SC 21018

SSF 1120-1

IOT CONNECTED DEVICES

REQUIREMENTS AND TESTING

MAY 2021

SSF 1120-1 Edition 1

SSF
Stöldskyddsföreningen

SSF (the Swedish Theft Prevention Association) is a non-profit association. The aim of the association is to promote safety and security for individuals and property through crime prevention measures, and to help shape opinions and disseminate information with regard to crime prevention. (Excerpt from SSF's by-laws § 1 and § 2. Laid down on May 13, 2011)

SSF, the Swedish Theft Prevention Association, develops and specifies standards for testing and classification within areas considered relevant to the aims of the association. A list of current SSF standards can be found on the SSF website at www.stoldskyddsforeningen.se

CONTENTS

FOREWORD ... **3**

ORIENTATION ... **3**

1 SCOPE ... **4**

2 REFERENCES ... **5**

3 DEFINITIONS ... **6**

4 REQUIREMENTS ... **8**

4.1 GENERAL ... 8
4.2 DEVELOPMENT ... 8
4.3 INSTALLATION ... 10
4.4 ACCOUNT MANAGEMENT ... 11
4.5 OPERATION ... 13
4.6 DATA PROTECTION ... 15

5 TESTING ... **16**

5.1 GENERAL ... 16
5.2 TEST IMPLEMENTATION ... 16
5.3 VULNERABILITY DISCLOSURE POLICY ... 16
5.7 TEST REPORT ... 18

6 CERTIFICATION ... **18**

7 COMPLIANCE WITH REQUIREMENTS ... **18**

APPENDIX A PENETRATION TEST (NORMATIVE) ... **19**

APPENDIX B LINK BETWEEN SSF 1120 AND ETSI EN 303 645 2.1 (INFORMATIVE) ... **23**

APPENDIX C BIBLIOGRAPHY (INFORMATIVE) ... **24**

Foreword

SSF's regulations state characteristics that are considered to be of importance for burglar resistance, performance and reliability. The regulations seek to specify quality and security ratings that can be applied in general, both in terms of specifying requirements and in conjunction with procurement.

The regulations refer to, or wherever possible are based on, national and international standards and other applicable technical specifications or international quality standards.

Satisfying statutory requirements can be demonstrated by testing and certification by recognized testing and certification organizations. Products, services, companies and persons that comply with applicable standards are listed by SSF on its website.

Orientation

SSF 1120 has been produced as a joint project involving SSF Swedish Theft Prevention Association and F-Secure AB. Several stakeholders have contributed to the guidelines for this standard, including ETSI NCSC. The working group for this standard contains representatives from Axis, AssaAbloy, IKEA, dormakaba, Dina Försäkringar, Parakey, Sensative, Svensk Brand- och Säkerhetscertifiering SBSC, Verisure, F-Secure and SSF.

SSF 1120 is for consumer products for personal home use, but can also form the basis for use within companies. This document has been adapted from the provisions set out in ETSI EN 303 645. The requirements in this document can form the basis for insurance.

A product that complies with SSF 1120 also complies with the 'shall' requirements in ETSI EN 303 645. The objective is for this to harmonize the security requirements from various European bodies. SSF 1120 also provides support for the practical application of selected sections of GDPR.

The document has been drafted to create a framework, whose target group is both producers and consumers of IoT devices. This document describes the requirements that are placed on producers. **Appendix A** describes Penetration Tests. **Appendix B** describes the link between the requirements in this standard and the provisions in ETSI EN 303 645.

This document describes several information processes in the lifecycle of an IoT device. The information processes are divided as follows in the chapters: Development, Installation, Account Management, Maintenance, Operation and Data Protection.

Testing for SSF 1120 shall be performed by a competent and recognized third party.

Certification for SSF 1120 shall be performed by a recognized body.

1 Scope

A standard for the classification, requirements and testing of IoT devices and data collection sensors.

Examples of IoT devices include:

— home automation

— personal assistance and connected health

— building control (Internet-enabled control engineering)

— connected toys

— IP cameras

— connected alarms

— digital locks

— access points, routers and hubs for network traffic and wireless transfer

— connected weather sensors for personal use

— white goods, kitchen equipment and washing systems with network connections

— entertainment systems, such as smart TVs

— home assistants based on acoustic sensor technology

— connected light sources

This standard covers security in the digital data processing of IoT devices. This standard covers software security, communications protocols, the storage and processing of data in the IoT device, and methods for administration and troubleshooting.

