# ETSI TS 103 815 V1.1.1 (2024-01)


**CYBER;**
**Cyber Security for Consumer Internet of Things;**
**Requirements for Residential Smart Door Locking Devices**

Reference
DTS/CYBER-0058

Keywords
cybersecurity, IoT, security, smart appliance

***ETSI***

650 Route des Lucioles
F-06921 Sophia Antipolis Cedex - FRANCE

Tel.: +33 4 92 94 42 00 Fax: +33 4 93 65 47 16

Siret N° 348 623 562 00017 - APE 7112B
Association à but non lucratif enregistrée à la
Sous-Préfecture de Grasse (06) N° w061004871

# Contents

# Intellectual Property Rights

## Essential patents

IPRs essential or potentially essential to normative deliverables may have been declared to ETSI. The declarations pertaining to these essential IPRs, if any, are publicly available for **ETSI members and non-members**, and can be found in ETSI SR 000 314: *"Intellectual Property Rights (IPRs); Essential, or potentially Essential, IPRs notified to ETSI in respect of ETSI standards"*, which is available from the ETSI Secretariat. Latest updates are available on the ETSI Web server (https://ipr.etsi.org/).

Pursuant to the ETSI Directives including the ETSI IPR Policy, no investigation regarding the essentiality of IPRs, including IPR searches, has been carried out by ETSI. No guarantee can be given as to the existence of other IPRs not referenced in ETSI SR 000 314 (or the updates on the ETSI Web server) which are, or may be, or may become, essential to the present document.

## Trademarks

The present document may include trademarks and/or tradenames which are asserted and/or registered by their owners. ETSI claims no ownership of these except for any which are indicated as being the property of ETSI, and conveys no right to use or reproduce any trademark and/or tradename. Mention of those trademarks in the present document does not constitute an endorsement by ETSI of products, services or organizations associated with those trademarks.

**DECT™**, **PLUGTESTS™**, **UMTS™** and the ETSI logo are trademarks of ETSI registered for the benefit of its Members. **3GPP™** and **LTE™** are trademarks of ETSI registered for the benefit of its Members and of the 3GPP Organizational Partners. **oneM2M™** logo is a trademark of ETSI registered for the benefit of its Members and of the oneM2M Partners. **GSM®** and the GSM logo are trademarks registered and owned by the GSM Association.

**BLUETOOTH®** is a trademark registered and owned by Bluetooth SIG, Inc.

# Foreword

This Technical Specification (TS) has been produced by ETSI Technical Committee Cyber Security (CYBER).

# Modal verbs terminology

In the present document "**shall**", "**shall not**", "**should**", "**should not**", "**may**", "**need not**", "**will**", "**will not**", "**can**" and "**cannot**" are to be interpreted as described in clause 3.2 of the ETSI Drafting Rules (Verbal forms for the expression of provisions).

"**must**" and "**must not**" are **NOT** allowed in ETSI deliverables except when used in direct citation.

# Introduction

As more Smart Door Locking Devices (SDLs) in the home connect to the internet, the cyber security of the Internet of Things becomes a growing concern. People entrust their personal data to an increasing number of online devices and services. Products and appliances that have traditionally been offline are now connected and need to be designates to withstand cyber threats.

The present document brings together widely considered good practise in security for Internet-connected consumer devices in a set of high-level outcome-focused provisions. The objective of the present document is to support all parties involved in the development and manufacturing of consumer IoT with guidance on securing their products.

The present document is a vertical standard of ETSI EN 303 645 [1], which describes and uses a corresponding methodology to modify existing and add new security and data protection requirements specifically for Residential Smart Door Locking Devices. The present document also includes reference to security characteristics defined for building hardware in CEN EN standards.

A separate document will provide guidance on how to assess and assure Residential Smart Door Locking Devices against provisions within the present document.

# 1 Scope

The present document specifies requirements for consumer residential Smart Door Locking Device (SDL) including apps:

- cyber security;
- credential related security; and
- electromechanical security and/or mechanical security.

The present document builds on ETSI EN 303 645 [1] for cyber security requirements, adding additional provisions specific to smart door locking devices.

The present document also builds on other EN standards for credential related security, electromechanical security and mechanical security.

A description of the basic concepts of Residential Smart Door Locking Devices is given in Annex A.

# 2 References

## 2.1 Normative references

References are either specific (identified by date of publication and/or edition number or version number) or non-specific. For specific references, only the cited version applies. For non-specific references, the latest version of the referenced document (including any amendments) applies.

Referenced documents which are not found to be publicly available in the expected location might be found at https://docbox.etsi.org/Reference.

NOTE: While any hyperlinks included in this clause were valid at the time of publication, ETSI cannot guarantee their long term validity.

The following referenced documents are necessary for the application of the present document.

[1] ETSI EN 303 645 (V2.1.1): "CYBER; Cyber Security for Consumer Internet of Things: Baseline Requirements".

[2] EN 1303: "Building hardware - Cylinders for locks - Requirements and test methods" (produced by CEN).

[3] EN 1906: "Building hardware - Lever handles and knob furniture - Requirements and test methods" (produced by CEN).

[4] EN 12209: "Building hardware - Mechanically operated locks and locking plates - Requirements and test methods" (produced by CEN).

[5] EN 14846: "Building hardware - Locks and latches - Electromechanically operated locks and striking plates - Requirements and test methods" (produced by CEN).

[6] EN 16867: "Building hardware - Mechatronic door furniture - Requirements and test methods" (produced by CEN).

[7] EN 15684: "Building hardware - Mechatronic cylinders - Requirements and test methods" (produced by CEN).

[8] FprEN 15685: "Building hardware - Requirements and test methods - Multipoint locks, latches and locking plates - Characteristics and test methods".

[9] EN 1627:2021: "Pedestrian doorsets, windows, curtain walling, grilles and shutters - Burglar resistance - Requirements and classification (produced by CEN)".

## 2.2 Informative references

References are either specific (identified by date of publication and/or edition number or version number) or non-specific. For specific references, only the cited version applies. For non-specific references, the latest version of the referenced document (including any amendments) applies.

NOTE: While any hyperlinks included in this clause were valid at the time of publication, ETSI cannot guarantee their long term validity.

The following referenced documents are not necessary for the application of the present document but they assist the user with regard to a particular subject area.

Not applicable.

# 3 Definition of terms, symbols and abbreviations

## 3.1 Terms

For the purposes of the present document, the terms given in ETSI EN 303 645 [1] and the following apply:

**cloud (cloud storage):** saves data (coming from SDL) and files in an off-site location

**home gateway/router:** physical device that lies between the in-home network and the public network with a primary purpose of managing traffic between these networks

**input devices:** device that allows a user to interact with the door unit

EXAMPLE: PIN pad, RFID reader or a biometric reader.

