



Methods for Testing & Specification (MTS); Device Security Passport

Sample Document

get full document from standards.iteh.ai

Reference

DTR/MTS-TST12DevSecPas

Keywords

device, IoT, security, testing

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

Important notice

The present document can be downloaded from the
[ETSI Search & Browse Standards](#) application.

The present document may be made available in electronic versions and/or in print. The content of any electronic and/or print versions of the present document shall not be modified without the prior written authorization of ETSI. In case of any existing or perceived difference in contents between such versions and/or in print, the prevailing version of an ETSI deliverable is the one made publicly available in PDF format on [ETSI deliver](#) repository.

Users should be aware that the present document may be revised or have its status changed,
this information is available in the [Milestones listing](#).

If you find errors in the present document, please send your comments to
the relevant service listed under [Committee Support Staff](#).

If you find a security vulnerability in the present document, please report it through our
[Coordinated Vulnerability Disclosure \(CVD\)](#) program.

Notice of disclaimer & limitation of liability

The information provided in the present deliverable is directed solely to professionals who have the appropriate degree of experience to understand and interpret its content in accordance with generally accepted engineering or other professional standard and applicable regulations.

No recommendation as to products and services or vendors is made or should be implied.

No representation or warranty is made that this deliverable is technically accurate or sufficient or conforms to any law and/or governmental rule and/or regulation and further, no representation or warranty is made of merchantability or fitness for any particular purpose or against infringement of intellectual property rights.

In no event shall ETSI be held liable for loss of profits or any other incidental or consequential damages.

Any software contained in this deliverable is provided "AS IS" with no warranties, express or implied, including but not limited to, the warranties of merchantability, fitness for a particular purpose and non-infringement of intellectual property rights and ETSI shall not be held liable in any event for any damages whatsoever (including, without limitation, damages for loss of profits, business interruption, loss of information, or any other pecuniary loss) arising out of or related to the use of or inability to use the software.

Copyright Notification

No part of this document may be reproduced in any form, by any means and in any media, without the prior written authorization of ETSI and except as expressly permitted below.

By way of exception and when the document is a normative deliverable (European Standard (EN), Technical Specification (TS), Group Specification (GS) or ETSI Standard (ES)), ETSI authorizes to reproduce and incorporate into products, services and technical documentation only those extracts (e.g. templates) that are strictly necessary for the technical implementation of the normative deliverable, to ensure compliance with the latter. Nothing in this notice shall be construed as limiting any mandatory exceptions to copyright provided by applicable law.

© ETSI 2026.
All rights reserved.

Contents

Intellectual Property Rights	4
Foreword.....	4
Modal verbs terminology.....	4
Executive summary	4
Introduction	5
1 Scope	6
2 References	6
2.1 Normative references	6
2.2 Informative references.....	6
3 Definition of terms, symbols and abbreviations.....	8
3.1 Terms.....	8
3.2 Symbols.....	8
3.3 Abbreviations	8
4 State of the art of device descriptors	9
4.1 Bill of Material (BOM)	9
4.1.1 Introduction.....	9
4.1.2 Software Bill of Material (SBOM)	10
4.1.3 Hardware Bill of Material (HBOM)	11
4.1.4 Cryptography Bill of Material (CBOM)	12
4.2 Manufacturer Usage Description (MUD).....	12
4.3 Vulnerability Information Exchange Formats	13
4.3.1 Vulnerability Exploitability Exchange Format (VEX)	13
4.3.2 Vulnerability Disclosure Report (VDR)	14
4.4 Security Assessment Frameworks.....	15
4.4.1 Open Security Control Assessment Language (OSCAL)	15
4.4.2 Security Content Automation Protocol (SCAP)	17
5 Rationale for a device security passport.....	18
5.1 Limitations of existing device security descriptors	18
5.2 Need for an integrated and lifecycle-aware approach	18
5.3 Design principles of a Device Security Passport	18
5.4 Considered alternatives and design choices	19
6 Device Security Passport specification	19
6.1 Concept and objectives.....	19
6.2 Device Security Passport lifecycle	20
6.3 Stakeholders and roles.....	21
7 DOSS: Using the DSP for supply chain management.....	22
7.1 DOSS overview.....	22
7.2 The role of the DSP in the DOSS project.....	23
7.3 DSP data model.....	23
8 Role of the Device Security Passport in regulatory context.....	25
8.1 Alignment with the Cyber Resilience Act (CRA)	25
8.2 Alignment with the NIS2 directive.....	26
8.3 Alignment with the CSA	27
9 Lessons learned and recommendations	27
History	29

Intellectual Property Rights

Essential patents

IPRs essential or potentially essential to normative deliverables (European Standard (EN), Technical Specification (TS), Group Specification (GS) or ETSI Standard (ES)) 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 IPR online database](#).

