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

EESTI STANDARDIMIS- JA AKREDITEERIMISKESKUS
ESTONIAN CENTRE FOR STANDARDISATION AND ACCREDITATION

EESTI STANDARDI EESSÕNA

NATIONAL FOREWORD

See Eesti standard EVS-EN 17927:2023 sisaldab Euroopa standardi EN 17927:2023 ingliskeelset teksti.	This Estonian standard EVS-EN 17927:2023 consists of the English text of the European standard EN 17927:2023.
Standard on jõustunud sellekohase teate avaldamisega EVS Teatajas	This standard has been endorsed with a notification published in the official bulletin of the Estonian Centre for Standardisation and Accreditation.
Euroopa standardimisorganisatsioonid on teinud Euroopa standardi rahvuslikele liikmetele kättesaadavaks 08.11.2023.	Date of Availability of the European standard is 08.11.2023.
Standard on kättesaadav Eesti Standardimis-ja Akrediteerimiskeskusest.	The standard is available from the Estonian Centre for Standardisation and Accreditation.

Tagasisidet standardi sisu kohta on võimalik edastada, kasutades EVS-i veebilehel asuvat tagasiside vormi või saates e-kirja meiliaadressile standardiosakond@evs.ee.

ICS 35.030, 35.240.95

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

Contents

Page

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of an identical text or by endorsement, at the latest by May 2024, and conflicting national standards shall be withdrawn at the latest by May 2024.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.

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.

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