NOTE: The input device can be integrated with the door unit or can be a separate device.

**SDL back-end on premise:** cloud infrastructure (including pc-server, operating systems, pc-storage, etc.) physically located at the customer site

**SDL cloud-backend:** function that powers front-end and enables users for making operations/configurations on the SDL

**SDL device:** lock used in the context of the Smart Door Lock ecosystem

NOTE: Principles are described in Annex A.

**SDL gateway:** physical device that lies between the internal network (where SDL is located) and the public network with a primary purpose of managing traffic between these networks

## 3.2 Symbols

For the purposes of the present document, the symbols given in ETSI EN 303 645 [1].

## 3.3 Abbreviations

For the purposes of the present document, the abbreviations given in ETSI EN 303 645 [1] and the following apply:

SDL Smart Door Locking device

# 4 Methodology and general requirements

## 4.1 Introduction

ETSI EN 303 645 [1] specifies high-level security and data protection provisions for consumer IoT and their interactions with associated services. Residential Smart Door Locking devices are such consumer IoT devices, but due to higher safety and security needs there is a need for modifications and new requirements specific for Residential Smart Door Locking devices.

Therefore, the provisions from ETSI EN 303 645 [1] are adopted using a corresponding methodology, which is described in clauses 4.2 and 4.3. The provisions are specified in clauses 5 to 7 of the present document.

## 4.2 Handling of provisions

The present document adopts the provisions of ETSI EN 303 645 [1] as a baseline for the Residential Smart Door Locking Devices. The methodology used for the adoption is described in the present clause, which includes different operations to modify provisions from ETSI EN 303 645 [1] and add new provisions specific to the Residential Smart Door Locking Devices.

**All provisions from ETSI EN 303 645 [1] shall apply in the present document, unchanged, to the consumer IoT device in the Residential Smart Door Locking Devices domain, unless otherwise noted in the present document.**

Consumer IoT devices in the Residential Smart Door Locking Devices domain are not constrained devices. Consequently, all provisions from ETSI EN 303 645 [1] regarding constrained devices are adjusted accordingly.

There are different types of modifications indicated by a naming convention as described in clause 4.3. Within clauses 5 and 6 of the present document, the following modifications can be applied to the set of provisions defined in ETSI EN 303 645 [1]:

- **Information:** Providing additional information (in the form of informative text) to an unmodified provision. The original provision in ETSI EN 303 645 [1] is still valid.
- **Promotion:** Promoting a recommendation to a mandatory provision. The wording of the provision remains as in the original provision, but the promoted modal verb is replaced by the new modal verb (e.g. "should" is replaced by "shall"). The original provision in ETSI EN 303 645 [1] is replaced by the promotion and is not valid anymore.
- **Refinement:** Refining a provision with additions or modifications to its normative definition text, including stronger scoping of conditionality. The original scope and spirit remain in force. The original provision in ETSI EN 303 645 [1] is replaced by the refinement and is not valid anymore.

NOTE: A refinement can be used to scope the conditionality of a provision, i.e. to remove one or more conditions from the provision, as part of the clarification on the provision's constraints.

- **Extension:** Extending an existing provision with one or more new sub-provisions. The original provision in ETSI EN 303 645 [1] is still valid.
- **Substitution:** Replacing a recommendation that is not applicable for the Residential Smart Door Locking Devices with another recommendation of equivalent effect (that provides, possibly in combination with other recommendations or provisions, the same security outcome as the replaced recommendation). The original provision in ETSI EN 303 645 [1] is replaced by the substitution and is not valid anymore.
- **Exclusion** (only possible for recommendations and conditional provisions): Declaring a recommendation or conditional provision as "not applicable" for the Residential Smart Door Locking Devices. The original provision in ETSI EN 303 645 [1] is excluded and is not valid anymore.

The present document allows to define new provisions within clause 7 that are not covered in ETSI EN 303 645 [1]. There is one type of new provisions, that is also covered by the naming convention in clause 4.3:

- **Addition:** Defining a new provision specific to the Residential Smart Door Locking Devices that cannot be linked to any provision in ETSI EN 303 645 [1].

## 4.3 Naming conventions

The provisions in the present document are named following the naming conventions described in the present clause.

Each provision contains an acronym representing the Residential Smart Door Locking Devices. The acronym for the Residential Smart Door Locking Devices is set to "SDL".

Names for provisions that are specific to the present document are constructed as follows:

- The name starts with the string "Provision" to which the acronym "SDL" is appended.
- A provision identifier (id) is appended. An example id is 5.1-1.
- One or more suffixes are appended (according to the types of provisions as described in clause 4.2).

NOTE: A provision can be at the same time promoted and refined, in which case the two suffixes are appended to its name.

- For provisions that are extensions, an alphabetical index is appended, that is unique to the provision, for example, "-a". The alphabetical index is appended only in cases where there is more than one extension to a given provision.

The following list describes the suffixes depending on the type of the provision as described in clause 4.2:

- **Information:** The id is the id of the original provision in ETSI EN 303 645 [1] additional informative information is provided for. The suffix is "(information)".
- **Promotion:** The id is the id of the original provision in ETSI EN 303 645 [1] that is promoted. The suffix is "(promoted)".
- **Refinement:** The id is the id of the original provision in ETSI EN 303 645 [1] that is refined. The suffix is "(refined)".
- **Extension:** The id is the id of the original provision in ETSI EN 303 645 [1] that is extended. The suffix is "(extended)".
- **Substitution:** The id is the id of the original provision in ETSI EN 303 645 [1] that is substituted. The suffix is "(substituted)".
- **Exclusion:** The id is the id of the original provision in ETSI EN 303 645 [1] that is excluded. The suffix is "(excluded)".
- **Addition:** The id is a new and unique id added in clause 7 that reflects the clause in which it is defined. The suffix is "(added)".

## 4.4 Reporting implementation

**Provision SDL 4-1 (extended):** A justification shall be recorded for each recommendation in the present document that is considered to be not applicable for or not fulfilled by the SDL device.

# 5 Adapted cyber security provisions for Residential Smart Door Locking Devices

## 5.1 No universal default passwords

Existing provisions from ETSI EN 303 645 [1], clause 5.1 are modified as follows:

**Provision SDL 5.1-5 (refined):** The SDL device shall have mechanisms available which make brute force attacks on authentication mechanisms via network interfaces impracticable.

EXAMPLE 1: The SDL device limits the number of authentication attempts within a certain time interval.

EXAMPLE 2: The SDL device introduces a delay after a failed authentication attempt. The delay increases after each subsequent failed authentication attempt.

## 5.2 Implement a means to manage reports of vulnerabilities

Existing provisions from ETSI EN 303 645 [1], clause 5.2 are modified as follows:

**Provision SDL 5.2-2 (promoted) (refined):** Disclosed vulnerabilities shall be acted on in a timely manner.

NOTE: The manufacturer's policy provides the corresponding information.

EXAMPLE: The timeline for acting on a vulnerability can depend on factors such as the type of product, the risk associated with the vulnerability, and the complexity of the mitigation plan.

**Provision SDL 5.2-3 (promoted):** Manufacturers shall continually monitor for, identify and rectify security vulnerabilities within the SDL Device and security relevant SDL services. they sell, produce, have produced and services they operate during the defined support period.

EXAMPLE: The manufacturer performs security tests and vulnerability scans against public vulnerability databases for devices, mobile apps and web services. This includes third party components used in the product.

## 5.3 Keep software updated

Existing provisions from ETSI EN 303 645 [1], clause 5.3 are modified as follows:

**Provision SDL 5.3-1 (promoted):** All manufacturer-controlled software components shall be securely updateable.

**Provision SDL 5.3-1 (extended)-a:** All security relevant associated services of the SDL in control of the device manufacturer shall be kept up to date.

**Provision SDL 5.3-1 (extended)-b:** An update of the SDL device shall not change the locking status of the SDL device.

NOTE: A lock which was closed before an update is still closed during and after an update, unless changed by an authorized user

**Provision SDL 5.3-2 (excluded):** The provision is covered by Provision SDL 5.3-1 (promoted) and shall not apply.

**Provision SDL 5.3-6 (extended):** The user shall have the option to be notified of updates for SDL mobile application.

**Provision SDL 5.3-7 (extended)-a:** The order of the algorithms offered in an algorithm negotiation should follow best practice cryptography.

**Provision SDL 5.3-7 (extended)-b:** The SDL device shall prevent the installation of update versions older than the currently installed version.

**Provision SDL 5.3-9 (promoted):** The SDL device shall verify the authenticity and integrity of software updates.

**Provision SDL 5.3-12 (promoted) (refined):** The SDL device shall notify the user when the application of a software update will disrupt the basic functioning of the SDL device. When the application of a software update will disrupt the basic functioning of the SDL device, the user should be informed about the approximate expected duration for which the device will be offline.

**Provision SDL 5.3-12 (extended)-a:** The notification shall include information about the criticality of the update, the impact on the functioning of the SDL device, and the expected duration of the disruption.

**Provision SDL 5.3-12 (extended)-b:** The notification shall be displayed to the user in a recognizable and apparent manner.

EXAMPLE: The notification is visible on a web interface or mobile app.

**Provision SDL 5.3-14 (excluded):** The provision is not applicable for the Residential Smart Door Locking Devices and shall not apply.

**Provision SDL 5.3-15 (excluded):** The provision is not applicable for the Residential Smart Door Locking Devices and shall not apply.

## 5.4 Securely store sensitive security parameters

Existing provisions from ETSI EN 303 645 [1], clause 5.4 are modified as follows:

**Provision SDL 5.4-1 (info):** Sensitive security parameters that are used for locking or unlocking need a secure storage.

## 5.5 Communicate securely

Existing provisions from ETSI EN 303 645 [1], clause 5.5 are modified as follows:

**Provision SDL 5.5-1 (extended):** The communications between separate components of a SDL device shall be encrypted and authenticated using best practice cryptography.

**Provision SDL 5.5-2 (extended):** The communications between a SDL device and its associated services shall be encrypted and authenticated using best practice cryptography.

**Provision SDL 5.5-5 (information):** Enabling, disabling or postponing installation of security updates and changes in audit trail is a security-relevant change.

## 5.6 Minimize exposed attack surfaces

Existing provisions from ETSI EN 303 645 [1], clause 5.6 are modified as follows:

**Provision SDL 5.6-3 (promoted):** SDL device hardware shall not unnecessarily expose physical interfaces to attack.

NOTE: See Annex C.

**Provision SDL 5.6-5 (promoted):** The manufacturer shall only enable software services that are used or required for the intended use or operation of the SDL device.

**Provision SDL 5.6-7 (promoted):** Software on the SDL Device shall run with least necessary privileges, taking account of both security and functionality.

**Provision SDL 5.6-8 (promoted):** The SDL device shall include a hardware-level access control mechanism for memory.

**Provision SDL 5.6-9 (promoted)** The manufacturer shall follow secure development processes for software deployed on the SDL device.

## 5.7 Ensure software integrity

No modifications to the provisions from ETSI EN 303 645 [1], clause 5.7 are defined in the present document.

## 5.8 Ensure that personal data is secure

Existing provisions from ETSI EN 303 645 [1], clause 5.8 are modified as follows:

**Provision SDL 5.8-1 (promoted):** The confidentiality of personal data transiting between a SDL device and a service, especially associated services, shall be protected, with best practice cryptography.

**Provision SDL 5.8-2 (information):** SDL device audit logs are sensitive personal data.

**Provision SDL 5.8-2 (extended)-a:** The confidentiality of audit logs communicated between the SDL device and associated services shall be protected by end-to-end encryption.

## 5.9 Make systems resilient to outages

Existing provisions from ETSI EN 303 645 [1], clause 5.9 are modified as follows:

**Provision SDL 5.9-1 (extended)-a:** It shall be possible for the user to lock or unlock the SDL device in the event of a loss of power.

EXAMPLE: The SDL device could operate on battery power or have a mechanical means to lock or unlock.

**Provision SDL 5.9-1 (extended)-b:** The SDL device shall operate in a defined state after a denial of service attack.

**Provision SDL 5.9-1 (extended)-c:** A DoS attack shall not change the locking status of the device.

NOTE: A lock which is closed before a DoS attack is still closed during and after the DoS attack, unless changed by an authorized user.

**Provision SDL 5.9-1 (extended)-e:**-In the case where the SDL device is permanently and directly connected to a network, it shall locally store all data that it usually transmits through the network during a power loss of the network and send this locally stored information once it regains network connectivity.

**Provision SDL 5.9-2 (promoted) (refined):** The SDL device shall remain operating and locally functional in the case of a loss of network access and shall recover cleanly.

**Provision SDL 5.9-2 (information):** Remaining operating and locally functional as well as recovering cleanly includes the locking status of the lock to persist during outage of network or power in the status as it was before, unless changed by an authorized user.

## 5.10 Examine system telemetry data

Existing provisions from ETSI EN 303 645 [1], clause 5.10 are modified as follows:

**Provision SDL 5.10-1 (promoted):** If telemetry data is collected from SDL device and services, such as usage and measurement data, it shall be examined for security anomalies.

## 5.11 Make it easy for users to delete user data

Existing provisions from ETSI EN 303 645 [1], clause 5.11 are modified as follows:

**Provision SDL 5.11-1 (substituted):** The user shall be provided with functionality such that personal user data, except for data required for security purposes including immutable audit logs, can be erased from the device in a simple manner.

