

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



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

(<https://standards.iteh.ai>)

Document Preview

[ETSI TR 103 937 V1.1.1 \(2024-08\)](https://standards.iteh.ai/catalog/standards/etsi/79705180-9ece-4a72-9ac0-b859ec542e88/etsi-tr-103-937-v1-1-1-2024-08)

<https://standards.iteh.ai/catalog/standards/etsi/79705180-9ece-4a72-9ac0-b859ec542e88/etsi-tr-103-937-v1-1-1-2024-08>

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

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](#).

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 may be reproduced or utilized in any form or by any means, electronic or mechanical, including photocopying and microfilm except as authorized by written permission of ETSI.

The content of the PDF version shall not be modified without the written authorization of ETSI.

The copyright and the foregoing restriction extend to reproduction in all media.

© ETSI 2024.
All rights reserved.

Contents

Intellectual Property Rights	4
Foreword.....	4
Modal verbs terminology.....	4
Executive summary	4
Introduction	4
1 Scope	5
2 References	5
2.1 Normative references	5
2.2 Informative references.....	5
3 Definition of terms, symbols and abbreviations.....	7
3.1 Terms.....	7
3.2 Symbols.....	7
3.3 Abbreviations	7
4 Concepts and model frameworks	8
4.1 Cyber resiliency.....	8
4.2 Supply chain risk management.....	8
4.2.1 Government-driven supply chain risk management model frameworks.....	8
4.2.2 Industry-developed supply chain risk management model frameworks	10
4.3 Zero trust model frameworks	12
4.3.1 Government-driven model frameworks to enable Zero Trust.....	12
4.3.2 Industry-developed model frameworks to enable Zero Trust	13
5 Implementation platforms and measures.....	14
5.1 Cyber resiliency platforms and measures.....	14
5.2 Supply chain management platforms and measures	14
5.3 Zero trust platforms and measures	15
Annex A: Bibliography	16
History	17

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 Chain 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.