The baseline requirements described in this document should be supplemented with product-specific protection mechanisms for the intended use of the product.

1.1 Scope

This cybersecurity standard for the Internet of Things sets requirements for the security of IoT devices for data in storage, use and transport.

This means that the document sets requirements for communication in and out of the IoT device and between IoT devices in the home.

The areas that this document does not cover are:

- General and/or third-party applications or services, not released by the product's producer or specifically intended for the product.
- Communication processes and information flows that do not originate from or are not received by the IoT device.

- Mobile applications and storage in mobile devices.
- Applications in personal computers or storage in personal computers.
- Connected application for steering vehicles.
- Devices that are used as personal computers or cell phones.
- For connected locking devices with burglar-resistant characteristics; SSF 3523 'Digital locking devices' shall be used.
- For intruder alarm products and fire alarm products that have specific product standards; these specific standards shall be used.

2 References

These regulations contain dated or undated references to regulations in other publications. These normative references can be found in the body copy.
The publications are listed below. With regard to dated references to publications that have subsequently been amended or supplemented, such amendments and supplements are only valid if they have been inserted into these regulations. For undated references, the latest edition of the publication applies.

ETSI EN 303 645 2.1	*Cyber Security for Consumer Internet of Things: Baseline Requirements*
NIST SP 800-52 Rev. 2	*Guidelines for the Selection, Configuration, and Use of Transport Layer Security (TLS) Implementations*
NIST SP 800-57 Part 2	*Recommendation for Key Management: Part 2 – Best Practices for Key Management Organizations*
NIST SP 800-90A	*Recommendation for Random Number Generation Using Deterministic Random Bit Generators*
SSF 3523	*Digital locking devices – Classification, requirements and testing*
SSF 1130	*Certification bodies – Requirements*

3 Definitions

The terms and definitions specified below are applicable when using this document.

3.1
constrained devices
An IoT device that has limited calculation capacity, communication ability or power supply.
Constrained devices match at least two of the four statements below:

- A sensor or transducer but not a control unit.
- The power supply has a capacity of less than 1Ah or a non-replaceable primary battery.
- A device that can only send but not receive instructions.
- Devices that do not communicate on networks where IP (Internet Protocol) is used.

Example: A constrained device cannot perform a TLS handshake procedure as its limited microprocessor cannot complete the cryptographic calculation before the time interval for a response has expired with the peer.

3.2 entropy
cryptography that is suitable for the corresponding use case and has no indications of a feasible attack with current readily available techniques.

3.3
external networks
An external network is a network where IoT devices and infrastructures are owned by others and not the person or organization.

3.4
on-premises network
An on-premises network is a network where IoT devices and the infrastructure are owned by the person, organization or property owner.

3.5 secret data
critical security parameters and general security parameters.

3.6
the principle of least privilege
A security philosophy based on minimalism.

Note The aim is to reduce risks by reducing information flows and storage to a minimum amount or to minimize access to the task in question.

3.7
personal data
The definition of different categories of personal data is set out in European legislation and complementary national legislation. See GDPR and the Swedish Data Protection Act.

3.8
secure by design
Secure by design is a concept that describes various principles for how a product is created based on experiences from the security world.

Note 'The principle of least privilege' is an example of secure by design.

3.9
secure boot
A secure boot mechanism obtains security information from a hardware component that describes the system's original integrity before it is started.

3.10
Internet Of Things, IoT devices
The Internet of Things is equipment that uses electronic media as the carrier. IoT devices can collect data and regulate the surroundings using sensors and mechanics. IoT devices are designed with a specific purpose in mind and not as a general tool. The Internet of Things relates to devices that have sufficient capacity to perform cryptographic protection mechanisms in network traffic. Devices that are exempt from classification are devices whose characteristics or circumstances have limitations in satisfying the requirements. See definition 3.1.

4 Requirements

4.1 General

The requirements in the following document have been drafted with reference to the provisions in ETSI EN 303 645 (see references for the dated version).

4.2 Development

4.2.1 Vulnerability disclosure policy

The device manufacturer shall publish an official vulnerability disclosure policy. This vulnerability disclosure policy shall define a contact address for vulnerabilities and a timeline for responses and confirmation. This vulnerability disclosure policy shall explain that when information about new or known vulnerabilities is received, identification and actions shall be initiated without delay.

To be verified in accordance with 5.3.

Note 1 A typical action flow for software should be completed within 90 days. This flow includes the identification of a vulnerability, the modification of software, and communication with the person who reported the vulnerability, customers and the public.

Note 2 In an action flow for vulnerabilities involving hardware, the actions and change work can take longer than for a software vulnerability.

4.2.1.1 Device manufacturers shall monitor and identify vulnerabilities for all of the products and services they sell and have sold during the defined support period. The policy shall stipulate how this shall be done.

To be verified in accordance with 5.3.1.

Note Software solutions are often based on third-party software. The device manufacturer can, for example, keep a list of the third-party software and versions used in the device. The third-party list is the source of a list of software that should be continually monitored for vulnerabilities. This continual monitoring for vulnerabilities will then form the decision-making data when performing a risk analysis for introducing new third-party software and associated software licenses.

4.2.2 Maintenance/Handling

A device that is not a ‘constrained device’ shall have support for the ‘secure installation of updates’.

To be verified in accordance with 5.3.2.

4.2.2.1 A software update shall be simple for the user to apply. Exceptions are made for constrained devices.

To be tested and verified in accordance with 5.3.3.

Note Software updates should preferably be applied automatically without the user's involvement.

A check for new versions and security updates should be performed each time a device is initialized and then on a regular basis.

4.2.2.2 The cryptological applications used for security updates shall be applied in accordance with the relevant security practice.

To be tested in accordance with Appendix A, Section A.2.1.

Note The security practice for cryptology is for the theoretical model and the application of the cryptographic algorithm to not display any indications of a feasible attack using currently-known techniques. When a security practice is followed, a cryptographically secure pseudo-random number generator (CSPRNG) shall be used; see NIST SP 800-90A

4.2.2.3 Security updates shall be made available in accordance with the policy.

To be verified in accordance with 5.3.4.

Note The period of time defined in the policy should depend on the severity of the vulnerability. Vulnerabilities that do not require interaction with users or require previous authentication should be given top priority. For a general description of a vulnerability management cycle, see 4.2.1 Note 2. 2.

4.2.2.4 The authenticity and sender of updates shall be verified using a trust relationship that is established in advance between the device and the distributor of updates.

To be verified in accordance with 5.3.5.

4.2.2.5 The device manufacturer shall clearly report to its customers the period of time when the device will receive security updates.

To be verified in accordance with 5.3.6.

Note The device manufacturer can, for example, report information on security updates on the product's website.

4.2.2.6 The device manufacturer's name, the model name and the hardware revision shall be clearly visible on the device's label or surface.

To be verified in accordance with 5.3.7.

4.2.2.7 The device manufacturer shall follow a secure management process for critical security parameters that is used by the device.

To be verified in accordance with 5.3.8.

Note The management process relates to open standards for secure key exchange and key management. An example of such a standard is NIST SP 800-57 Part 2.

4.3 Installation

The following section describes requirements for security during the device's installation flow.

4.3.1 Secret data

When storing secrets, such as security parameters, integrity verification or authenticity control of software updates, requirements in accordance with 4.3.1.1 up to 4.3.1.4 shall be met.

4.3.1.1 Secret data shall be stored on secure storage media. Secure storage media is a storage location with integrity and confidentiality provided by the hardware.

To be tested in accordance with Appendix A, Sections A.4.1, A.5.2.

Examples of this kind of hardware are Trusted Execution Environment (TEE), encrypted storage media, Secure Elements (SE), Dedicated Security Components (DSC) or process capacity from a U-SIM/UICC.

4.3.1.2 When a hard-coded identity is used for security purposes, it shall be implemented using a method that protects it against physical, electronic and software manipulation.

To be tested in accordance with Appendix A, Section A.5.3.

Example: A master key that is used for network access and the identification of devices is stored in a SIM card/UICC, which is compliant to ETSI's guidelines for SIM cards and protection against manipulation.

4.3.1.3 Secret data shall not be 'hard coded' in the software's source code.

To be tested in accordance with Appendix A, Section A.5.4.

4.3.1.4 Secret data shall be unique for each device's identity and shall be produced using a mechanism that hinders guess attacks.

To be tested in accordance with Appendix A, Sections A.5.4 and A.5.5.