NOTE: Normal individual users that are authorized to unlock the door may not have the possibility to erase themselves from all memories and databases because of immutable audit trail.

**Provision SDL 5.11-3 (promoted):** Users shall be given clear instructions on how to delete their personal data.

**Provision SDL 5.11-4 (promoted):** Users shall be provided with clear confirmation that personal data has been deleted from services, devices and applications.

## 5.12 Make installation and maintenance of devices easy

Existing provisions from ETSI EN 303 645 [1], clause 5.12 are modified as follows:

**Provision SDL 5.12-1 (information):** Security best practice includes specifying default options that are appropriately secure.

**Provision SDL 5.12-2 (promoted):** The manufacturer shall provide users with guidance on how to securely set up their device.

**Provision SDL 5.12-2 (extended):** Security options shall be explained during the installation procedure itself with all advantages and disadvantages.

**Provision SDL 5.12-3 (promoted):** The manufacturer shall provide users with guidance on how to check whether their device is securely set up.

## 5.13 Validate input data

No modifications to the provisions from ETSI EN 303 645 [1], clause 5.13 are defined in the present document.

# 6 Adapted data protection provisions for Residential Smart Door Locking Devices

Existing provisions from ETSI EN 303 645 [1], clause 6 are modified as follows:

**Provision 6-2 (extended):** Collection and processing of telemetry data from the SDL device and services shall be based on the user's consent.

# 7 Additional cyber security provisions for Residential Smart Door Locking Devices

## 7.1 Storing personal data securely

**Provision SDL 7.1-1 (added):** Personal data in persistent storage of the SDL shall be stored securely by the device.

**Provision SDL 7.1-2 (added):** Personal data stored by the SDL and/or associated services shall only be accessible by an authorized entity.

## 7.2 System failure documentation

**Provision SDL 7.2-1 (added):** Network and power losses shall be documented.

NOTE: Audit trail can be considered.

## 7.3 Web and SDL mobile applications

**Provision SDL 7.3-1 (added):** The manufacturer should follow the latest version of OWASP security verification standard for web and SDL mobile applications.

# Annex A (informative): Basic concepts, threat models, risk analysis

## A.1 Drawing/overview of a Residential Smart Door Locking Devices

### A.1.1 General

Residential Smart Door Locking Device is a lock designed to perform locking and unlocking a door when it receives such instructions from an authorized device using a wireless protocol and cryptographic key to execute the authorization process. Principles are described in Figure A.1.

### A.1.2 Interfaces

Smart Door Locking Devices interfaces are in principle described in Figure A.1.

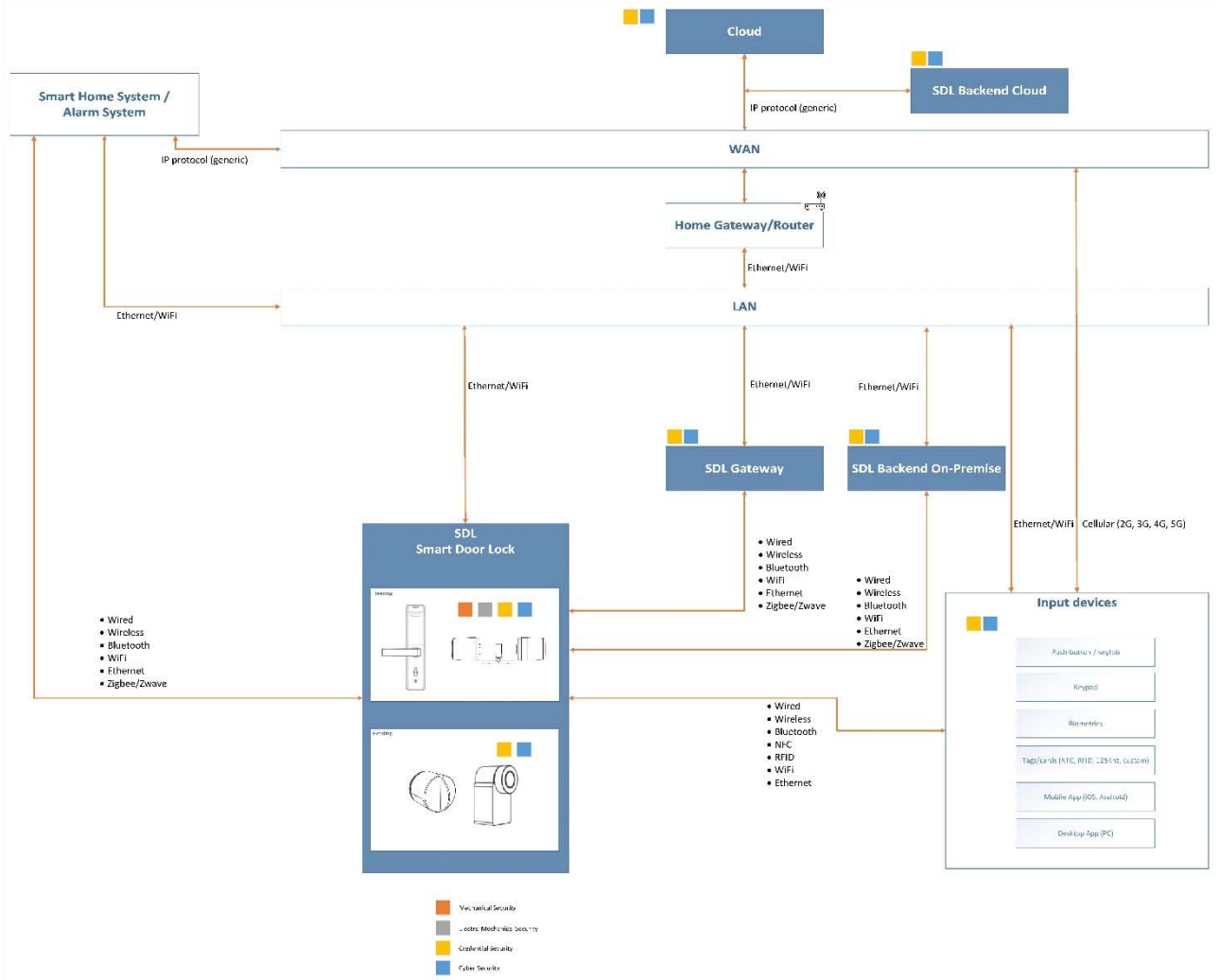


**Figure A.1: Smart Door Locking Device interfaces**

# A.2 Components of a Residential Smart Door Locking Devices solution

## A.2.1 Components in a Residential Smart Door Locking Devices

Typical components in a smart door locking solutions:

**Door Unit/Smart Door Actuator:** Enables the opening mechanism of a door lock. This can be a motor driving a key, a thumb-turn or a clutch mechanism enabling the usage of the door handle or another opening element. The actuator gets controlled by the door unit where the decision gets taken to change the status of the lock.

