the validity of a transmission, message, or originator, or a means of verifying an individual's authorization to receive specific categories of information

[SOURCE: IEC 62443-1-1:2009, 3.2.13]

3.1.7**authorization**

right or permission that is granted to a system entity to access a system resource

[SOURCE: IEC 62443-1-1:2009, 3.2.14]

3.1.8**data confidentiality**

property that information is not made available or disclosed to any unauthorized system entity, including unauthorized individuals, entities, or processes

[SOURCE: IEC 62443-1-1:2009, 3.2.37]

3.1.9**data integrity**

property that data has not been changed, destroyed, or lost in an unauthorized or accidental manner

Note 1 to entry: This term deals with constancy of and confidence in data values, not with the information that the values represent or the trustworthiness of the source of the values.

[SOURCE: IEC 62443-1-1:2009, 3.2.38]

3.1.10**security objective**

aspect of security whose purpose is to use certain mitigation measures, such as confidentiality, integrity, availability, user authenticity, access authorization, accountability, etc.

[SOURCE: IEC 62443-1-1:2009, 3.2.109]

3.1.11**data confidentiality**

property that information is not made available or disclosed to any unauthorized system entity, including unauthorized individuals, entities, or processes

[SOURCE: IEC 62443-1-1:2009, 3.2.37]

3.2 Abbreviated terms and acronyms

AAS	Asset Administration Shell
ABAC	attribute-based access control
API	Application Programming Interface
DPP	digital product passport
EBNF	Extended Backus–Naur form
JSON	JavaScript Object Notation
OPC	Open Platform Communications
OPC UA	Open Platform Communications Unified Architecture

3.3 Conventions

The following conventions are used throughout this document:

- All AAS parts and roles are referred to in singular. Statements made in this document either apply to all parts (e.g., all AAS, all Submodels) or it is assumed that the roles in question need to agree on a common rule (e.g., all AAS Responsibles).
- The entity operating the AAS User Application is referred to as user. This does neither imply that the user is a human being nor that the AAS User Application is attended by a human being during operation.
- To avoid confusion this document refers to AAS class attributes for attributes of the classes in the AAS information model (e.g., Property.valueType) and refers to ABAC attributes for attributes related to attribute-based access control.

4 Protection Goals**4.1 Integrity protection**

Consistent data exposure: AAS shall ensure that data is exposed in a consistent way. Data exposure shall only depend on well-defined ABAC attributes independent of the means of access being used. ABAC attributes to be considered are, subject attributes (who is requesting the data), which action is to be performed (e.g., read, write, execute), object attributes (which data is accessed), and environmental conditions (contextual information like time, system state).

Integrity and accountability of data: The AAS user expects the data provided by the AAS to be correct and reliable. AAS shall consider the following:

- Protection against the entry of data by an unauthorized user. Entry/modification of data shall only be possible for an authorized user. AAS should allow to detect unintentional change of data and allow to trace the originator of data.
- Protection against manipulation of stored data. AAS should allow to protect AAS against unauthorized manipulation including the manipulation of origin/authorship. This is especially important in case the AAS is operated by a 3rd party.
- Protection against the manipulation of the AAS structure. It is possible that moving Properties or SubmodelElements between different SubmodelElementCollections results in incorrect interpretation of the provided data.

- Protection against the manipulation of AAS management data. Management data especially includes the data relevant for the control of data exposure (e.g., access control).

Integrity of relation between data and asset: AAS shall protect against pretense of incorrect relations between an asset and its related data stored in the AAS. It is important to know that AAS data belongs to the asset as identified by the asset identifier recorded in the AAS.

Integrity of relation between services and asset: AAS shall protect against pretense of incorrect relations between an asset and asset related services provided by the AAS. It is essential that services announced by the AAS affect the intended asset and that the behavior of the service is described correctly.

4.2 Confidentiality protection

Data leakage protection: Access to information considered sensible by the AAS Responsible shall be controlled by well-defined rules. Only an authorized user shall be able to access sensitive information managed by the AAS. This applies to both,

- actual values, as well as the
- structure and meta-data represented by the AAS (topology described Submodels, SubmodelElements, SubmodelElementCollections, ...).