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™**, **LTE™** and **5G™** logo 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.

Foreword

This Technical Report (TR) has been produced by ETSI Technical Committee Methods for Testing and Specification (MTS).

Modal verbs terminology

In the present document **"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.

Executive summary

The increasing complexity of digital supply chains and the growing regulatory pressure on cybersecurity have highlighted the need for improved mechanisms to manage, share and reuse device security information throughout the lifecycle. Current practices rely on a fragmented ecosystem of security descriptors, tools and documents that are often disconnected, difficult to maintain and poorly suited for automation. The present document analyses the concept of a Device Security Passport (DSP) as a unifying, machine-readable mechanism to aggregate and reference security-related artefacts associated with connected devices. The DSP is presented as a lifecycle-aware construct capable of supporting supply-chain transparency, continuous security management and regulatory compliance, while preserving existing standards, ownership models and responsibilities. The present document reviews the state of the art of security descriptors, introduces the DSP concept and lifecycle, and describes its concrete instantiation in the DOSS project. The applicability of the DSP to regulatory frameworks such as the Cyber Resilience Act, the NIS2 Directive and the EU Cybersecurity Act is analysed, highlighting its potential to support transparency, evidence reuse and continuous compliance. Based on the experience gained, the present document identifies key lessons learned and outlines recommendations for future standardization and research. Overall, the present document demonstrates that the DSP is a viable and promising approach to improve trust, traceability and automation across device supply chains.

Introduction

Digital products and connected devices are increasingly embedded in complex and dynamic ecosystems involving multiple stakeholders across global supply chains. Manufacturers, system integrators, operators and service providers each contribute to the security posture of a device at different stages of its lifecycle. At the same time, cybersecurity threats are becoming more frequent and sophisticated, while regulatory frameworks are imposing stricter obligations related to transparency, vulnerability management and lifecycle support.

In response to these challenges, a growing number of security descriptors and standards have emerged, including components inventory, network behaviour profiles, vulnerability disclosure formats and risk reporting mechanisms. While these artefacts address specific aspects of device security, they are typically developed and managed in isolation. As a result, security information is fragmented across multiple documents, formats and repositories, making it difficult to obtain a consistent and up-to-date view of a device's security posture.

This fragmentation is further exacerbated by the dynamic nature of security information. Vulnerabilities, configurations and operational contexts evolve continuously after deployment, requiring mechanisms that support updates, traceability and accountability over time. Traditional documentation-based approaches are poorly suited to this task, as they rely heavily on manual processes and human interpretation.

In parallel, regulatory pressure is increasing. New European frameworks, such as the Cyber Resilience Act (CRA) [i.1], the Network and Information Systems 2 Directive (NIS2) [i.2] and the EU Cybersecurity Act (CSA) [i.3], introduce lifecycle-oriented obligations for manufacturers and operators, including transparency requirements, vulnerability management processes and post-market support obligations. Meeting these requirements using ad hoc documentation and disconnected artefacts introduces significant overhead for manufacturers and operators and limits the potential for automation.

These challenges highlight the need for a unified approach to managing device security information across the entire lifecycle. The Device Security Passport (DSP) is proposed as a response to this need. Rather than introducing yet another standalone descriptor, the DSP acts as an aggregation layer that links existing security artefacts while preserving their original formats and ownership. By providing a single logical entry point to security information, the DSP improves visibility, supports automation and enables continuous security assurance.

get full document from standards.iteh.ai

1 Scope

The present document focuses on presenting the results, observations and lessons learned derived from the analysis and application of the Device Security Passport (DSP) concept in real project environments. In particular, it examines its instantiation within the DOSS project, which addresses security challenges in complex device supply chains with a focus on lifecycle-oriented security management and information sharing. The present document analyses how the DSP can be used as a unifying mechanism to support transparency, traceability and automation across the device lifecycle, and discusses its applicability to emerging regulatory and certification frameworks. The present document does not define normative requirements, but rather provides technical insights and experience-based observations intended to inform future standardization and research activities.

2 References

2.1 Normative references

Normative references are not applicable in the present document.

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 may be useful in implementing an ETSI deliverable or add to the reader's understanding, but are not required for conformance to the present document.

