ETSI TR 103 937 V1.1.1 (2024-08)

Cyber Security (CYBER);
Cyber Resiliency and Supply Chain Management

Reference
DTR/CYBER-0099

Keywords
cyber security, cyber-defence, risk management

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

Contents

Intellectual Property Rights

Essential patents

IPRs essential or potentially essential to normative deliverables 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 Web server (https://ipr.etsi.org/).

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™** and **LTE™** 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 Cyber Security (CYBER).

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 development of tools for cyber resiliency under a broad "Zero Trust Model" aegis continue evolve and include Supply Chain Bill of Materials (SBOM), community exchange of vulnerability and remediation code, Continuous Monitoring for threat anomalies, and application of Critical Security Controls.

Introduction

Over the past several years, the increasing significant attacks on ICT infrastructure has led to a return to cybersecurity fundamentals developed after the conceptualization of packet data networks to provide access to computer resources. It was a realization that persistent vulnerabilities in every digital element and system will always exist, that "ex ante" trust certifications were minimally useful, and that a different set of tools was necessary. The development of these tools for cyber resiliency proceeded under a broad "Zero Trust Model" aegis that includes Supply chain Bill Of Materials (SBOM), community exchange of vulnerability and remediation code, Continuous Monitoring for threat anomalies, and application of Critical Security Controls.

1 Scope

The present document addresses cyber resiliency throughout the supply chain and the various related frameworks and measures using risk-based, system of trust, and zero trust approaches, including the proposed EU Cyber Resilience Act, [i.1] through [i.8].

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 are not necessary for the application of the present document but they assist the user with regard to a particular subject area.

[i.1] Proposal for a Regulation of the European Parliament and of the Council on horizontal cybersecurity requirements for products with digital elements and amending Regulation (EU) 2019/1020.

[i.2] Regulation (EU) 2019/1020 of the European Parliament and of the Council of 20 June 2019 on market surveillance and compliance of products and amending Directive 2004/42/EC and Regulations (EC) No 765/2008 and (EU) No 305/2011.

[i.3] 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.4] Directive (EU) 2022/2557 of the European Parliament and of the Council of 14 December 2022 on the resilience of critical entities and repealing Council Directive 2008/114/EC (Text with EEA relevance).

[i.5] Regulation (EU) 2022/2554 of the European Parliament and of the Council of 14 December 2022 on digital operational resilience for the financial sector and amending Regulations (EC) No 1060/2009, (EU) No 648/2012, (EU) No 600/2014, (EU) No 909/2014 and (EU) 2016/1011.

[i.6] Consolidated text: Commission Delegated Regulation (EU) 2021/2106 of 28 September 2021 on supplementing Regulation (EU) 2021/241 of the European Parliament and of the Council establishing the Recovery and Resilience Facility by setting out the common indicators and the detailed elements of the recovery and resilience scoreboard.

[i.7] United Kingdom: "Product Security and Telecommunications Infrastructure Act 2022".

[i.8] Switzerland: "120.73 Ordinance of 27 May 2020 on Protection against Cyber Risks in the Federal Administration (Cyber Risks Ordinance, CyRV)".

[i.9] 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) (Text with EEA relevance).

[i.10] ETSI TR 103 866: "Cyber Security (CYBER); Implementation of the Revised Network and Information Security (NIS2) Directive applying Critical Security Controls".

[i.11] ETSI TR 103 305-1: "Cyber Security (CYBER); Critical Security Controls for Effective Cyber Defence; Part 1: The Critical Security Controls".

[i.12] ETSI TR 103 305-4: "Cyber Security (CYBER); Critical Security Controls for Effective Cyber Defence; Part 4: Facilitation Mechanisms".

[i.13] NIST SP 800-161r1: "Cybersecurity Supply Chain Risk Management Practices for Systems and Organizations".

[i.14] MITRE: "System of Trust™: Supply Chain Security".

[i.15] NIST SP 800-207: "Zero Trust Architecture".

[i.16] 3GPP TR 33.894: "Technical Specification Group Services and System Aspects; Study on applicability of the Zero Trust Security principles in mobile networks (Release 18)".

[i.17] Cloud Security Alliance, Zero Trust publications.

[i.18] NIST NCCoE: "Implementing a Zero Trust Architecture".

[i.19] CISA: "Zero Trust Maturity Model", Version 2.0.

[i.20] National Security Agency: "Cybersecurity Information: Embracing a Zero Trust Security Model".

[i.21] NCSC: "Zero trust architecture design principles".

[i.22] ITU-T: "MITRE"s System of Trust™, Software Supply Chair Risks That May Need to Be Addressed".

[i.23] IETF RFC charter-ietf-scitt: "Supply Chain Integrity, Transparency, and Trust (scitt)".

[i.24] IETF RFC draft-ietf-scitt-architecture: "An Architecture for Trustworthy and Transparent Digital Supply Chains".

[i.25] US ODNI, NSA, CISA: "Securing the Software Supply Chain: Recommended Practices for Software Bill of Materials Consumption".

[i.26] NCSC: "Guidelines for secure AI system development".

[i.27] NSA: "Advancing Zero Trust Maturity Throughout the Device Pillar".

[i.28] GSMA: "Supply Chain Toolbox".

[i.29] NTIA: "Software Bill of Materials".

[i.30] ITU-T TR.zt-acp: "Technical Report on Guidelines for zero trust based access control platform in telecommunication networks".

[i.31] ITU-T X.st-ssc: "Security threats of software supply chain".

[i.32] CISA: "Information and Communications Technology Supply Chain Security".

[i.34] U.S. Executive Office of the President, NSM-22: "National Security Memorandum on Critical Infrastructure Security and Resilience", 30 April 2024.