4.3.2 Exceptions

4.3.2.1 Shared secrets are allowed for access to shared networks, such as WiFi passwords or APN settings in 3GPP, but not for application security.

4.3.2.2 Constrained devices that act as sensors do not need to verify incoming data from a control device with hardware-protected security.

4.3.3 Installation and settings

Requirements in accordance with 4.3.3.1–4.3.3.3 apply for the installation flow of devices:

4.3.3.1 The device manufacturer shall minimize the number of security-related decisions that require domain-specific knowledge of the user during the installation process.

To be tested in accordance with 5.4.

4.3.3.2 The device manufacturer shall guide the users to configure the device securely.

To be tested in accordance with Appendix A, Sections A.6.1 and A.6.2.

4.3.3.3 The device manufacturer shall guide the users to understand whether the device's configuration has created security breaches.

To be tested in accordance with 5.4.1 and Appendix A, Section A.6.1.

4.4 Account management

4.4.1 Authentication

Requirements in accordance with 4.4.1.1 and 4.4.1.2 shall be included in devices where passwords are applied.

4.4.1.1 Where passwords are used and in any state other than the factory default, all IoT device passwords shall be unique per device or defined by the user.

To be tested in accordance with Appendix A, Section A.5.1.

4.4.1.2 When generated passwords are used, the algorithm for random numbers shall not be linked to identified information or device class.

To be verified in accordance with 5.5.

4.4.2. Requirements in accordance with 4.4.2.1–4.4.2.3 apply for the authentication flow.

4.4.2.1 The authentication mechanisms used in the device shall apply cryptological recommendations in accordance with known recommendations for the application.

To be tested in accordance with Appendix A, Sections A.2.3 and A.2.4.

4.4.2.2 The authentication value in a device shall be interchangeable. The Administrator/User must be able to change passwords, PIN codes or add a biometric attribute.

To be verified in accordance with 5.5.1.

4.4.2.3 Protection from repeated guess attempts for the authentication mechanism shall be applied, unless the device is considered to be a 'constrained device'.

To be tested in accordance with Appendix A, Section A.3.1.

4.4.3 Personal data

4.4.3.1 General

Personal data is information that is processed, stored or transported by the IoT device that describes a person.

4.4.3.2 The confidentiality of sensitive personal data between devices and associated services shall be protected by cryptographic applications that have been adapted for the technology and its use.

To be tested in accordance with Appendix A, Sections A.2.1 and A.6.2.

4.4.3.3 The device's external sensors shall be clearly documented and the information shall be made available to the device's user.

To be verified in accordance with 5.5.2.

4.4.3.4 The user shall be allowed to delete personal data in a simple manner.

To be verified in accordance with 5.5.3.

Example: A user that intends to close their account for the IoT device so that they can sell it on the second-hand market can choose to log in on the device's control panel and choose to close their user account. The device then deletes the account's personal data and all personal settings, along with telemetry from the device's storage media. This can be achieved by performing a factory reset of the system or by removing individual accounts.

4.4.3.5 The device manufacturer shall give the user the ability to obtain clear information about the kinds of data collected by the device, how it is used and for which purposes. This requirement applies for each device and service that the device communicates with, as well as third parties and advertisers.

To be verified in accordance with 5.5.4.

4.4.3.6 When collecting personal data, the device manufacturer shall first obtain the user's consent in a valid way.

To be verified in accordance with 5.5.5.

4.4.3.7 Users who have given their consent for the processing of personal data shall be given the ability to withdraw it at any time.

To be verified in accordance with 5.5.6.

Note The user's consent is a free and clear selectable option to start data collection for a stated purpose.

4.5 Operation

Security requirements for operational functions in the IoT device.

4.5.1 Secure communication

The device shall apply established cryptographic practice to communicate securely across networks.
To be tested in accordance with Appendix A, Sections A.2.1, A.2.2, A.2.3 and A.2.4.

4.5.1.1 Functionality that allows changes to be made to security parameters across network interfaces, such as password changes, the installation of keys and changes of authority levels, shall only be accessible following authentication.

This requirement does not apply to network protocols that do not have authentication, but are required for operation.

To be tested in accordance with Appendix A, Sections A.1.2 and A.6.3.

Note Protocols that are exempt are ARP, DHCP, DNS, ICMP, and NTP.

4.5.1.2 Devices shall protect the confidentiality of critical security parameters through encryption when they communicate across external networks.

