ILNAS

Institut luxembourgeois de la normalisation
de l'accréditation, de la sécurité et qualité
des produits et services

ILNAS-EN 17927:2023

Security Evaluation Standard for IoT Platforms (SESIP). An effective methodology for applying cybersecurity assessment and re-use

Sicherheitsbewertungsstandard für IoT Plattformen (SESIP) - Ein effektives Verfahren zur Anwendung der Cybersicherheitsbewertung und

Norme d'évaluation de la sécurité pour les plates-formes IoT (SESIP) - Une méthodologie efficace pour appliquer et réutiliser des évaluations de la

11/2023

ILNAS-EN 17927:2023 - Preview only Copy via ILNAS e-Shop

National Foreword

This European Standard EN 17927:2023 was adopted as Luxembourgish Standard ILNAS-EN 17927:2023.

Every interested party, which is member of an organization based in Luxembourg, can participate for FREE in the development of Luxembourgish (ILNAS), European (CEN, CENELEC) and International (ISO, IEC) standards:

- Participate in the design of standards
- Foresee future developments
- Participate in technical committee meetings

https://portail-qualite.public.lu/fr/normes-normalisation/participer-normalisation.html

ILNAS-EN 17927:2023 - Preview only Copy via ILNAS e-Shop

THIS PUBLICATION IS COPYRIGHT PROTECTED
Nothing from this publication may be reproduced or utilized in any form or by any mean - electronic, mechanical, photocopying or any other data carries without prior permission!

EUROPEAN STANDARD **EN 17927**

NORME EUROPÉENNE

EUROPÄISCHE NORM

November 2023

ICS 35.030; 35.240.95

English version

Security Evaluation Standard for IoT Platforms (SESIP). An effective methodology for applying cybersecurity assessment and re-use for connected products.

Norme d'évaluation de la sécurité pour les plates-formes IoT (SESIP) - Une méthodologie efficace pour appliquer et réutiliser des évaluations de la cybersécurité de produits connectés

Sicherheitsbewertungsstandard für IoT-Plattformen - Eine effektive Methode zur Anwendung der Cybersicherheitsbewertung und Wiederverwendung für vernetzte Produkte

This European Standard was approved by CEN on 13 April 2023.

CEN and CENELEC members are bound to comply with the CEN/CENELEC Internal Regulations which stipulate the conditions for giving this European Standard the status of a national standard without any alteration. Up-to-date lists and bibliographical references concerning such national standards may be obtained on application to the CEN-CENELEC Management Centre or to any CEN and CENELEC member.

This European Standard exists in three official versions (English, French, German). A version in any other language made by translation under the responsibility of a CEN and CENELEC member into its own language and notified to the CEN-CENELEC Management Centre has the same status as the official versions.

CEN and CENELEC members are the national standards bodies and national electrotechnical committees of Austria, Belgium, Bulgaria, Croatia, Cyprus, Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Iceland, Ireland, Italy, Latvia, Lithuania, Luxembourg, Malta, Netherlands, Norway, Poland, Portugal, Republic of North Macedonia, Romania, Serbia, Slovakia, Slovenia, Spain, Sweden, Switzerland, Türkiye and United Kingdom.

ILNAS-EN 17927:2023 - Preview only Copy via ILNAS e-Shop

CEN-CENELEC Management Centre:
Rue de la Science 23, B-1040 Brussels

© 2023 CEN/CENELEC All rights of exploitation in any form and by any means reserved worldwide for CEN national Members and for CENELEC Members.

Contents

Page

ILNAS-EN 17927:2023 - Preview only Copy via ILNAS e-Shop

European foreword

This document (EN 17927:2023) has been prepared by Technical Committee CEN/JTC 13 “Cybersecurity and Data Protection”, the secretariat of which is held by DIN.

This European Standard shall be given the status of a national standard, either by publication of an identical text or by endorsement, at the latest by May 2024, and conflicting national standards shall be withdrawn at the latest by May 2024.