**Mobile Phone App (input devices):** Application allows the user to interact with the Door unit. This can be commands to change the status of the door (will activate the actuator) or for settings of the Smart Door Locking Device (like door opening time, Autolock/unlock features, etc.).

Often is the user management also handled in the application (add user, delete user, send invitation to guest, etc.).

The communication between the mobile applications can be done via different protocols/interfaces. This can be Bluetooth®, NFC® or Wi-Fi®.

**SDL Backend-Cloud:** Server application allows the user(s) to store their user account details and settings/information about one or multiple Smart Door Locking Devices dedicated to this user. The backend (cloud) is normally where a so called cloud-to-cloud integration is made with another system, as an enabler. It is however, typically a decision made by the SDL owner to activate such an integration or not.

The backend is also typically the source for providing new firmware for the SDL (also known as Firmware Over The Air, (FOTA)).

It is also used for remote commands when the Door Unit has a connection to the backend. The connection can be made via the mobile phone or via Wi-Fi® with or without a bridge (depending on the capability of the door unit).

Differently from the cloud (storage), backend cloud enables users (owners of the SDL etc) to operate/configurate the SDL.

**Reading device (Input device):** A reading device can be a PIN pad, RFID reader, Biometric reader or any devices which allows the user to present a credential (non-mechanical key). The reading device may be integrated with the Door Unit, or may be an entirely separate device that communicates with the door unit. This can be done wired or wireless. Depending of the features of the Door Unit, and how it has been setup, it may (with a greater or lesser certainty) be used to identify the user of such credential.

**Gateway:** Although often not strictly necessary for basic functionality, frequently to enjoy the full feature set experience of an SDL, the user will benefit from a bridge device. For all remote use-cases (when the user is further away from their SDL than the aforementioned radios will reach), or when additional features rely on backend (cloud) to fulfil on their promise.

A bridge/gateway simply assists in bringing the SDL on-line and available to communicate with. With the exception of SDLs with integrated Wi-Fi®, all other radio technologies typically need to be transcoded (bridged) between the radio technology used by the SDL and (most typically) the home Access Point (as known as internet router). This is true for BLE, Zigbee®, Z-Wave or other proprietary radios, all needing to transmit via Wi-Fi® to the home Access Point. NFC® is such short range it does not lend itself for this use-case.

**Cloud storage:** it saves data and files in an off-site location. It can be accessed through the public internet. Data transferred in the off-site storage becomes the responsibility of a third-party cloud provider. The provider hosts, secures, manages, and maintains the servers and associated infrastructure and ensures (usually guaranteeing a certain QoS-Quality of service) the access to the data whenever it is needed.

**Home Gateway/Router:** It manages the data/traffic coming from the in-home networks (e.g. LAN) delivering the data/traffic to the public networks (e.g. WAN). Typically, it has a dedicated software (firewall or similar) to protect LAN from external cyber-attacks (possible coming from WAN).

**SDL Back-end on Premise:** Usually it is used on dedicated appliances, for instance where the customer (e.g. for security reasons) needs to have a local/private network and the physically infrastructure in their site. Usually backend is not enabled to directly links LAN in the public network (WAN), it may require authorization by the customer.

### A.2.2 Interfaces

There are multiple interfaces between the different components within the SDL solution implemented with different technologies such as BLE, WLAN, RFID, etc.

For example the following interfaces can occur:

- BLE - used between the mobile phone and the Door Unit or between the door unit and different peripherals/accessories like an external reading device. BLE can also be used to communicate with a bridge device.
- Wi-Fi® used for the communication between the bridge device and the home Access Point (ultimately to the backend), an SDL with supporting Wi-Fi® is expected to communicate directly with the home Access Point.
- Radio-Frequency Identification (RFID) - used for key exchange between device carrying the credential (tag, card, mobile phone) and the Reading Device.

The data exchanged through the different interfaces is described below and Figure A.1:

1) Credentials (mobile app/fobs /cards) <--> Reading Device/Door Unit

   i. User's credentials for accessing the door.

2) SDL ←→Input Devices ←→ Cloud Backend:

   ii. User keys are transferred from the backend cloud to the user's mobile app.
   iii.
      a. SDL Operations (credential), e.g. Opening, closing/securing SDL.
      b. SDL Configurations, e.g. Enabling or Removing guest/users, configure opening time, automatically lock&secure in selected date e time, etc.
      c. SDL FW update files.

3) SDL ←→Input Devices ←→ Cloud (Storage):

   a. SDL maintenance data, e.g. battery status of the SDL, historical events registrations, list of the users and owners, any kind of alarm messages from the SDL (opening failure, closing failures, etc.).

4) SDL ←→SmartHome or Alarm systems:

   a. Credential for opening/closing SDL.

5) SDL ←→ SDL backend on premise

   a. SDL Operations (credentials), e.g. Opening, closing/securing SDL.
   b. SDL Configurations, e.g. Enabling or Removing guest/users, configure opening time, automatically lock and secure in selected date e time, etc.
   c. SDL FW update files.

## A.3 Use cases/applications

There are a number of user cases on how to operate a smart locking device.

They can be grouped into:

- Operation of the SDL, e.g.:
  - Lock and unlock the door either with an app, key pad, GPS position, biometric or other means.

  - Temporary access for friends or family while occupants away.
  - Single time access for deliveries or service.
- Configuration of the SDL, e.g.:
  - Set-up list of users, eventually with authorized periods of time.
  - Set-up user modes.
  - Adding/removing a single occupant to SDL use.
  - Parental monitoring of child use.
  - Change of ownership of dwelling, send entry code to other users.
  - QR code link to installation/use instructions.
  - Software update of SDL.
  - Reset to default settings.
  - Pairing and unpairing mechanism (SDL with credential).
- Information from the SDL, e.g.:
  - Locked/unlocked, close/open status.
  - Use of stolen credential.
  - Activity record of all operations (audit trail).
  - Error codes.
  - Mechanical forcing or circumvention of lock.
  - Detection of malicious use of the SDL in abusive relationships.
  - Status of connections (network status).

A Smart Door Locking Device adds convenience to the users of a property. Convenience is different to different people, not having to carry a physical key, may be attractive enough for some. A more advanced convenience may be to allow some flexibility in giving access to enter the home and when. Unlike a physical key, digital credentials can be sent/transferred from one user to another without them physically meeting. Digital credentials can have associated schedules, allowing or denying positive use of the credential based on date-/time stamp criteria (while an owner is allowed to enter 24/7, a guest can be restricted to a certain time frame (e.g. from the 1st to the 14th of June) or recurring (every Tuesday between 2 and 4 pm).

A Smart locking device also increases the security of the entrance point by secure locking (latch and bold). Often SDLs have features such as allowing to revoke credentials if they are perceived to be lost or no longer trusted.

In addition, a Smart Locking device can give information to the user/owner who entered when the home. As there is a unique identifier associated with each event this can be used to initiate other actions from a connected device (integration to a Smart Home, Smart Alarm or Smart Lighting system required). Meanwhile receiving a notification event, confirming a family member has arrived home, after e.g. school, can be re-assuring to a parent.

## A.4 Thread methodology based on use cases or interface

There are different methodologies for a Smart Door Locking device:

1) Mechanical attacks - picking, drilling, pulling, bumping, freezing (with ice spray) and rotation attack.

2) Electromechanical: Try to change the status of the actuator with a magnet/electromagnet, electromagnetic field, high voltage pulse.

3) Credential related attacks: Copy of a credential, recording of communication and replay it afterwards, relay attacks (hidden communication between the original credential and SDL by use of RF extender).

4) Cyber security: Attack surfaces identified for the SDL ecosystem are:

- o Attacks against the hardware (reading devices/door units/gateways):
  - Threats: compromise the HW physically by compromising for instance the keys, firmware, or any kind of data, or the interfaces which allows it to gain control of the SDL provoking for instance unintentional unlocking, denial of service, removing events, etc.
  - Mitigation: provisions from ETSI EN 303 645 [1] and the additional provisions included within the SDL standard.
  - Attacks against mobile app.
- Threats: compromise the mobile application to obtain control of the SDL or try to compromise the backend service (denial of service, access to non-authorized backend services, etc.).
- Mitigation: OWASP provisions referenced within SDL standard:
  - Attack against cloud backend.
- Threats: compromise the backend service from an availability, confidentiality or integrity perspective.
- Mitigation: OWASP provisions referenced within SDL standard.

## A.5 Security levels of Smart Door Locking Devices

**Table A.1: Different types of SDL**

| Type of product | Cyber security | Credential security | Mechanical/electromechanical security |
|---|---|---|---|
| Full lock set | ETSI EN 303 645 [1] | Reference to EN hardware standards | EN 12209 [4], EN 14846 [5], EN 16867 [6], EN 1303 [2], EN 15684 [7], FprEN 15685 [8] or EN 1906 [3] |
| Handle set | | | EN 1906 [3] or EN 16867 [6] |
| Knob cylinder | | | EN 15684 [7] |
| Electronic cylinder | | | EN 15684 [7] |
| Lock adaptor with cylinder | | | EN 1303 [2] or EN 15684 [7] |
| Lock adaptor | | | No EN available |

According to the present document Smart Door Locking Devices will be classified according to the following principles:

- For cyber security: pass or fail according to clause 5.
- Credential related security: two levels, level 1 and level 2. The requirements are described in clause C.3.
- Smart Door Locking Devices where the mechanical and electromechanical security can be assessed according to relevant and existing building hardware standards, see Table A.1. In this case the levels are defined, according to clauses C.1 and C.2.

The manufacturer determines the overall grade of its product by identifying the lowest grade or level amongst the grades or levels of each security field.

The final classification is obtained taking the minimum grade from each applicable standard.

# Annex B (informative): Implementation conformance statement pro forma

## B.1 The right to copy

Notwithstanding the provisions of the copyright clause related to the text of the present document, ETSI grants that users of the present document may freely reproduce the implementation conformance statement pro forma in this annex so that it can be used for its intended purposes and may further publish the completed implementation conformance statement.

## B.2 Implementation conformance statement

**Table B.1: Implementation Conformance Statement**

| Clause number and title | | | |
|---|---|---|---|
| **Reference** | **Status** | **Support** | **Detail** |
| **4 Reporting implementation** | | | |
| Provision SDL 4-1 (extended) | M | | |
| **5.1 No universal default passwords** | | | |
| Provision 5.1-1 (ETSI EN 303 645) | M C (1) | | |
| Provision 5.1-2 (ETSI EN 303 645) | M C (2) | | |
| Provision 5.1-3 (ETSI EN 303 645) | M C (5) | | |
| Provision 5.1-4 (ETSI EN 303 645) | M C (5) | | |
| Provision SDL 5.1-5 (refined) | M | | |
| **5.2 Implement a means to manage reports of vulnerabilities** | | | |
| Provision 5.2-1 (ETSI EN 303 645) | M | | |
| Provision SDL 5.2-2 (promoted) | M | | |
| Provision SDL 5.2-3 (promoted) | M | | |
| **5.3 Keep software updated** | | | |
| Provision SDL 5.3-1 (promoted) | M | | |
| Provision SDL 5.3-1 (extended)-a | M C (26) | | |
| Provision SDL 5.3-1 (extended)-b | M C (26) | | |
| Provision SDL 5.3-2 (excluded) | M | | |
| Provision 5.3-3 (ETSI EN 303 645) | M C (9) | | |
| Provision SDL 5.3-4 (extended) | M C (27) | | |
| Provision 5.3-5 (ETSI EN 303 645) | R C (9) | | |
| Provision 5.3-6 (ETSI EN 303 645) | R C (6, 9) | | |
| Provision SDL 5.3-7 (extended)-a | R C (28) | | |
| Provision SDL 5.3-7 (extended)-b | R C (28) | | |
| Provision 5.3-8 (ETSI EN 303 645) | M C (9) | | |
| Provision SDL 5.3-9 (promoted) | M | | |
| Provision 5.3-10 (ETSI EN 303 645) | M C (8, 9) | | |
| Provision 5.3-11 (ETSI EN 303 645) | R C (9) | | |
| Provision SDL 5.3-12 (promoted) (refined) | M C (9) | | |
| Provision SDL 5.3-12 (extended)-a | R C (9) | | |
| Provision SDL 5.3-12 (extended)-b | M C (9) | | |
| Provision 5.3-13 (ETSI EN 303 645) | M | | |
| Provision 5.3-16 (ETSI EN 303 645) | M | | |
| **5.4 Securely store sensitive security parameters** | | | |
| Provision 5.4-1 (ETSI EN 303 645) | M C (11) | | |
| Provision SDL 5.4-1 (extended)-a | M C (29) | | |
| Provision SDL 5.4-1 (extended)-b | M C (27) | | |
| Provision 5.4-2 (ETSI EN 303 645) | M C (7) | | |
| Provision 5.4-3 (ETSI EN 303 645) | M | | |
| Provision 5.4-4 (ETSI EN 303 645) | M C (12) | | |
| **5.5 Communicate securely** | | | |
| Provision 5.5-1 (ETSI EN 303 645) | M | | |
| Provision SDL 5.5-1 (extended) | M C (30) | | |