To be tested in accordance with Appendix A, Section A.6.2.

Note An authentication application that preserves confidentiality is, for example, a challenge response idiom with a non-predictable nonsense value.

This requirement relates to methodology where information elements in the security exchange are protected by cryptographic signatures.

Other methods include several authentication factors that ensure that the interception of the communication on a channel does not lead to the full exposure of the authentication flow.

4.5.1.3 When generating cryptographic keys, sufficient entropy shall be used for seed materials.

To be tested in accordance with Appendix A, Sections A.2.3, A.2.4 and A.2.5.

4.5.2 The device's attack surfaces

4.5.2.1 Devices that have a physical debug interface shall remain disabled in the software.

To be tested in accordance with Appendix A, Sections A.1.1, A.1.3, A.6.1 and A.6.2.

Example 1: An admin interface that is exposed to local networks (LAN), but disabled for global networks (WAN).

Example 2: A service for the direct update of firmware via Bluetooth that is used for development, but is disabled in the final product.

4.5.2.2 In its default state, the device's network interface shall minimize the exposure of security-related information without authentication.

To be tested in accordance with Appendix A, Section A.1.4.

Note The default state is the state that the device is in before it is deployed or a device that does not have authentication information.

4.5.2.3 Devices with a physical debug interface shall remain disabled through settings in the software.

To be tested in accordance with Appendix A, Section A.6.4.

Example: A serial port's interface is disabled in the device's bootloader software. No login or interaction is possible over the serial port when the device is in its production state. Note that a secure update function is not considered to be a debug interface.

4.6 Data protection

4.6.1 General

Several IoT devices process personal data. Device manufacturers are expected to provide functionality for the protection of personal data. They must also comply with GDPR.

This section aims to clarify the kind of functionality that can facilitate the protection of personal data.

4.6.1.1 The user shall be given information in their documentation about the kinds of telemetric data that is collected by the IoT device, how data is used, who the data is shared with and for which purposes.

To be verified in accordance with 5.6.

5 Testing

5.1 General

The tests described in the following chapter have a clearly defined scope. This scope describes the attack surfaces to be tested, the test methodology and the information available (white/gray/black box etc.).
The exact approach that is applied to perform the test can vary, but it shall be described in a test report.

5.2 Test implementation

The tester shall be provided with: user details, documentation and the device.

The penetration tester shall be provided with: user details, the device, debug ports and the relevant source code.

An up-to-date list of third-party software and their version numbers or patch levels shall be provided. The penetration test report covers the software that is set out in this list.

5.3 Vulnerability disclosure policy

The requirement as stated in 4.2.1 is verified by means of the manufacturer's documentation.

5.3.1 The requirement as stated in 4.2.1 is verified by means of the manufacturer's documentation.

5.3.2 Maintenance/Handling

The requirement as stated in 4.2.2 is verified by means of the manufacturer's documentation.

5.3.3 To be tested by performing an update. Verify that the process for updates is simple and instructive so that a user can perform an update themselves.

5.3.4 Verify using documentation or a declaration from the device manufacturer that clarifies the amount of time a security update shall take in accordance with the relevant policy.

5.3.5 To be tested in the following way:

1. The tester sends an update with an invalid sender.
2. The tester sends an update with a valid sender and modified content.
3. The tester sends an update with a valid sender and non-modified content.

4. The tester verifies that 1 and 2 lead to an update being rejected and that 3 leads to a successful update.

5.3.6 Verify that the product's documentation clearly describes the relevant service agreement, warranty agreement, support time for software and firmware updates.

5.3.7 Verify that the necessary information is accessible on the product.

5.3.8 Verify that there is a document that describes the relevant policy.

5.4 To be tested in the following way:

1. The tester performs an installation of the device.
2. The tester documents all security issues.
3. Verify whether suggestions for answers to questions are available in the product's documentation or headings in the software.

5.4.1 Deliberately configure the device insecurely and verify information about insecurity.

Example: Set an insecure password, such as 'password' or '1234' and then verify whether the user interface warns the user.

5.5 To be verified through documentation.

5.5.1 Verify that interchangeability is possible.

5.5.2 Verify that the product's sensor description is accessible and correct. This is performed by opening the device's shell.

5.5.3 To be verified by deleting the user information and then checking that the data has not been stored in a way that is accessible to later users or other users.
Tests shall also be performed to recreate a user with the same username as a name that has previously been deleted.