- [i.1] [Regulation \(EU\) 2024/2847](#) of the European Parliament and of the Council of 23 October 2024 on horizontal cybersecurity requirements for products with digital elements and amending Regulations (EU) No 168/2013 and (EU) 2019/1020 and Directive (EU) 2020/1828 (Cyber Resilience Act).
- [i.2] [Directive \(EU\) 2022/2555](#) of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS 2 Directive).
- [i.3] [Regulation \(EU\) 2019/881](#) of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act).
- [i.4] National Telecommunications and Information Administration (NTIA) (2021): "[The Minimum Elements For a Software Bill Of Materials \(SBOM\) Pursuant to Executive Order 14028 on Improving the Nation's Cybersecurity](#)".
- [i.5] Cybersecurity and Infrastructure Security Agency CISA: "[Hardware Bill of Materials \(HBOM\) Framework for Supply Chain Risk Management](#)", September 25, 2023.
- [i.6] IBM: "[CBOM: Cryptography Bill of Materials](#)" June 29, 2023.
- [i.7] CycloneDX: "[Machine Learning Bill of Materials \(ML-BOM\)](#)".
- [i.8] CycloneDX: "[Manufacturing Bill of Materials \(MBOM\)](#)".
- [i.9] CycloneDX: "[Operations Bill of Materials \(OBOM\)](#)".

- [i.10] CycloneDX: "[Software as a Service \(SaaS BOM\)](#)".
- [i.11] [ISO/IEC 5962:2021](#): "Information technology — SPDX® Specification V2.2.1".
- [i.12] [ECMA-424](#): "CycloneDX Bill of materials specification", December 2025.
- [i.13] [ISO/IEC 19770-2:2015](#): "Information technology — IT asset management. Part 2: Software identification tag".
- [i.14] [IETF RFC 8520 \(March 2019\)](#): "Manufacturer Usage Description Specification", E. Lear, D. Romascanu, and R. Droms.
- [i.15] [IETF RFC 7950 \(August 2016\)](#): "The YANG 1.1 Data Modeling Language", M. Bjorklund.
- [i.16] [IETF RFC 9761 \(April 2025\)](#): "Manufacturer Usage Description (MUD) for TLS and DTLS Profiles for Internet of Things (IoT) Devices", T. Reddy.K, D. Wing, B. Anderson.
- [i.17] [IETF RFC 9472 \(October 2023\)](#): "A YANG Data Model for Reporting Software Bills of Materials (SBOMs) and Vulnerability Information", E. Lear, S. Rose.
- [i.18] S. Sebastio, S. Beena, S. Matheu, R. Atoui and A. Skarmeta: "Bolstering Up Smart Products Cybersecurity (Re-)Certification with Manufacturer's Evidence", 2025 IEEE International Conference on Smart Computing (SMARTCOMP), Cork, Ireland, 2025, pp. 270-275, doi: 10.1109/SMARTCOMP65954.2025.00085.
- [i.19] A. Molina Zarca, J. Bernal Bernabé, J. Ortíz, A. Skarmeta: "D2.5 Policy-based Definition and Policy for Orchestration Final Report", ANASTACIA Project, 2018.
- [i.20] NIST SP 1800-15 (2019): "Securing Small-Business and Home Internet of Things Devices".
- [i.21] CISA: "[Minimum Requirements for Vulnerability Exploitability eXchange \(VEX\)](#)", 2023.
- [i.22] CycloneDX: "[Vulnerability Exploitability eXchange \(VEX\)](#)".
- [i.23] OASIS (2025): "[Common Security Advisory Framework Version 2.1](#)".
- [i.24] GitHub: "[OpenVEX](#)" March 10, 2026.
- [i.25] [NIST SP 800-161r1](#): "Cybersecurity Supply Chain Risk Management for Systems and Organizations", Boyens, Jon M, 2022.
- [i.26] CycloneDX: "[Vulnerability Disclosure Report \(VDR\)](#)".
- [i.27] NIST: "[OSCAL V1.2.0 Reference](#)".
- [i.28] Garcia, Jesus (06/09/2023): "[EUROSCAL -Paving the Road towards Automated Cybersecurity Certification in Europe \(Whitepaper\)](#)".
- [i.29] [NIST SP 800-126r4 ipd](#): "Technical Specification for the Security Content Automation Protocol (SCAP)", 2025.
- [i.30] CVE Foundation: "[Common Vulnerabilities and Exposures](#)".
- [i.31] NIST: "[CCE Platform listing](#)", 2015.
- [i.32] [NIST Interagency Report 7695](#): "Common Platform Enumeration: Naming Specification Version 2.3", 2011, Cheikes, Brant, David Waltermire, and Karen Scarfon.
- [i.33] FIRST Forum of Incident Response and Security Teams: "[Common Vulnerability Scoring System: Specification Document](#)", 2023.
- [i.34] [NIST Interagency Report 7275 \(Revision 4\)](#): "Specification for the Extensible Configuration Checklist Description Format (XCCDF) Version 1.2", Waltermire, David, Charles Schmidt, Karen Scarfone, and Neal Ziring.
- [i.35] OVAL Community: "The OVAL Community Guidelines 5.12.2 Documentation", 2024.