

**SSF 1120-1**

# **IOT CONNECTED DEVICES**

**REQUIREMENTS AND TESTING**

**MAY 2021**

**SSF 1120-1 Edition 1**

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](http://www.stoldskyddsforeningen.se)

Copyright © 2021 SSF Swedish Theft Prevention Association

## **CONTENTS**

<b>FOREWORD</b> .....	<b>3</b>
<b>ORIENTATION</b> .....	<b>3</b>
<b>1 SCOPE</b> .....	<b>4</b>
<b>2 REFERENCES</b> .....	<b>5</b>
<b>3 DEFINITIONS</b> .....	<b>6</b>
<b>4 REQUIREMENTS</b> .....	<b>8</b>
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
<b>5 TESTING</b> .....	<b>16</b>
5.1 GENERAL.....	16
5.2 TEST IMPLEMENTATION.....	16
5.3 VULNERABILITY DISCLOSURE POLICY .....	16
5.7 TEST REPORT .....	18
<b>6 CERTIFICATION</b> .....	<b>18</b>
<b>7 COMPLIANCE WITH REQUIREMENTS</b> .....	<b>18</b>
<b>APPENDIX A PENETRATION TEST (NORMATIVE)</b> .....	<b>19</b>
<b>APPENDIX B LINK BETWEEN SSF 1120 AND ETSI EN 303 645 2.1 (INFORMATIVE)</b> ....	<b>23</b>
<b>APPENDIX C BIBLIOGRAPHY (INFORMATIVE)</b> .....	<b>24</b>

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