5.5.4 Verify that the requirements text is followed.

5.5.5 Verify that the OPT-IN principle is applied for the approval of data collection.

5.5.6 Verify that the agreement for the device manufacturer's processing of personal data is revocable.

5.6. To be verified through documentation from the device manufacturer. Verify that information about telemetric data is provided, its purpose and the data that is used.

5.7 Test report

Information points that shall be available after testing are:

- date of testing
- testing institute and test participants
- test protocol
- information on execution of testing
- information on the assessment
- manufacturer
- type designation
- device covered by the test
- technical documentation (drawings, specifications, user agreement, etc.)

6 Certification

Certification for this standard shall be issued by a certification body that complies with the requirements pursuant to SSF 1130.

7 Compliance with requirements

Products that have been certified by a third party in accordance with the requirements in this standard can apply to use the SSF IoT mark.

Send applications to info@stoldskyddsforeningen.se

Appendix A
Penetration test
(normative)

Penetration tests shall be performed by an independent third party with documented experience in security in both hardware and software.

Security analyses and penetration tests shall be performed using the White Box principle with the technical documentation available.

The following questions shall be answered with the words **Passed**, **Not Passed** or **Not applicable** in a penetration test report. The method used to test a question shall be recorded in the penetration test report.

Scope of the security review:

A.1 Network
'Port-scan' the network interface for wireless, local and external networks.

A.1.1 Devices with a physical debug interface shall remain disabled in the software.

A.1.2 Authentication shall be required for all network services with functionality that allows security parameters to be changed across network interfaces.

A.1.3 There may be no undocumented exposed services.

Penetration tests shall verify a device in its default state and search for exposed network interfaces by service. Connect to all services with the protocol's associated client and collect the information available.

A.1.4 Penetration tests shall verify a device in its default state (before deployment or without authentication information) and search for exposed network interfaces by service. Connect to all services with the protocol's associated client and collect the information available. This information may not be security information.

Security information relates to customer-specific information about infrastructure or resources that could be used during an attack.

A.2 Network cryptography

Perform a key exchange from a client to exposed services that have support for cryptography.

A.2.1 Verify that applicable TLS certificates are up-to-date (valid dates, a relevant issuer of CA signatures) and follow NIST recommendations, and that other cryptographic applications of signatures are based on known practice.

Verify that cryptographic protection for exposed services is applied through TLS or other cryptography approved by NIST.

A.2.2 NIST SP 800-52 recommendations in the TLS communication shall be followed.

A.2.3 General recommendations from NIST SP 800-175B for key exchanges in other cryptological exchanges shall be followed.

A.2.4 NIST SP 800-57 recommendations for key length in other cryptographic exchanges shall be followed.

A.2.5 The security practice for cryptology is for the theoretical model and the application of the cryptographic algorithm to not display any indications of a feasible attack using currently-known techniques. When a security practice is followed, a cryptographically secure pseudo-random number generator (CSPRNG) shall be used; see NIST SP 800-90A.

A.3 Authentication

Perform multiple invalid authentication procedures for each applicable service and at least one valid procedure.

A.3.1 It shall not be possible to guess a valid authentication with multiple authentication attempts.

Protection from repeated guess attempts for the authentication mechanism shall be applied, unless the device is considered to be a ‘constrained device’.

A.4 Storage and boot

A.4.1 It shall not be possible to use physical means to extract secret data in clear text from the device’s storage media.

Examples of extraction technologies for physical access can be reading a SATA interface, PCI, the extraction of Flash or reading SD cards.

A.5 Code review

Review the library with functionality for generating passwords.

A.5.1 Verify that known identifiers are used as input data for generating passwords.

Review functionality to verify the integrity of the operating system/core.

If passwords are used and in any state other than the factory default, all IoT device passwords shall be unique per device or defined by the user.

A.5.2 Verify that hardware support is used to verify the integrity of the operating system.

Examples of hardware-supported libraries are ‘Trousers’ for TPM or u-Boot with TPM 2.0 support.

Review functionality for identity management for security purposes.

A.5.3 Verify that the identity data is stored in a variable or in a medium whose integrity is verified using hardware.

Review libraries with functionality for processing ‘secret data’.

A.5.4 Verify that there are no hard-coded secret values that are used by security functionality and that are also the same in other devices.