Attention is drawn to the possibility that some of the elements of this document may be the subject of patent rights. CEN shall not be held responsible for identifying any or all such patent rights.

Any feedback and questions on this document should be directed to the users’ national standards body. A complete listing of these bodies can be found on the CEN website.

According to the CEN-CENELEC Internal Regulations, the national standards organisations of the following countries are bound to implement this European Standard: Austria, Belgium, Bulgaria, Croatia, Cyprus, Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Iceland, Ireland, Italy, Latvia, Lithuania, Luxembourg, Malta, Netherlands, Norway, Poland, Portugal, Republic of North Macedonia, Romania, Serbia, Slovakia, Slovenia, Spain, Sweden, Switzerland, Türkiye and the United Kingdom.

ILNAS-EN 17927:2023 - Preview only Copy via ILNAS e-Shop

ILNAS-EN 17927:2023 - Preview only Copy via ILNAS e-Shop

Introduction

This document specifies the Security Evaluation for Secure IoT Platforms (SESIP). It includes general requirements for Security Functional Requirements (SFRs), Security Process Packages (SPPs) and Security Assurance Requirements (SARs) designed to be used in the evaluation and certification of IoT platforms.

SESIP is a methodology for the security evaluation of platforms on which connected products are based. The term “platform” in SESIP is defined as the implementation of underlying features for an application layer; a platform can be subdivided in “platform parts”.

SESIP does not address the final connected product itself, but the results of the SESIP evaluation of connected platforms are meant to be able to be used as evidence for compliance demonstration to standards addressing Connected Products.

This makes SESIP not redundant with current IoT standards but a tool on which those standards can base on by reusing outputs. It is indeed impossible for a product vendor to provide, with reasonable effort, assessment evidences for all platform parts integrated from different developers/manufacturers.

This SESIP methodology specific goals are summarized below:

- To be accessible to applicable IoT products stakeholders;
- To provide clear but harmonized security claims;
- To consider time-to-market needs by providing an optimized and efficient methodology;
- To enable the reuse of evaluation results in different products and/or between different standards and avoid redundant evaluations of same platform (parts)without added value;
- To support Connected Products compliance demonstration to Connected Product standards.

Fulfilling of these goals allows SESIP raising the overall security in IoT ecosystems by increasing the number of security evaluations through clarity in security claims and optimized efforts.

ILNAS-EN 17927:2023 - Preview only Copy via ILNAS e-Shop

1 Scope

This document specifies a cybersecurity evaluation methodology, named SESIP, for platforms and platform parts of connected IoT products. Security claims in SESIP are made based on the security services offered by those platforms. Platform parts can be in hardware and software. SESIP aims to support comparability between and reuse of independent security evaluations. SESIP provides a common set of requirements for the security functionality of platform parts which apply to the foundational platforms of devices that are not application specific. The methodology specifies the re-use of evaluation results.

2 Normative references

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

ISO/IEC 17000:2020, *Conformity assessment — Vocabulary and general principles*

ISO/IEC 17065:2012, *Conformity assessment — Requirements for bodies certifying products, processes and services*

3 Terms, definitions, symbols and abbreviated terms

For the purposes of this document, the terms and definitions given in ISO/IEC 17000:2020, ISO/IEC 17065:2012 and the following apply.

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

- IEC Electropedia: available at https://www.electropedia.org/
- ISO Online browsing platform: available at https://www.iso.org/obp

3.1
composite platform
platform integrating a certified platform (part)

3.2
connected application
application
overall software layer implementing an IoT end-user use case based on the underlying connected platform

3.3
connected application part
application part
subset of the connected application defined by a specific context (e.g. data, resources, etc.) and to be isolated from the rest of the application

3.4
connected platform
platform
hardware and/or software that provides secure services to a connected application

3.5
connected platform developer
platform developer
developers who build platform (parts) and supply them to product vendors or to other platform developers, and who need to certify the security of the platform (parts) that they build.