| Clause number and title | | | |
|---|---|---|---|
| **Reference** | **Status** | **Support** | **Detail** |
| Provision SDL 5.5-2 (extended) | M | | |
| Provision 5.5-3 (ETSI EN 303 645) | R | | |
| Provision 5.5-4 (ETSI EN 303 645) | R C (13) | | |
| Provision 5.5-5 (information) | M C (14) | | |
| Provision 5.5-6 (ETSI EN 303 645) | R C (15) | | |
| Provision 5.5-7 (ETSI EN 303 645) | M C (16) | | |
| Provision 5.5-7 (ETSI EN 303 645) | M | | |
| Provision 5.5-8 (ETSI EN 303 645) | M C (17) | | |
| **5.6 Minimize exposed attack surfaces** | | | |
| Provision 5.6-1 (ETSI EN 303 645) | M | | |
| Provision 5.6-2 (ETSI EN 303 645) | M | | |
| Provision SDL 5.6-3 (promoted) | M | | |
| Provision 5.6-4 (ETSI EN 303 645) | M C (10) | | |
| Provision SDL 5.6-5 (promoted) | M | | |
| Provision 5.6-6 (ETSI EN 303 645) | R | | |
| Provision SDL 5.6-7 (promoted) | M | | |
| Provision SDL 5.6-7 (extended) | R | | |
| Provision SDL 5.6-8 (promoted) | M | | |
| Provision SDL 5.6-9 (promoted) | M | | |
| **5.7 Ensure software integrity** | | | |
| Provision 5.7-1 (ETSI EN 303 645) | R | | |
| Provision 5.7-2 (ETSI EN 303 645) | R | | |
| **5.8 Ensure that personal data is secure** | | | |
| Provision SDL 5.8-1 (promoted) | M C (18) | | |
| Provision SDL 5.8-2 (information) | M C (19) | | |
| Provision 5.8-3 (ETSI EN 303 645) | M C (20) | | |
| **5.9 Make systems resilient to outages** | | | |
| Provision SDL 5.9-1 (extended)-a | M | | |
| Provision SDL 5.9-1 (extended)-b | M | | |
| Provision SDL 5.9-1 (extended)-c | M | | |
| Provision SDL 5.9-1 (extended)-d | M | | |
| Provision SDL 5.9-1 (extended)-e | M | | |
| Provision SDL 5.9-2 (promoted) (refined) | M | | |
| Provision SDL 5.9-2 (information) | R | | |
| Provision 5.9-3 (ETSI EN 303 645) | R | | |
| **5.10 Examine system telemetry data** | | | |
| Provision SDL 5.10-1 (promoted) | M C (3) | | |
| **5.11 Make it easy for users to delete user data** | | | |
| Provision SDL 5.11-1 (refined)-a | M C (21) | | |
| Provision SDL 5.11-1 (extended)-b | M C (21) | | |
| Provision 5.11-2 (ETSI EN 303 645) | R C (22) | | |
| Provision SDL 5.11-3 (promoted) | M C (23) | | |
| Provision SDL 5.11-4 (promoted) | M C (23) | | |
| **5.12 Make installation and maintenance of devices easy** | | | |
| Provision SDL 5.12-1 (information) | R | | |
| Provision SDL 5.12-2 (promoted) | M | | |
| Provision SDL 5.12-2 (extended) | M | | |
| Provision SDL 5.12-3 (promoted) | M | | |
| Provision SDL 5.12-3 (extended) | M | | |
| **5.13 Validate input data** | | | |
| Provision 5.13 (ETSI EN 303 645) | M C (24) | | |
| **6 Data protection provisions for consumer IoT** | | | |
| Provision 6-1 (ETSI EN 303 645) | M C (25) | | |
| Provision SDL 6-2 (extended) | M C (4) | | |
| Provision 6-3 (ETSI EN 303 645) | M C (4) | | |
| Provision 6-4 (ETSI EN 303 645) | R C (3) | | |
| Provision 6-5 (ETSI EN 303 645) | M C (3) | | |
| **7.1 Bug fixing process** | | | |
| Provision SDL 7.1-1 (added) | M | | |
| Provision SDL 7.1-2 (added) | M | | |
| **7.2 Periodic security reviews** | | | |
| Provision SDL 7.2-1 (added) | M | | |

| Clause number and title | | | |
|---|---|---|---|
| **Reference** | **Status** | **Support** | **Detail** |
| **7.3 Storing personal data securely** | | | |
| Provision SDL 7.3-1 (added) | M C (22) | | |
| Provision SDL 7.3-3 (added) | M C (22, 26) | | |
| **7.4 System failure documentation** | | | |
| Provision 7.4-1 (ETSI EN 303 645) | M | | |
| **7.5 Web and mobile applications** | | | |
| Provision 7.5-1 (ETSI EN 303 645) | R C (31) | | |

**Conditions**

1) passwords are used;
2) pre-installed unique per device passwords are used;
3) telemetry data being collected;
4) personal data is processed on the basis of consumers' consent;
5) the device allowing user authentication;
6) the device supports automatic updates and/or update notifications;
7) a hard-coded unique per device identity is used for security purposes;
8) updates are delivered over a network interface;
9) an update mechanism is implemented;
10) a debug interface is physically accessible;
11) sensitive security parameters are stored persistently;
12) critical security parameters used for integrity and authenticity checks of software updates in device software or for protection of communication with associated services in device software exist;
13) access to device functionality via a network interface in the initialized state is possible;
14) device functionality that allows security-relevant changes in configuration via a network interface exists;
15) critical security parameters are transmitted;
16) critical security parameters are transmitted via remotely accessible network interfaces;
17) critical security parameters relating to the device exist;
18) personal data is transmitted between a device and a service;
19) sensitive personal data is transmitted between a device and a service;
20) external sensing capabilities exist;
21) user data is stored on the device;
22) personal data is stored on associated services;
23) personal data is stored;
24) data input via user interfaces or transferred via APIs or between networks in services and devices is supported;
25) personal data is processed;
26) a cloud background system is used;
27) a mobile app is used;
28) algorithm negotiation is used;
29) cryptographic keys are stored persistently;
30) audit trails are transmitted;
31) the device uses web or mobile applications.

# Annex C (normative): Non-cyber security aspects for Residential Smart Door Locking Devices

## C.1 Mechanical security

Applicable mechanical security for SDL door units is given in CEN EN standards. Depending on the type of SDL different mechanical requirements covered in different CEN EN standards shall apply for these door units.

The mechanical security, when applicable, for a SDL is defined in three SDL grades making reference to the relevant clauses and mechanical security grades in the CEN EN standards according to Table C.1 to C.5.

EXAMPLE: A SDL door units consists of an mechatronic cylinder that is combined with a mechanical lock and mechanical door furniture. The mechatronic cylinder has level 3 according to Table C.6 (compliance with EN 15684 [7]). The mechanical lock then has to fulfil the requirements of level 3 in Table C.2 (compliance with EN 12209 [4] digit 7 grade 3) and the door furniture has to fulfil the requirements of level 3 in Table C.4 (compliance with EN 1906 digit 7 class 3).

**Table C.1: Requirements mechanical security for cylinders for locks**

| Standard | Digit | Clause | Level 1 | Level 2 | Level 3 |
|---|---|---|---|---|---|
| EN 1303:2015 [2] | Digit 7 - Key related | 4.8 | Grade 6 | Grade 6 | Grade 6 |
| | Digit 8 - Attack resistance | 4.9 | Grade B | Grade C | Grade D |

**Table C.2: Requirements mechanical security for locks and latches**

| Standard | Digit | Clause | Level 1 | Level 2 | Level 3 |
|---|---|---|---|---|---|
| EN 12209:2016 [4] | Digit 7 - Security | 4.8 | Grade 3 | Grade 3 | Grade 5 |

NOTE 1: For EN 1627 RC 3 security grade 4 is required and för RC 4 security grade 7 or if drill-resistance is provided by the door construction security grade 6.

**Table C.3: Requirements mechanical security for multipoint locks, latches and locking plates**

| Standard | Digit | Clause | Level 1 | Level 2 | Level 3 |
|---|---|---|---|---|---|
| FprEN 15685 [8] (Draft) One locking point | Digit 7 - Security | 4.8 | Grade 3 | Grade 3 | Grade 5 |
| FprEN 15685 [8] (Draft) | Digit 9 - Security for anti-separation points | 4.10 | Grade 3 | Grade 3 | Grade 5 |

NOTE 2: For EN 1627 RC 3 security grade 4 is required and för RC 4 security grade 7 or if drill-resistance is provided by the door construction security grade 6.

**Table C.4: Requirements mechanical security for lever handles and knob furniture**

| Standard | Digit | Clause | Level 1 | Level 2 | Level 3 |
|---|---|---|---|---|---|
| EN 1906:2012 [3] | Digit 7 - Annex A | Annex A | Class 2 | Class 3 | Class 3 |

**Table C.5: Requirements mechanical security mechatronic door furniture**

| Standard | Digit | Clause | Level 1 | Level 2 | Level 3 |
|---|---|---|---|---|---|
| EN 16867 [6] | Digit 8 - Security | 4.8 | Class 1 | Class 2 | Class 2 |

# C.2 Electromechanical security

Applicable electromechanical security for SDL is given in CEN EN standards. Depending on the type of SDL different Electromechanical requirements covered in different CEN EN standards shall apply.

The electromechanical security, when applicable, for a SDL is defined in three SDL grades making reference to the relevant clauses and electromechanical security grades in the CEN EN standards according to tables C.6 to C.8.

**Table C.6: Requirements electromechanical security for mechatronic cylinders**

| Standard | Digit | Clause | Level 1 | Level 2 | Level 3 |
|---|---|---|---|---|---|
| EN 15684:2020 [7] | Digit 5- Mech. key related security | 4.6 | No requirement | No requirement | No requirement |
| | Digit 8 - Attack resistance | 4.8 | Grade C | Grade C | Grade D |
| | Digit 8 - Security - Attack Resistance | 4.8.12 to 4.8.18 | Grade 1 | Grade 2 | Grade 2 |
| | Digit 9 - Security related to EN 1906 (Annex A) | Annex A, Table A.1 | Class 2 | Class 3 | Class 3 |

**Table C.7: Requirements electromechanical security for Electromechanically operated locks and striking plates**

| Standard | Digit | Clause | Level 1 | Level 2 | Level 3 |
|---|---|---|---|---|---|
| EN 14846:2008 [5] | Digit 7 - Mechanical security | 5.8 | Grade 3 | Grade 3 | Grade 5 |
| | Digit 8 - Security electrical function | 5.9 | Grade 1 | Grade 1 | Grade 1 |
| | Digit 9 - Security electrical manipulation | 5.10.2 to 5.10.7 | Grade 2 | Grade 2 | Grade 3 |

NOTE: For EN 1627:2021 [9] RC 3 security grade 4 is required and for RC 4 security grade 7 or if drill-resistance is provided by the door construction security grade 6.

**Table C.8: Requirements electromechanical security for mechatronic door furniture**

| Standard | Digit | Clause | Level 1 | Level 2 | Level 3 |
|---|---|---|---|---|---|
| EN 16867 [6] + A1 2021 | Digit 8 - Attack resistance | 4.8 | Grade 1 | Grade 2 | Grade 3 |

# C.3 Credential security

Applicable credential security for SDL are given in CEN EN standards. Depending on the type of SDL different credential security requirements covered in CEN EN standards shall apply.

The credential security, when applicable, for a SDL is defined in two SDL levels making reference to the relevant clauses and credential security grades in the CEN EN standards according to Tables C.9 and C.10:

- Credential related security level 1 shall only be combined with mechanical/electromechanical security grades 3 and 4 in EN 15684 [7] and EN 16867 [6].
- Credential related security level 2 shall only be combined with mechanical/electromechanical security grade 5 in the relevant EN standards.

**Table C.9: Credential related security for mechatronic cylinders**

| Standard | Digit | Clause | Level 1 | Level 2 |
|---|---|---|---|---|
| prEN 15684:2020 [7] (Formal Vote version) | Digit 6 - Credential related security | 4.6.8 | ICC: Grade C | ICC: Grade D |
| | | | PIN: Grade B | PIN: Not permitted |
| | | | BIOM: Grade C | BIOM: Grade C |
| | | | ACCESS CARD: Not permitted | ACCESS CARD: Not permitted |
| | | | PIN: Grade B | PIN: Not permitted |
| | | | BIOM: Grade C | BIOM: Grade C |
| | | | ACCESS CARD: Not permitted | ACCESS CARD: Not permitted |

**Table C.10: Credential related security for mechatronic door furniture**

| Standard | Digit | Clause | Level 1 | Level 2 |
|---|---|---|---|---|
| EN 16867:2020 [6] +A1 2021 | Digit 7 - Credential related security | 4.7 | ICC: Grade C | ICC: Grade D |

# Annex D (informative): Bibliography

- ETSI TS 103 701: "CYBER; Cyber Security for Consumer Internet of Things: Conformance Assessment of Baseline Requirements".
- IETF RFC 4493: "The AES-CMAC Algorithm".
- ETSI TR 103 621: "Guide to Cyber Security for Consumer Internet of Things".

# History

| Document history | | |
|---|---|---|
| V1.1.1 | January 2024 | Publication |
| | | |
| | | |
| | | |
| | | |