A.5.5 Verify that there are no secret values that are used by security functionality whose differences are generated in a series or in any other predictable way.

A.6 Administration and authorization

Configure the device in accordance with the recommended configuration (default). Perform a vulnerability scan of the network interface and intercept network traffic to and from the device in operation.

A.6.1 Verify whether any attack routes are exposed during a vulnerability scan of exposed interfaces.

Perform an inspection of intercepted communication between the device in its recommended operation (default) and its periphery services.

A.6.2 Verify that there is no communication in clear text or protocols whose vulnerabilities can be exploited by an attacker that has control of the network.

A.6.3 Verify that the device administration cannot be carried out without valid authority.

Open the device's shell and examine the device's circuit card. Identify and test connection to a JTAG/USB/UART/SWD interface or a corresponding hardware interface for debugs.

A.6.4 Verify that it is not possible to extract debug information from the device over the exposed interface.

The penetration test shall verify that an interface of the type USB/JTAG/UART, etc. is disabled by software irrespective of whether they have exposed contact interfaces or not.

Appendix B

Link between the requirements in this standard and ETSI EN 303 645 2.1
(informative)

Requirements Section in SSF 1120	Provision in ETSI EN 303 645 2.1	Test procedure in SSF 1120	
		Verification/Test	PEN test (Appendix A)
4.2.1	5.2-1	5.3	
4.2.1 Note 1	5.2-2	5.3	
4.2.1.1	5.2-3	5.3.1	
4.2.2	5.3-2	5.3.2	
4.2.2.1	5.3-3	5.3.3	
4.2.2.1 Note	5.3-4 and 5.3-5	5.3.3	
4.2.2.2	5.3-7	-	A.2.1
4.2.2.3	5.3-8	5.3.4	
4.2.2.4	5.3-10	5.3.5	
4.2.2.5	5.3-13	5.3.6	
4.2.2.6	5.3-16	5.3.7	
4.2.2.7	5.5-8	5.3.8	
4.3.1.1	5.4-1	-	A.4.1, A.5.2
4.3.1.2	5.4-2	-	A.5.3
4.3.1.3	5.4-3	-	A.5.4
4.3.1.4	5.4-4	-	A.5.4, A.5.5
4.3.3.1	5.12-1	5.4	
4.3.3.2	5.12-2	-	A.6.1, A.6.2
4.3.3.3	5.12-3	5.4.1	A.6.1
4.4.1.1	5.1-1	-	A.5.1
4.4.1.2	5.1-2	5.5	
4.4.2.1	5.1-3	-	A.2.3, A.2.4
4.4.2.2	5.1-4	5.5.1	
4.4.2.3	5.1-5	-	A.3.1
4.4.3.2	5.8-2	-	A.2.1, A.6.2
4.4.3.3	5.8-3	5.5.2	
4.4.3.4	5.11-1	5.5.3	
4.4.3.5	6-1	5.5.4	
4.4.3.6	6-2	5.5.5	
4.4.3.7	6-3	5.5.6	
4.5.1	5.5-1	-	A.2.1, A.2.3, A.2.4
4.5.1.1	5.5-5	-	A.1.2, A.6.3
4.5.1.2	5.5-7	-	A.6.2
4.5.1.3	5.1-3	-	A.2.3, A.2.4, A.2.5
4.5.2.1	5.6-1	-	A.1.1, A.1.3, A.6.1, A.6.2
4.5.2.2	5.6-2	-	A.1.4
4.5.2.3	5.6-4	-	A.6.4
4.6.1.1	6-5	5.6	

Appendix C Bibliography
(informative)

SSF 1075	*Distribution, storage and use of digital keys – Classification, demands and evaluation*
SSF 1101	*Cybersecurity – Basic Level*
NIST 800-160 Volume 1	*Standard for development processes and security*
NIST SP 800-63B	*Digital Identity Guidelines – Authentication and Lifecycle Management*

The following documents are also available that describe the practice for managing security updates:

IoT Security Foundation in the document ‘Vulnerability Disclosure – Best Practice Guidelines’.

Stakeholder Cybersecurity Certification Group (SCCG).

EU Common Criteria (EUCC) candidate scheme on cybersecurity certification.

ISBN 978-91-88191-51-9

This standard can be ordered from:
stöldskyddsföreningen.se
Tel +46 (0)771 773 773

SSF
Stöldskyddsföreningen