4.3 Availability of data

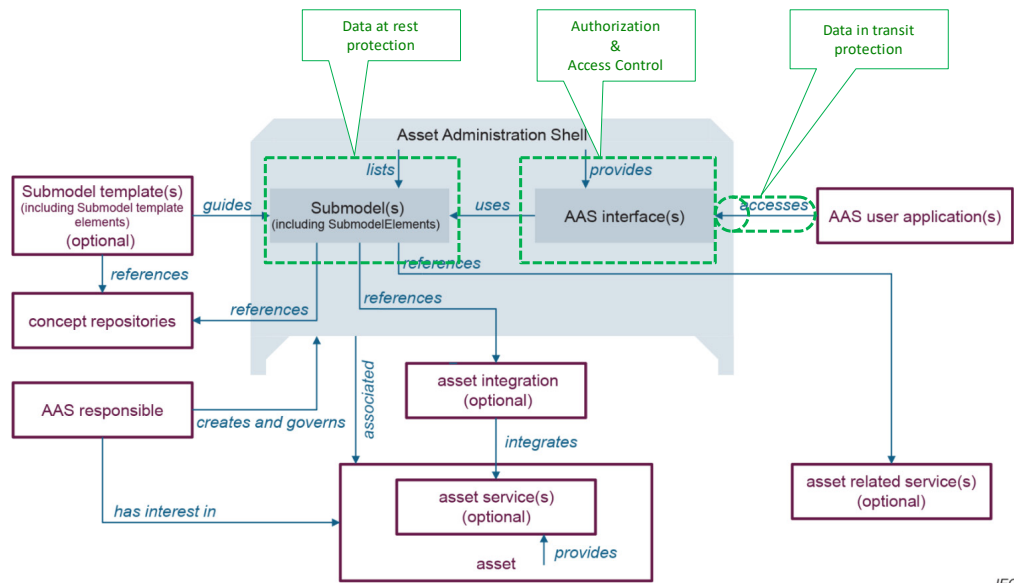
Timely availability of asset data: AAS shall protect against malicious hiding of current data. It shall be possible to determine whether data is sufficiently recent (lost updates) or data has been intentionally removed (malicious rollbacks).

5 AAS Security requirements

5.1 General

AAS security describes a holistic approach to address security concerns related to AAS (see Figure 1):

- Data at rest protection: Protection of integrity and confidentiality information stored in AAS and AAS Submodels.
- Authorization & Access control: AAS Interface ensures that only authorized users are allowed to interact with the AAS and enforces access control according to the rules defined by the AAS Responsible. Authorization of the user is determined based on attributes mapped to the users identity (attribute-based access control, ABAC). These attributes are referred to as ABAC attributes.
- Data in transit protection: Ensures that security properties of AAS information made available via the AAS Interface is maintained during the transit to the AAS User Application.



IEC

Figure 1 – AAS security model

The requirements towards the AAS structure have been derived from the foundational requirements given for systems and components in IEC 62443-3-3 and IEC 62443-4-2 respectively. The selection of requirements applicable for the AAS structure follows the analysis in annex A.1.

5.2 Security requirements concerning the AAS structure and interface

5.2.1 Overview

Following subclauses are based on the seven foundational requirements defined in the IEC 62443 series.

- FR1: Identification and authentication control.
- FR2: Use control.
- FR3: System integrity.
- FR4: Data confidentiality.
- FR5: Restricted data flow.
- FR6: Timely response to events.
- FR7: Resource availability.

5.2.2 Requirements regarding Authentication Control (FR1)

5.2.2.1 Identification and authentication of AAS users

AAS Interface shall ensure the proper identification and authentication of the AAS user accessing information and services offered by AAS.

Authentication of the AAS user shall be based on the authentication of ABAC attributes provided by the AAS User Application on behalf of a user.

Additional ABAC attributes provided by the AAS User Application can be used to provide extended information on the usage context. All ABAC attributes provided by the AAS User Application can be used for authorization decisions.

Subclause 6.2.3 describes an approach to provide ABAC attributes in an authenticated way.

NOTE Derived from IEC 62443-3-3 SR 1.1, IEC 62443-4-2 CR 1.1.

5.2.2.2 Identification and authentication of AAS Interface and AAS User Applications

AAS Interface shall ensure the proper identification and authentication of AAS User Applications accessing information and services offered by AAS. Authentication of the AAS User Application has to include the authentication of attributes provided by the AAS User Application and which affect the behavior of the Asset Administration Shell.

Identification and authentication of the AAS User Application can be achieved by different means, depending on the underlying communication technology and required security level.

IEC 63278-5 should elaborate this for REST API, for example, use of TLS [IETF RFC 5246], [IETF RFC 8446] mutual authentication between the AAS User Application and the AAS Interface.

NOTE Derived from IEC 62443-3-3 SR 1.2, IEC 62443-4-2 CR 1.2.

5.2.2.3 Account management

Asset Administration Shell shall allow to either refer to accounts from an existing service or provide a built-in account database.

The AAS Responsible shall ensure that account information is properly protected and can only be modified by authorized users.

Account management may be made accessible via the AAS Interface.

NOTE Derived from IEC 62443-3-3 SR 1.3, IEC 62443-4-2 CR 1.3.

5.2.2.4 Identifier management

Asset Administration Shell shall support and facilitate the use of secure identities and provide the capability to integrate into a system used to manage these identities across security domains of the different stakeholders interacting along a value chain.

Examples for secure identities are:

- PKI X.509 identities.
- Decentralized Identifiers (DID) and Verifiable Credentials (VC).

NOTE Derived from IEC 62443-3-3 SR 1.4, IEC 62443-4-2 CR 1.4.

5.2.2.5 Authenticator feedback

In case a request send from the AAS User Application to the AAS Interface cannot be processed, AAS Interface shall not disclose any information that would allow conclusions to be drawn about the content or structure of the AAS nor conclusions on why a specific request was rejected.

Additional information to support trouble shooting or debugging may only be made available to dedicated users after authorization for this function.

IEC 63278-5 should elaborate this for REST API, for example, restriction the HTTP status code to a single value, e.g., HTTP-status=404 [IETF RFC 7231]