3.6
connected platform part
platform part
part
hardware and/or software that implements a subset of the features of a connected platform, and that can be evaluated separately e.g. the hardware, a cryptographic library, an OS.

3.7
connected product
product
combination of a connected platform and a connected application that a product vendor puts on the market.

3.8
keystore
repository in which certificates, private keys, or secrets can be stored.

3.9
SESIP profile
security profile generic to a type of platform (part), template for a SESIP Security Target of a platform of type targeted by the profile

3.10
SESIP Security Target
SESIP ST
ST
statement of SESIP security requirements in terms of security features (SFRs and SPPs) and evaluation activities (SARs) to be addressed during the evaluation of a platform (part)

4 Overview

4.1 General

This clause provides an overview of the essential principles underlying SESIP:

- The base concepts of the methodology
- A threat model adapted to the IoT ecosystem
- A life cycle adapted to connected products in the IoT ecosystem
- Reusability, an essential objective of SESIP, in order to handle at an acceptable cost the increasing complexity of the connected platforms that need to be evaluated in the IoT ecosystem
- Accessibility, which is required to encourage product vendors to leverage security features included in evaluated connected platforms; the results of an evaluation is expected to be accessible and exploitable by security-proficient developers without the need to be evaluation specialists.
- Security self-assessment in SESIP

ILNAS-EN 17927:2023 - Preview only Copy via ILNAS e-Shop

ILNAS-EN 17927:2023 - Preview only Copy via ILNAS e-Shop

4.2 SESIP concepts

SESIP is originated from the ISO 15408 series ([4], [5], [6]), specialized for the evaluation of connected platforms in the context of IoT; it provides the base concepts as follows:

- SESIP keeps the main definitions and high-level concepts introduced in ISO 15408-1 [4].

- SESIP Security Functional Requirements (SFRs) for the security features to be implemented by platforms (parts) and to be evaluated; SESIP does not use the SFR catalogue specified in ISO 15408-2 [5] but keeps the concept of a catalogue of SFRs, specialized for the IoT ecosystem, but each SFR being at a level of final service to the user.

- SESIP Secure Process Packages (SPPs) for the security processes to be implemented by the developer of the platform under evaluation.

- SESIP Security Assurance Requirements (SARs) for the evaluation activities to be performed; SESIP keeps the categorization of the Security Assurance Requirements and the associated type of developer's inputs as in ISO 15408-3 [6], however it specifies again the content as described in 7.1.

- SESIP assurance levels; SESIP does not use "EAL" packages specified in ISO 15408-3 [6], but defines its own assurance packages adapted to the IoT ecosystem: the SESIP levels (see Clause 8).

See details about SESIP implementation of those concepts in Clauses 5 to 8.

SESIP is an evaluation methodology that specifies as precisely as possible how to evaluate the security of a product, in this case a connected platform. Similarly, SESIP does not specify any particular procedure, nor does it explicitly organize the mutual recognition principles between certificates, and only provides guidance and directions. A SESIP evaluation/certification scheme based on this SESIP evaluation methodology is expected to be specified in another document by the certification scheme owner.

4.3 IoT use cases and threat model

4.3.1 General

IoT is a broad term, but always contains a product ("thing") and some form of connectivity ("internet"). SESIP focuses on the "thing" side of IoT, and on the security of connected platforms, on which connected products are based.

4.3.2 Architecture

A connected platform typically includes the following components:

- Hardware (processing unit, memory, possibly a secure element, at least one network interface, possibly some sensors) and associated features e.g. Firmware, Boot Loader and Root-of-Trust.

  o It is assumed that the connected platform includes at least one network interface that is directly or indirectly connected to a network and exposed to potential attackers.

- An operating system, providing a foundation to run Connected Applications on the hardware.

- A network connectivity layer (e.g. Comm library), allowing the connection of the product to backend or other products.

- Software application services offered to connected applications, providing an application framework to product vendors (e.g. Crypto library, Secure Storage, Identity and Attestation features).

The Figure 4-1 shows an example of a Connected platform: