



Cyber Security (CYBER); Cyber Resilience Act (CRA); Essential cybersecurity requirements for Network Management Systems (NMS)

Exercising one of the **Principles of International Standardization – Openness** – and taking them to a different level, ETSI CYBER-EUSR has conducted open consultations on the vertical standards in support of the Cyber-Resilience Act, at a much earlier stage than it is usual in the standardization world. In this context, please keep in mind that the present document is an INTERIM draft, which expectably will be subject to substantial changes before their target publication date in the second semester of 2026.

ETSI CRA vertical standards v1.1.1 are being finalized and undergoing Public Enquiry via the National Standardization Organizations (NSO). Therefore, starting from 16 April 2026, ETSI CYBER-EUSR may only be able to address your comments in a future revision of the standard. **To enable ETSI CYBER-EUSR to address your comments before the first publication of the standards, you should cumulatively submit to your NSO any comments submitted here from 16 April 2026 onwards.** If you don't know how to do this, email us at cybersupport@etsi.org and we will guide you in the process.

Disclaimer: The INTERIM DRAFTS available for download in this page are provided for information and are for future development work within the ETSI Technical Committee CYBER EUSR Working Group (CYBER-EUSR) only. ETSI and its Members accept no liability for any further use/implementation of these specifications. Approved and published specifications and reports shall be obtained exclusively via the ETSI Documentation Service at <http://www.etsi.org/standards-search>

Commenting guidelines: Your comments to improve this early draft are very welcomed. To ensure the effectiveness of your contribution, please make sure to include the following elements in your comment:

1. Clear identification of the section of the draft your comment is referring to.
2. Objective proposal to delete content, add content or substitute content.
3. Concrete contribution (exact content you suggest including in the draft as an addition to, or in substitution of, existing content).
4. Brief rationale to justify the proposal (e.g. why the suggested content should be added an/or the existing content should be deleted or substituted).

Please note that comments without concrete contributions will be noted but not acted upon by ETSI CYBER-EUSR. We trust and value your expertise and therefore expect you to take this opportunity to proactively contribute to solving the issues you find while analysing this early draft.

Use of Artificial Intelligence (AI): Please do not use large language models to generate your comments. Inclusion of language generated by “AI” creates a potential for intellectual property conflicts and liability for ETSI, which is not acceptable.

How to comment: To comment or provide feedback on the present interim draft please visit:

<https://labs.etsi.org/rep/stan4cra/en-304-621> and submit your comments as “issues” following the guidelines provided on this site. Alternatively, you may also send your comments to: cybersupport@etsi.org using the “[ETSI Commenting Format for Open Consultation.xlsx](#)” available in <https://docbox.etsi.org/CYBER/EUSR/Open>

Feedback on your comments: The resolutions made in **Consensus** by ETSI CYBER-EUSR members, on each comment received through these Open Consultations will be published at the ETSI Open Area and ETSI Lab, assuring full **Transparency**.

Reference

< TC/WI-Number >

Keywords

< CRA, Cybersecurity, Network >

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.

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 2025.
All rights reserved.

Contents

Intellectual Property Rights	6
Foreword.....	6
Modal verbs terminology	7
Introduction	7
1 Scope	8
1.1 General.....	8
1.2 Products in scope	8
2 References	8
2.1 Normative references.....	8
2.2 Informative references	8
3 Definition of terms, symbols and abbreviations.....	9
3.1 Terms.....	9
3.2 Abbreviations.....	9
4 Product context.....	10
4.1 General.....	10
4.3 Product overview and architecture.....	10
4.4 Use cases.....	11
4.4.1 Distributed deployment.....	12
4.4.1.1 IoT network with monitoring data collection	13
4.4.1.2 Home network deployment	14
4.4.2 Multi-user deployment.....	15
4.4.2.1 Enterprise network.....	15
4.4.2.2 Telecom network.....	17
4.4.3 Alternative deployments.....	17
4.4.3.1 Logical network deployment.....	18
4.4.3.2 Physical network deployment with RDPS.....	19
4.5 Risk Factors	21
4.5.1 List of Risk Factors	22
4.5.1.1 Service requesting users	22
4.5.1.2 Complexity of managed network element implementation	22
4.5.1.3 Security expectations of the deployment context	23
4.5.1.4 Deployment context network segmentation	24
4.5.2 Mapping of use cases to risk factors	24
4.6 Security Profile	24
4.7 Essential functions	25
4.8 Operational Environment.....	25
4.9 Users	25
4.10 Distribution of security functions	25
4.10.1 External security functions, not in scope of the present document	26
4.10.2 Security functions provided to other products.....	26
5 Requirements specifications.....	26
5.1 General.....	26
5.1.1 No known exploited vulnerabilities	27
5.1.2 Secure design, development and production	27
5.1.3 Product vulnerability management process.....	27
5.2 Technical cybersecurity requirements specifications.....	27
5.2.1 Secure channel	28
5.2.2 Cryptographic key intialisation and rotation	28
5.2.3 Network segmentation.....	29
5.2.4 State-of-the-art cryptographic libraries	29
5.2.5 Software Bill of Materials	29
5.2.6 Role based authorisation	29

5.2.7	Remote Data Processing Systems	30
5.3	Risk Mitigations.....	30
5.3.1	Mitigations for user identity integrity	30
5.3.2	Mitigations for ingested data integrity and confidentiality.....	30
5.3.3	Mitigations for managed device configuration integrity and confidentiality	31
5.3.4	Secure updates.....	31
5.3.5	Logging.....	32
5.3.6	Metrics	32
5.3.7	Data minimisation	33
5.3.8	High Availability.....	33
6	Conformity assessments and tests.....	34
6.1	General requirements assessments.....	34
6.1.0.0	REQ-GEN-0.....	34
6.1.0.1	REQ-GEN-1	34
6.1.0.2	REQ-GEN-2	35
6.1.1	No known exploited vulnerabilities tests	35
6.1.1.0	REQ-EXPLOIT-0.....	35
6.1.1.1	REQ-EXPLOIT-1	36
6.1.1.2	REQ-EXPLOIT-2.....	36
6.2	Technical cybersecurity requirement tests and assessments	37
6.2.0.0	REQ-TECH-0.....	37
6.2.0.1	REQ-TECH-1.....	37
6.2.0.2	REQ-TECH-2.....	38
6.2.0.3	REQ-TECH-3.....	38
6.2.0.4	REQ-TECH-4.....	39
6.2.0.5	REQ-TECH-5.....	39
6.2.0.6	REQ-TECH-6.....	40
6.2.0.7	REQ-TECH-7.....	40
6.2.5.0	REQ-SBOM-0	41
6.2.5.1	REQ-SBOM-1	41
6.2.5.2	REQ-SBOM-2	41
6.3	Risk mitigations tests	42
6.3.6	Metrics tests	42
6.3.6.0	REQ-METRICS-0	42
6.3.6.1	REQ-METRICS-1	42
6.3.6.2	REQ-METRICS-2	43
6.3.6.3	REQ-METRICS-3	43
6.3.6.4	REQ-METRICS-4	44
6.3.6.5	REQ-METRICS-5	45
6.3.6.6	REQ-METRICS-6	45
6.3.6.7	REQ-METRICS-7	46
6.3.6.8	REQ-METRICS-8	46
6.3.6.9	REQ-METRICS-9	47
6.3.8	High availability tests.....	47
6.3.8.0	REQ-HA-0.....	47
6.3.8.1	REQ-HA-1.....	48
6.3.8.2	REQ-HA-2.....	48
6.3.8.3	REQ-HA-3.....	49
Annex A (informative): Mapping with essential requirements of the CRA.....		50
Annex B (informative): Relationship between the present document and any related ETSI standards (if any).....		51
Annex C (informative): Risk acceptance criteria and risk management methodology		52
C.1	Risk acceptance and risk management methodology.....	52
C.2	Risk assessment methodology	52
C.2.1	Assets	52
C.2.1.1	Data assets.....	53
C.2.2	Threats.....	53
C.3	Assumptions	54

Annex D (informative): Risk evaluation guidance.....	55
Annex L (informative): Relationship between the present document and the requirements of EU Regulation 2024/2847	56
Annex <L+3> (informative): Bibliography.....	57
Annex <L+4> (informative): Change history.....	57
History	58

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 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

DRAFT FOREWORD - DO NOT CONSIDER THE CONTENT

This draft Harmonised European Standard (EN) has been produced by ETSI Technical Committee Cyber Working Group for EUSR (CYBER-EUSR), and is now submitted for the combined Public Enquiry and Vote phase of the ETSI Standardisation Request deliverable Approval Procedure (SRdAP).

It is one of a series of standards prepared under the Commission's standardisation request to the European Committee for Standardisation (CEN), the European Committee for Electrotechnical Standardisation (Cenelec) and the European Telecommunications Standards Institute (ETSI) as regards products with digital elements in support of 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).

The present document has been prepared under the Commission's standardisation request C(2025) 618 final to provide one voluntary means of conforming to the requirements of Regulation (EU) No 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) No 2019/1020 and Directive (EU) 2020/1828 (Cyber Resilience Act).

Once the present document is cited in the Official Journal of the European Union under that Regulation, compliance with the normative clauses of the present document given in table A.1 confers, within the limits of the scope of the present document, a presumption of conformity with the corresponding requirements of that Regulation and associated EFTA regulations.

Transposition table

The Harmonised Standard shall have appropriate transposition periods specified. A Harmonised Standard confers presumption of conformity when it has been published in the Official Journal of the European Union (OJEU) and transposed by a member state.

The Technical Body may propose different dates to the default ones (3, 6, 18). Technical Bodies who wish to propose different dates are advised to indicate this clearly in the approved committee draft.

Proposed national transposition dates	
Date of latest announcement of this EN (doa):	3 months after ETSI publication
Date of latest publication of new National Standard or endorsement of this EN (dop/e):	6 months after doa
Date of withdrawal of any conflicting National Standard (dow):	18 months after doa

The Technical Body should advise the ETSI Secretariat if the above default national transposition dates are inappropriate for the particular standard.

Modal verbs terminology

In the present document "**shall**", "**shall not**", "**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.

Introduction

This document is a European harmonised standard that defines cybersecurity requirements for network management systems.

1 Scope

1.1 General

The present document is created for EU Regulation 2024/2847, the Cyber Resilience Act.

1.2 Products in scope

The implementing regulation [i.11] defines in section (2) that the core functionality of a product defines what category it should be evaluated under. The regulation continues to define in section (3), that when the product is a composite of other recognised products, the composite product doesn't inherit all other regulations, but is evaluated only in its own category.

The implementing regulation [i.11] (ANNEX I, Class I, 6.) defines the following:

Products with digital elements that manage connected network elements, such as servers, routers, switches, workstations, printers or mobile devices, by monitoring them and controlling their network operations and configuration.

This category includes but is not limited to end-to-end management systems and dedicated configuration management systems, such as controllers for software-defined networking.

This quotation is not to be used as a source of the truth, as the definition might change. Refer to the source for the latest description.

The NMS is defined in the implementing regulation [i.11] in Annex I, Class I (6) and is not restricted to only systems that are IP connected. The scope covers all connected elements in the network, that are managed. This includes, but is not limited to, Mobile Device Management systems and Software Defined Networking.

Bluetooth consumer devices are usually not managed by an NMS, however, if they are capable, a NMS management could control them too, as Bluetooth is just a communication media and can be used also for management traffic. Such, NMS's often control more than just network configuration - e.g., MDM systems.

2 References

2.1 Normative references

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 necessary for the application of the present document.

- [1] ENISA April 2025 (Version 2.0) "Agreed Cryptographic Mechanisms"
- [2] prEN 40000-1-3 "Vulnerability Handling"

2.2 Informative references

References are either specific (identified by date of publication and/or edition number or version number) or nonspecific. 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] EU 2024/2847 "Cyber Resilience Act"
- [i.2] ETSI EN 304 XXX IAM (CEN/TC 224 WG 17 output)

- [i.3] ETSI EN 304 620 "Virtual Private Networks (VPNs)"
- [i.4] CEN/CLC EN 50XXX-4 "VPN"
- [i.5] ETSI EN 304 626 "Essential cybersecurity requirements for operating systems"
- [i.6] ETSI EN 304 624 "PKIs and certificate issuance software"
- [i.7] ETSI EN 304 622 "Essential cybersecurity requirements for Security information and event management (SIEM) systems"
- [i.8] ETSI EN 304 627 "Router, modems and switches"
- [i.9] ETSI EN 304 642 "Cybersecurity Requirements for Telecommunication Systems"
- [i.10] [Mitre ATT&CK](#) framework
- [i.11] EU 2025/2392 Commission implementing regulation on the technical description of the categories of important and critical products with digital elements pursuant to Regulation EU 2024/2847 (CRA)
- [i.12] ISO/IEC 27000:2018
- [i.13] NIST SP 800-63B-4 Authentication & Authenticator Management
- [i.14] prEN 40000-1-1 "Vocabulary"
- [i.15] prEN 40000-1-2 "Principles for cyber resilience"

3 Definition of terms, symbols and abbreviations

3.1 Terms

This section provides terms and definitions based on CEN/CLC JTC13 WG09's work on terms and definitions, terms and definitions provided by ETSI EN 303 645/TS 103 701 and terms and definitions provided by CEN/CLC EN 18031 series.

For the purposes of the present document, the following terms apply:

1. **Operating System (OS):** software product that provides an abstract interface to the underlying hardware and control the execution of software
2. **Identity Provider (IDP):** system maintaining identity information
3. **Service Requesting Users (SRU):** users relying on the correct functioning of the network element
4. **user:** person having the credentials to login to the NMS to operate administrative actions to control and maintain the managed element
5. **machine user:** virtual user used to access the system programming interfaces
6. **component:** software or hardware intended for integration into an electronic information system
7. **Application Programming Interface (API):** interface used to communicate with the running program
8. **log:** record of an operational event
9. **trace:** record of a system status with all relevant data that can be gathered

3.2 Abbreviations

For the purposes of the present document, the following abbreviations apply:

CRA	Cyber Resilience Act
OS	Operating System

IDP	Identity Provider
VPN	Virtual Private Network
SIEM	Security Information and Event Management Systems
NMS	Network Management System
2FA	Two Factor Authentication
CSP	Communication System Provider
SDN	Software Defined Networks
GUI	Graphical User Interface
NE	Network Element
MDM	Mobile Device Management

4 Product context

4.1 General

NOTE: This section's structure is built upon CEN/CLC JTC13 PT01's deliverable and might require restructuring based on its progress.

4.3 Product overview and architecture

Network management systems are commonly deployed using centralized management services that provide command, control, monitoring, and administration functions.

Depending on the design and autonomy of the managed elements, some elements may continue limited operation when connectivity to the network management system is unavailable. In larger deployments, network design and operational parameters can affect the reliability and scalability of connectivity between managed elements and the network management system.

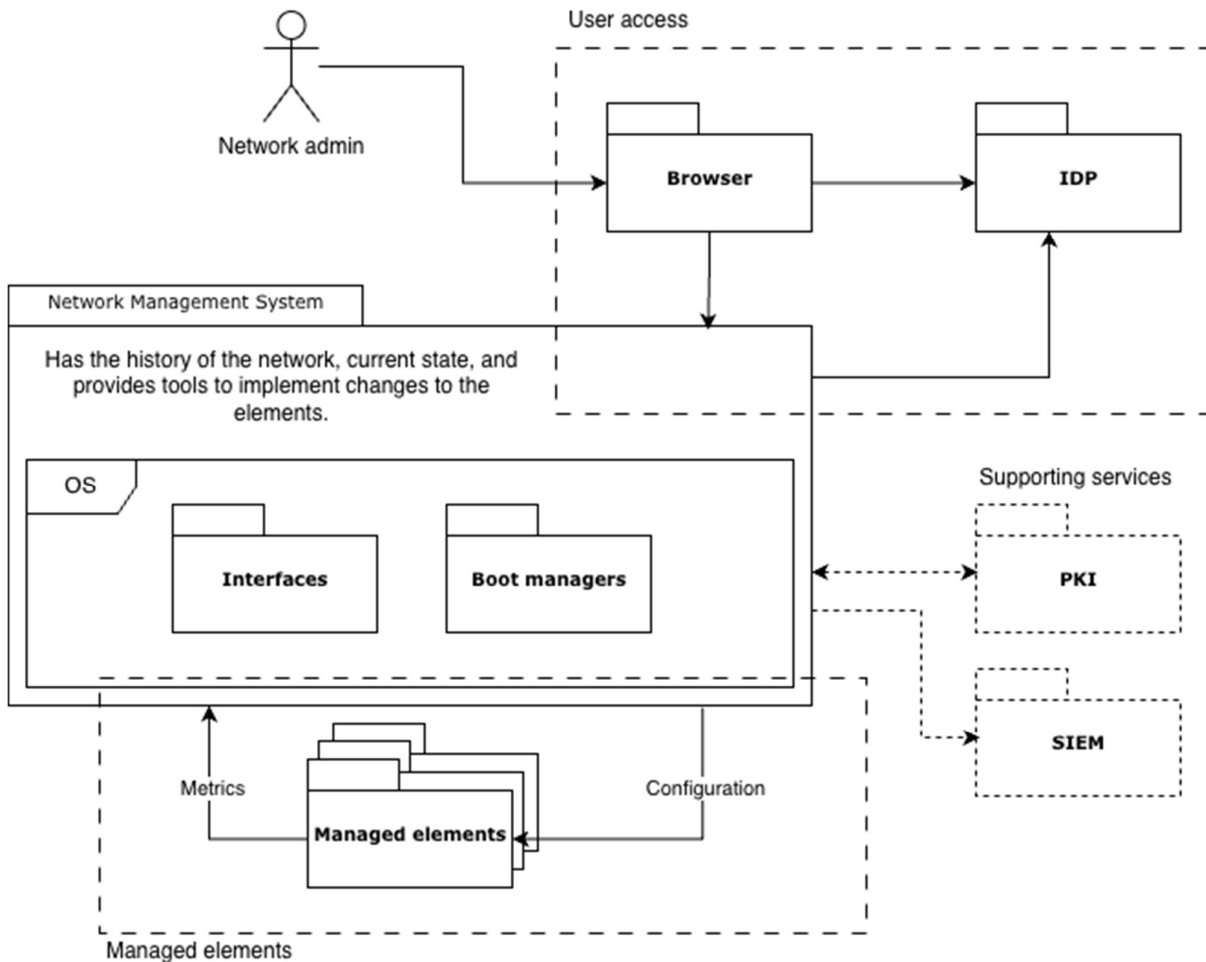


Figure 4.3-1: Product overview and architecture

Network management systems are operated by users or by programs that interface with an API. These programs can be internal or external to the system depending on the product design and deployment context.

The system is often accessed with a browser using an identity outside of the installation context. Identity Provider (IdP) can be used as base for the users identity. In an enterprise setting, or equivalent, the high number of users and the volume of role changes has lead to adoption of dedicated identity management platforms.

The system typically runs on hardware and software components that provide the necessary operating environment and network connectivity. The Operating System can be part of the deliverable and hence, part of the product. The OS best practices and requirements are defined outside of this document.

Where relevant to the deployment context, the NMS may interface with external services such as identity, cryptographic, logging, or event management systems, though cybersecurity requirements of these systems, even if integrated into the NMS product, are not addressed by this standard.

The primary function of an NMS is to monitor, configure, administer, or otherwise manage connected network elements.

More about assets in [Annex C.1 Assets](#) and [Annex C.2 Data](#).

4.4 Use cases

This list of use cases is a resource for manufacturers to simplify the selection of a set of cybersecurity requirements.

Manufacturer's technical documentation may benefit from including or referring to these use cases and to security profiles.

An NMS is a product controlling at least partially connected devices with network access. Despite its central positioning, an NMS can be an aggregate of several components, including but not limited to: end-to-end management systems, dedicated configuration management systems, or controllers for software-defined networking as described in chapter 1.2.

NMS can be composed of several components or can implement additional functions that are outside the scope of the present standards. One example of this type of aggregate product design would an implementation where the operating system acts as abstraction layer for the system(s) that host the NMS, or the networking interfaces.

4.4.1 Distributed deployment

- Distributed element design
- Insignificant amount of interconnectivity within the network elements
- Lesser importance by the type of the controlled managed elements in their functionality and role in the deployment context
- Isolated management system design
- Pocket deployments with high independency

Devices are limited in functionality like:

1. Simple low-risk embedded device (coffee machine, fridge)
2. Stationary IoT embedded device (lightbulb, thermostat)

The affected Service Requesting Users base is small like in:

1. IoT network elements in a small deployment
2. Single home network deployment

4.4.1.1 IoT network with monitoring data collection

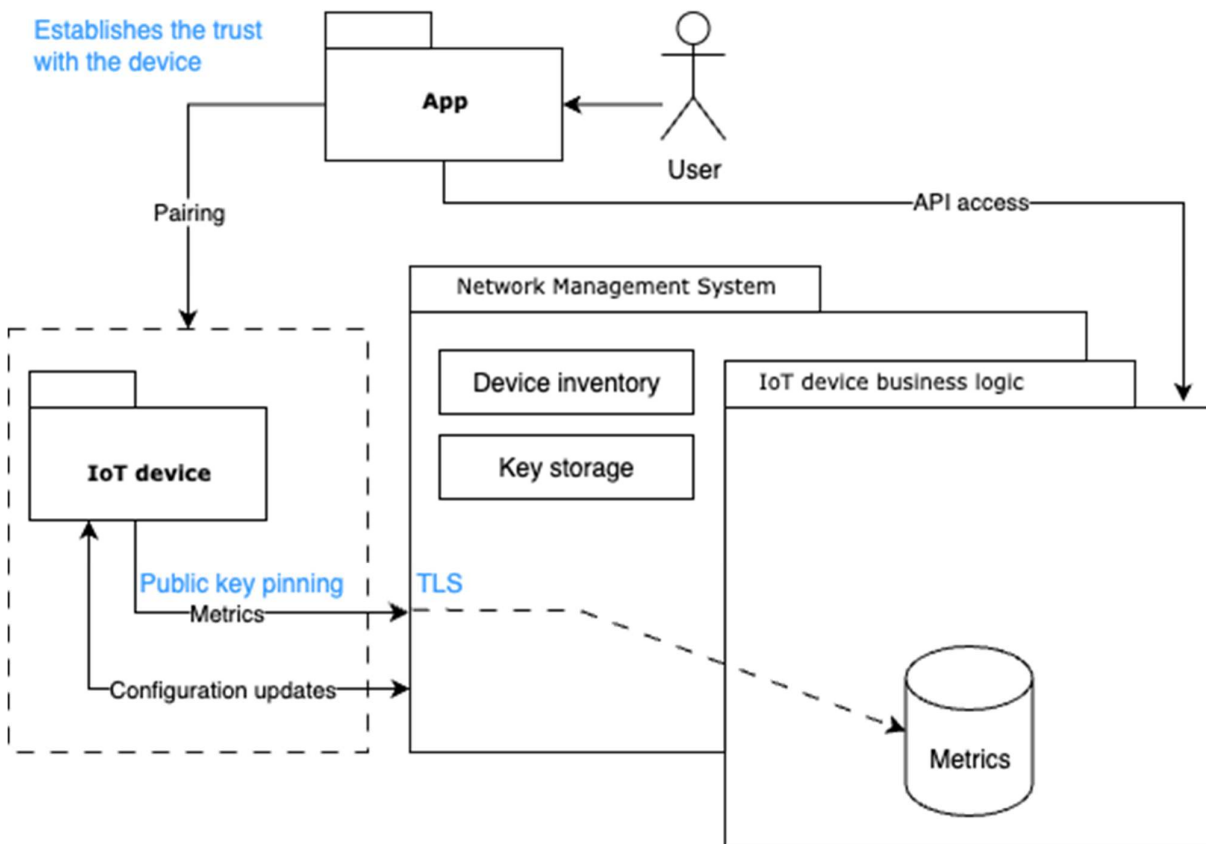


Figure 4.4.1.1-1: IoT network with monitoring data collection

An IoT network is a network of devices, each of which almost always has limited computational capabilities and consumes a low amount of power. The exact purpose of these device varies, but they are all connected to an NMS, and often to each other and to an IoT business logic, which may be a RDPS. The main focus of an IoT network is almost always data collection, and the NMS in this use case usually visualises the collected data metrics and provides them to the end-user. The NMS-analysis of the data metrics can be automated, including triggering warnings, alarms, or even taking actions based on discovered abnormal events.

The NMS controls the configuration of the connected devices, and has a two minimum functions:

1. Establishes and maintains a trust-based relation between itself and the devices.

To initialize a trust-based relationship between this type of network management system and connected devices, both of which store credentials, usually in the form of pre-installed keys, identity confirming certificates, or unique serial numbers. These credentials are used during initialisation to create the trusted relationship between the NMS, the devices and, if present, with the IoT device business logic. Credential or key initialisation, and key enrolment or establishment limit the NMS's ability to establish a trusted relationship to the intended devices, an ability further limited as these methods require physical access or close proximity to the IoT device. For example, an IoT device user can pair the IoT device and establish a trust-based relationship with the NMS through Bluetooth (tm) mechanisms or with a physical cable connection.

Once the trust-based relationship has been established, the NMS can provide cryptographically protected configuration and update services to the devices at runtime. Depending on the initial NMS and managed element configurations, the device can either request its configuration from the NMS, or the NMS can push the configuration to the device. The trust-based relationship can also provide for secured identification, authentication, and communication with other applications on a device.

The IoT network NMS collects the meta traffic data and management related data from networked devices, or forwards it to other systems for data collection and storage. All data transmitted from the devices to the NMS and all data

transmitted from the NMS to the devices is cryptographically protected with authentication of the endpoints, and with integrity and confidentiality protection. Independent of any of the host system's capabilities, the NMS can also be remotely accessible.

2. Generates and maintains an inventory of devices that are part of the managed network,

The second primary function of an IoT network NMS is to generate, keep, and maintain a network inventory. This inventory holds information about the connectivity capabilities for each connected device. When new devices are added and a trust-based relationship is established with them, they extend the network and the inventory is amended.

Users of the IoT device business logic or of managed elements are protected from unauthorised access when interacting with each other or with the NMS. Malicious impact on these communication channels, such as interception, interruption, or inducing data packets is detected and the system creates an event that is recorded, and if applicable, reported.

The above given example architecture of figure 3 can serve as explanation help during the conformity assessment to meet CRA [i.1] Annex I part 1.

NOTE: This use case seems to focus on two security functions of IoT products, but make no distinctions between large and small IoT networks (with corresponding botnet risks) or products designed for higher risk environments (e.g. home "convenience" devices such as a set of speakers < home essential devices such as lighting < enterprise and industrial deployments such as warehouse or factory lighting and < high risk infrastructural device/environments such as freezer units at a large scale meat storage facility.) To me these levels of risk represent sub use cases and maybe lesser requirements/mitigations for low risk/impact devices? Additionally the degree of remote service involved in the NMS may also create sub classes (or potentially it could be modelled as a risk factor?)

4.4.1.2 Home network deployment

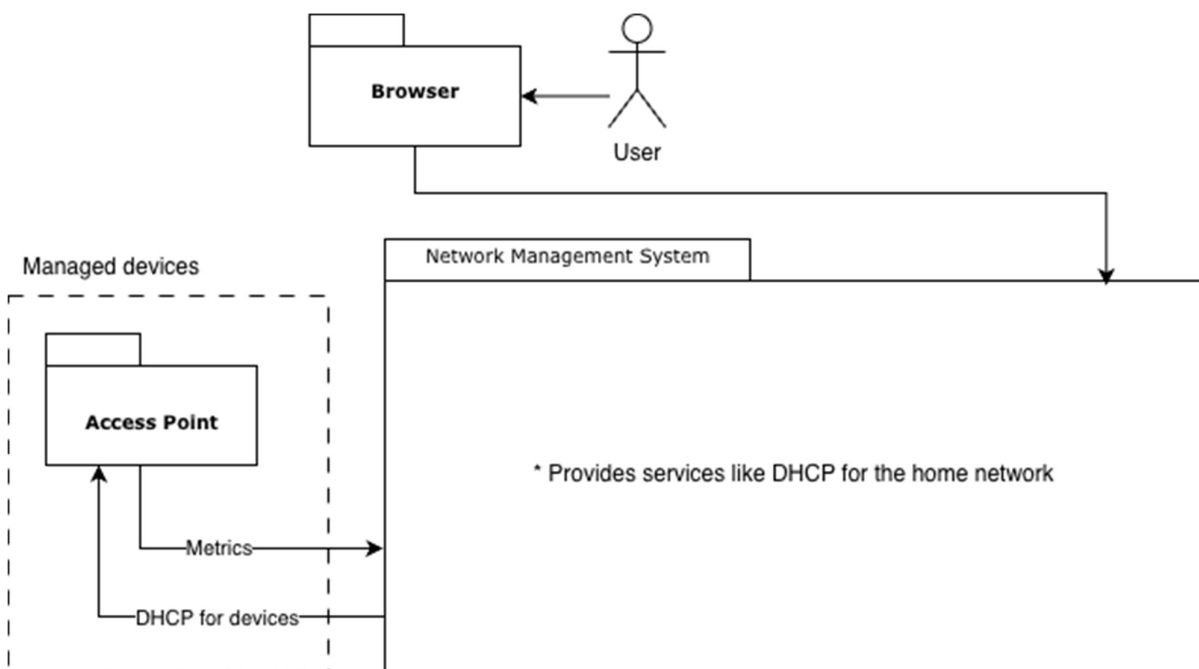


Figure 4.4.1.2-1: Home network deployment

In this use case, the network management system controls the user's home network of devices and often acts as a gateway or an access point providing connectivity for the user's home to outside networks, usually public. Access points are devices such as a router, switch, modem, or other wireless or wired device controlled and governed by the NMS and physically deployed to the service requesting users home.

The device can also make the upstream connection technology transparent to the user. Depending on the available infrastructure in the deployment location, connectivity can be through a variety of alternatives, including a mobile network or fiber optics network.

The NMS in this use case is most often locally installed on the device but may be running on a different device within the same network, or as a remote service, a RDPS.

The devices can actively send metrics to the NMS and can serve multiple devices in the same network. The devices can also provide supporting services like DHCP and DNS caching, but beyond such a minimum they can offer more extensive services such as remote connectivity options like VPN server depending on the product.

Meterics from the devices and other elements within the home network can be forwarded to the NMS, where the user can percieve these meterics and control the configuration of each networked device. In many deployments actual configuration control and review of metrics collected by ther NMS is achieved with an additional service or alternate piece of software, most often a browser, but sometimes is other ways, such as through a command-line interface.

4.4.2 Multi-user deployment

- The network connects to a broad variety and large number of devices, including single user devices and a number of distant or local other networks themselves connected to other user devices.
- Users and connected networks are usually distant and outside controlled operational environments.
- Deployment has a high number of elements.
- User base is of significant size, and the number of users and network functions affected by compromise of failure of the NMS is potentially high.

4.4.2.1 Enterprise network

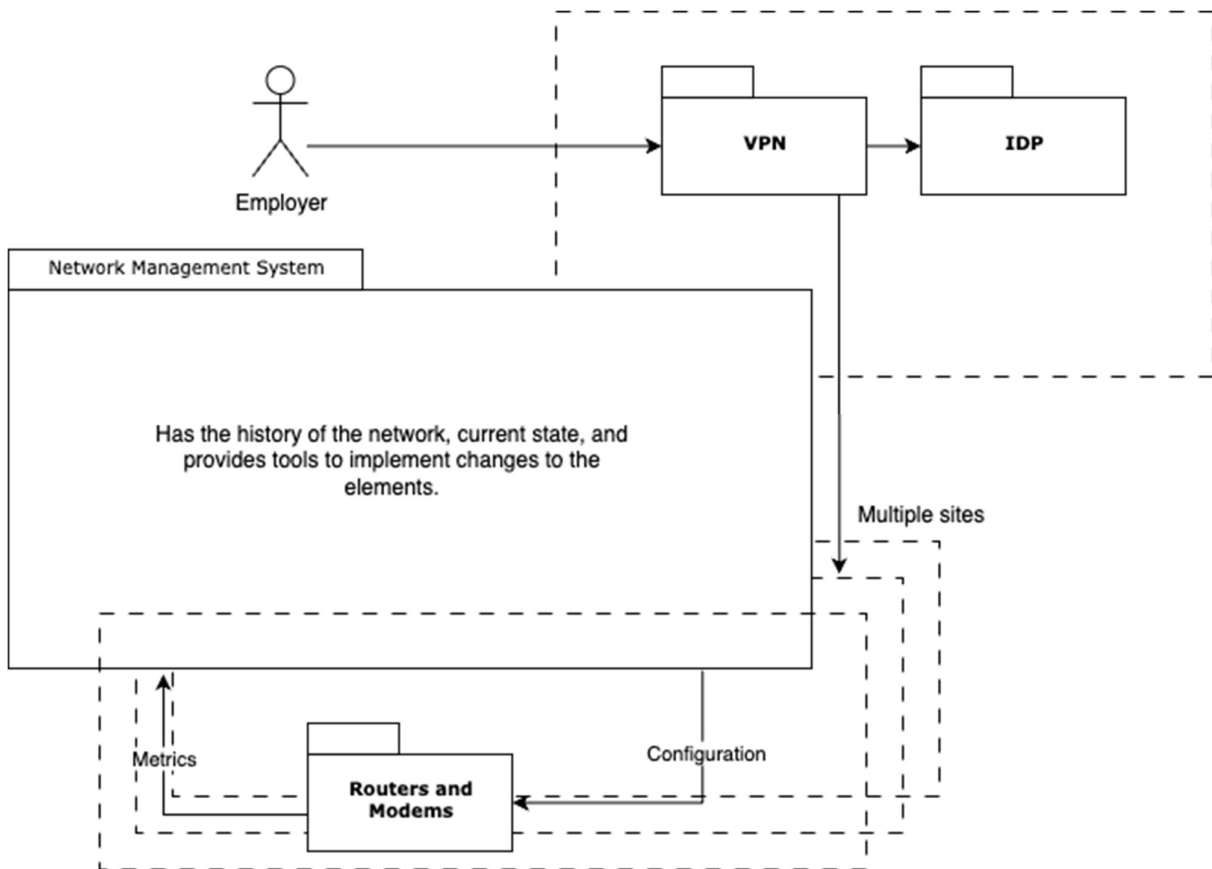


Figure 4.4.2.1-1: Enterprise network

A typical enterprise or office network has multiple service requesting users connecting simultaneously to a shared infrastructure.

Infrastructure may include multiple sites connected through a variety of technologies, including but not limited to: public networks, dedicated routing infrastructure like IP-MPLS-tunnel, massive-scale computing and storage systems via data center (cloud systems), or third party service providers, or 5G slicing. An office network also typically operates for long periods, developing layered history of past versions and functions.

With modern remote working expectations, enterprise networks almost always include remote connectivity options, such as VPNs, that enable remote users to connect to the office network and work with the subset of curated services through a shared intranet environment.

User identity verification, authorization, and the maintenance of a user is needed for each such intranet service or environment. This identity pool can be local for the service, shared within the same intranet, or provided as a service outside of the network context. In office environments, larger identity pools provide redundancy, but also complicate the administration of credentials, and reduce response time when credentials are rotated, such as when they are leaked and misused.

While it is possible to maintain the identities of all of available intranet services by hand, this is often impractical even with a moderate pool of users. A contemporary enterprise NMS deployment will instead rely on an Identity Provider (IdP) for most or all of its services. IdP's may be part of an NMS or separate, decoupled from the NMS. Likewise IdP's can be implemented locally or as a remote service, including as an RDPS. In all varieties the nature of the IdP deployed to the network is relevant to this document as it is a major risk factor, especially if the NMS product does not support a relevant integration methods or IdP technique.

As the importance of the operational context rises, so does the level of accuracy needed to securely manage identity. A larger enterprise has more staff, roles, job, and responsibility rotation, required services, data classes, levels of classified information, and working sites.

The increase in size and complexity contribute to increasing multiple risks that requires more elaborate management structures. While many small businesses can perform the credential cleanup on former employees by hand, a large enterprise is likely to find this difficult, and see the value of deploying an administrator credential management service.

Additionally, entities within this context may store and work with extremely personal and sensitive data, such as a medical facility's patient records or a bank that needs to secure financial data. The type of deployment and actions of the service requesting users are not important to the NMS, except to the degree that the NMS must ensure that the system has the features, hardware, and security to match operational needs.

4.4.2.2 Telecom network

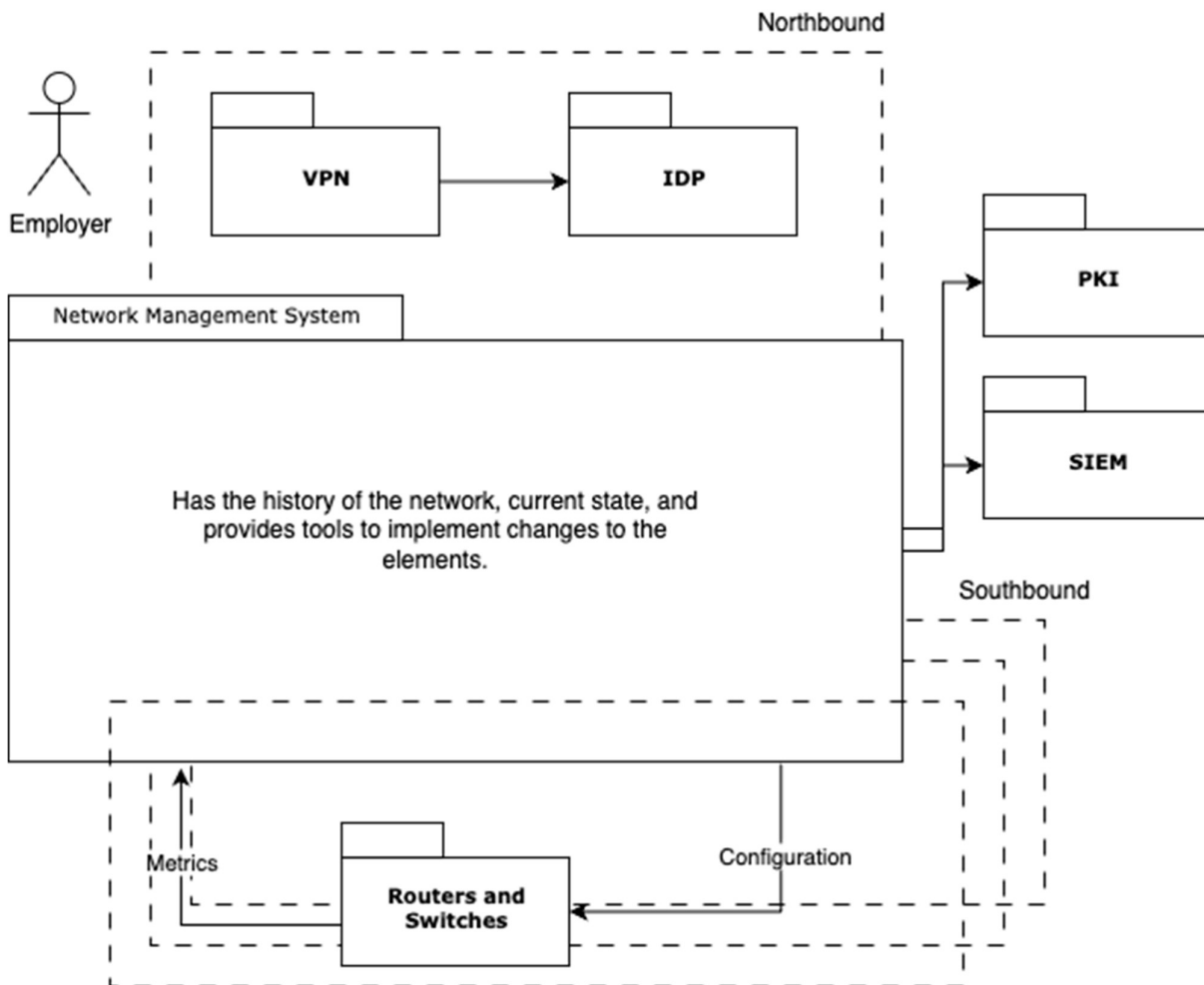


Figure 4.4.2.2-1: Telecom network

A telecom network resembles an enterprise network, with the obvious added complexity throughout. The telecom NMS will handle a greater load, including more users, devices, and identities. Identity providers (IdPs) are often used to create segmentation and redundancy, and network uses its routers and switches as base stations serving thousands of users simultaneously.

Telecom networks are modelled by division into northbound and southbound abstraction levels or descriptors, where southbound describes traffic from the NMS and hardware controlled by the network. Northbound traffic comes from lower layers of the network such as routers and switches and from the applications and users. Services supporting and the telecom network, both internal and third party, are described as being eastbound or westbound, depending on the objectives of the modelled architecture. In the above figure, SIEM is an example service that is adjacent to the NMS, and is often used in modern deployments.

In telecom deployments of NMS it is common to provide an in-house Public Key Infrastructure (PKI), that declares its own certificate authority (CA) or authorities deployed to the managed machines within the network. The number of these managed machines, number of CA's, and how the CA's are used is dependent on design of the network. Alternatively, even at telecom scale, and NMS can even provide its own certificates and form an independent and segregated trust domain.

4.4.3 Alternative deployments

As the use of extremely large scale network services, or hyperscalers, becomes increasingly popular and the networked services perform an ever greater number of software functions, how we understand network structures depends on how we model their connectivity. The following two use cases in sub chapters consider such deployment and other complex

deployments primarily by focusing two approaches. These complex networks can be modeled by how the functions are virtualised in the network [4.4.3.1 Logical network deployment](#) or examining how much RDPS is involved in the design [4.4.3.2 Physical network deployment with RDPS](#).

Yet, the protocols used for all network deployments remain consistent. TCP and UDP dominate the network and transport layers in the OSI-model. DNS root servers are still trusted to point to the desired IP address and browser maintained TLS CA pools builds trust beyond that provided by the DNS.

Encryption can be applied to the transport layer, but is rarely seen as it imposes increased computational requirements, higher cost, and more complex management. Even with the emerging private networks popularised by the 5G slicing features, the transport layer rarely is fully encrypted throughout a private intranet. Only in networks that need greater integrity assurance, does the network need to be responsible for encrypting its own traffic.

4.4.3.1 Logical network deployment

Early versions of Software Defined Networking (SDN) imitated the physical network structure by replacing the real-world devices with digital counterparts. Such SDNs needed an IP subnetwork definition to provide IP addresses with a DHCP from a switch.

The Virtual Machines uses Virtual Ethernet interface (veth) to transfer information in the same way that other networks would with a physical card. The veth is connected to virtual switch, that handles ARP protocol duties, and relies the DHCP queries to the control layer.

The subnet virtual switch is connected to a virtual router acting as a gateway, enabling the virtual machine to communicate with rest of the connected infrastructure. All of these virtual devices can be independent instances of virtual machines running OS with a linux kernel.

The virtual imitation of real world devices copies over the same design flaws that we have had for years. Only after a few iterations of cluster based application development in scale, the network requirements have started to evolve.

The paradigm shift happens, when the application design takes more responsibility from the High-Availability and the application is already expecting faults to happen. In a fluid, often container based, environment where computational nodes can be dropped unannounced, the application execution context vanishes without warning. It is often expected, when cluster changes are made, the application can resume it's task only with minimal overhead and loss of progress whe it is relaunched elsewhere. This elsewhere can be a new node added into the pool, or the old one when it rejoines the cluster after a forced reboot. When the application changes, the network changes with it, thanks to the flexibility of SDN.

The latest network control structures are utilising low level kernel features. While the Berkeley Packet Filter has been the stable base for linux Netfilter stack, the extended version of it(eBPF) moves the computational decision making to the kernel.

While the previous OS user level tools are now rendered useless, and the packet routing decision is done before the packet is introduced to the host OS, the eBPF implementations are often built for the cluster use. Decision, what was previously segregated to different OSI-model layers, is now solved in a single process. Combining eBPF and cluster application knowledge and control, the cluster becomes the NMS.

The application describes it's needs as how much distribution it requires, what parts of the different processes can be in the same or different computational context, and even how much capacity it expects from the backend. The eBPF can provide answer to all of the requests by partially resolving the Session layer and fully implementing the control of Transport-, Network-, Data link- and Physical-layers.

In highly interconnected cluster, where multiple sites are used to host the workloads, this means, that the virtual or physical port definition is made available only in the machine where the corresponding workload is located to. In an optimal case, there is no need for additional firewall configuration, as the node does not simply accept traffic in for the services it is not hosting. In reality, multiple layers of firewalling is still used to limit accidental configurations exposing services undesireably.

In theory, the database can be in Portugal, when the business logic is driven in Singaporean datacenter. These two services are often placed into a single namespace, that often translates directly to a IP subnet that stays fixed within the cluster. This subnet is used in the application internal routing and communication, and does not necessarily mind where it is implemented. The namespace and IP subnet follows seamlessly to the new datacenter location, if the application failover tolerates it and the cluster design makes it possible.

This highly abstract and fluid control scheme can host emergency services critical information, nations polling results or a non-profit organisations read-only website. Only the implementing entities risk appetite sets the upper limit on what this structure can be used for.

4.4.3.2 Physical network deployment with RDPS

When almost everything can be software, the minimum sill remains: the user needs to have some form of User Equipment to be able to connect. This Network Interface can be a radio in the cellphone, a WiFi Access Point in the living room, or router with SFP+ ports serving the local datacenter. How much the network structure has autonomy on control and local network routing the device has can be modeled in function of how much RDPS is involved in the design.

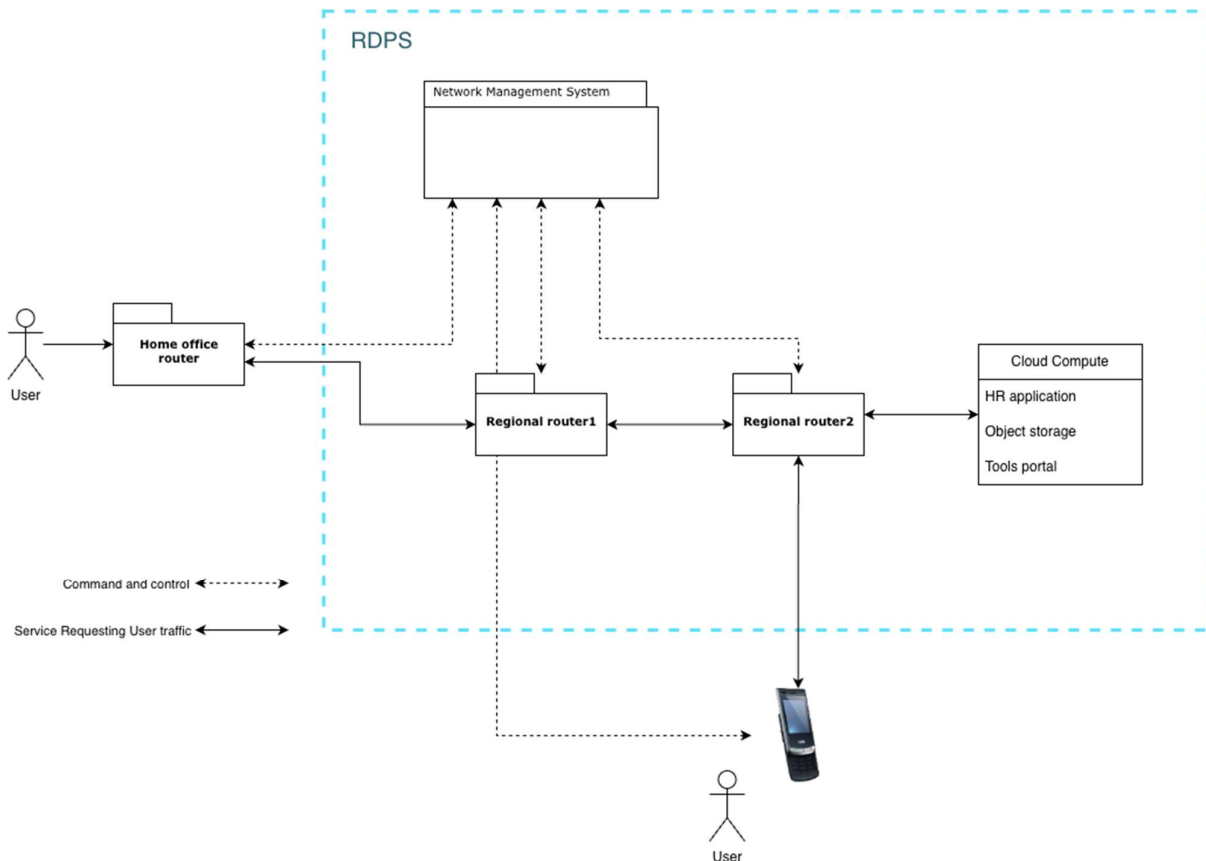


Figure 4.4.3.2-1: Maximum RDPS involvement

In figure the maximum RDPS involvement, the network design follows the hot potato design rule. The connection is handed over for RDPS as soon as possible. The local network is used as little as possible, and even the home office routing can take a detour through RDPS in order to provide auditable trail of how the remote working employee is using the network.

With technologies like 5G slicing, the closest point of return in respect to re-routing back to your network could be the nearest basestation or it could be the squid proxy in other side of the world. These two scenarios results to different user experience where the latter would most likely show as slow and unresponsive service, but both are valid designs that can be deployed.

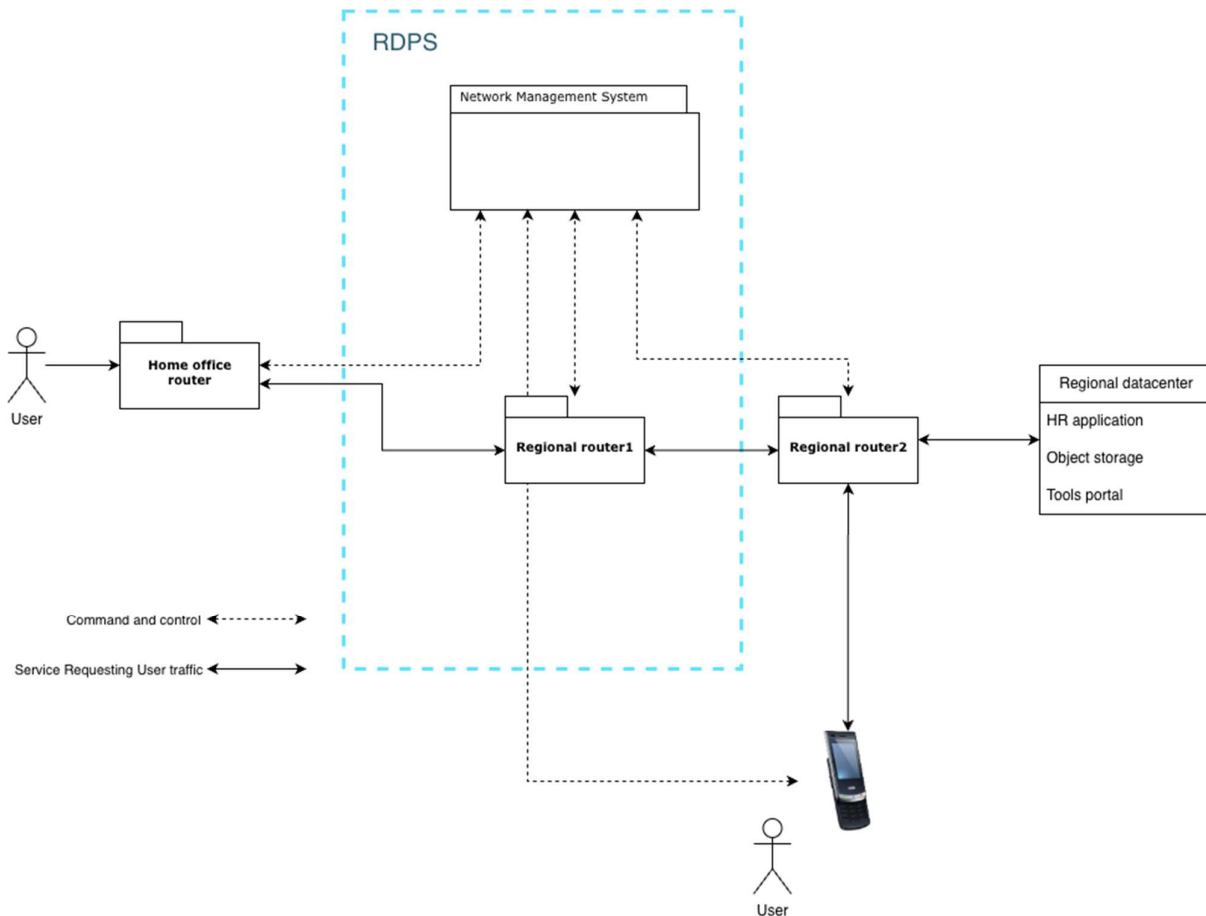


Figure 4.4.3.2-2: Medium RDPS involvement

Medium RDPS involvement is a common hybrid setup, where the company already has older assets, that are grown into the enterprise, and are kept around as there is little or no need to change the infrastructure. Part of the network design is created with virtual assets, that could be the new IT infrastructure for the latest acquired company, while the still significant portion of networking assets are tied to the headquarters datacenter.

Control structures are different, device management strategies are varying, and even the physicality can extend to multiple nations. The balance of owned assets and bought services is often selected due to ease of deployment, while the partial reliance on headquarters datacenter offers resilience towards major outages in the connectivity. End result might not be optimal, but often acceptable in the eyes of company risk management.

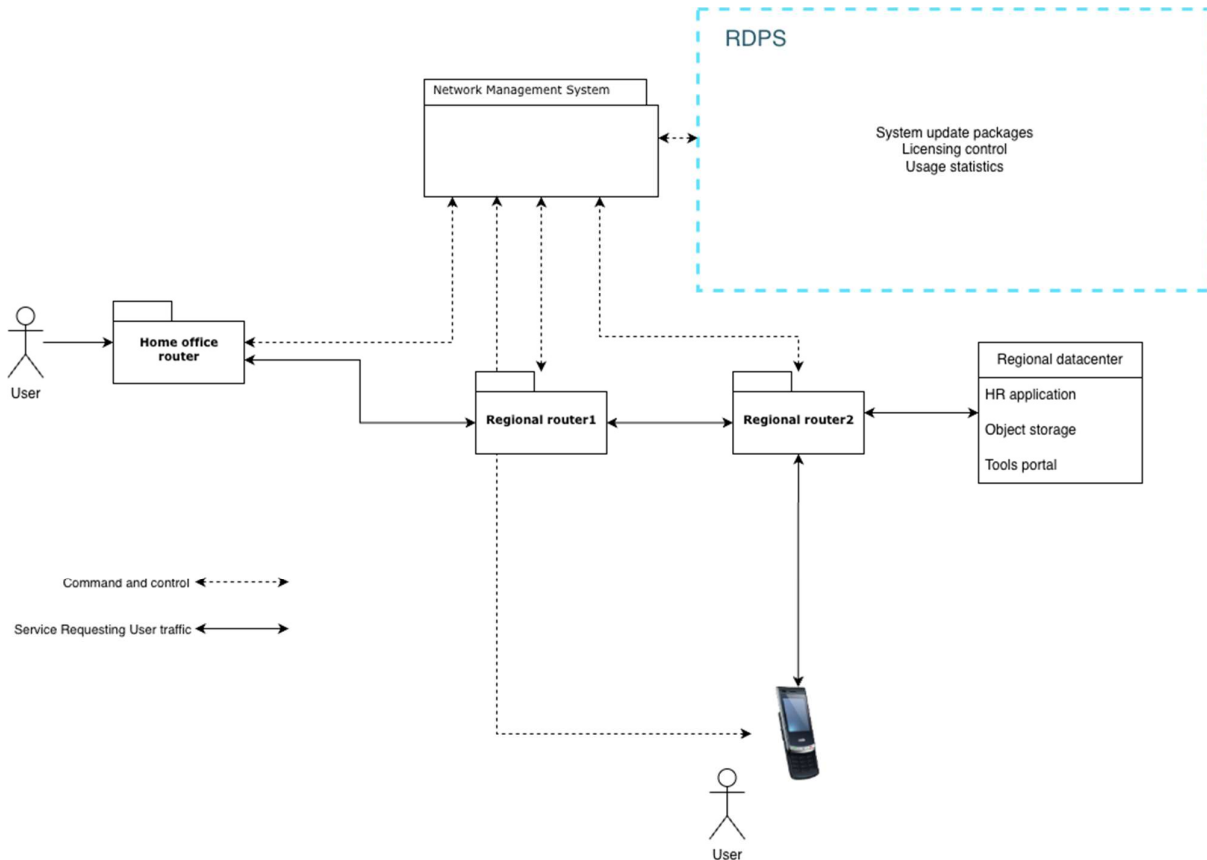


Figure 4.4.3.2-3: Minimal RDPS involvement

In a minimal RDPS involvement, all of the relevant infrastructure is not fulfilling the RDPS definition, and can be deployed to an underground infrastructure spanning multiple locations for example. Interconnection between the sites is either owned, or leased from a provider.

Some links can be through dedicated IP/MPLS tunnels, while some could be implemented through public connectivity with VPN tunnels. The RDPS mainly serves only update packages to the NMS, validates licensing if needed and can collect usage statistics for product development purposes.

While system updates are critical for the product, the installation is fully independent and no functionality is relying on the RDPS connectivity. The system updates can be delivered with a removable medium, if no connectivity to software repositories is available.

4.5 Risk Factors

To address the risks of an NMS product prior a manufacturer's placing it on the market this standard encourages the manufacturer to threat model and risk profile of the use of the product, including its foreseeable uses, and considering the interplay between:

- The complexity of foreseeable uses
- The likelihood of incidents, given the foreseeable uses
- The impact of incidents, given the foreseeable uses

The security profile requirements in clause X reflect use cases and intended deployment of the NMS. Security profiles are based on overall risk of the product, a combination of likelihood and potential impact of incidents. Individual risks are judged using the risk factors described here in Annex D, and determine the degree and type of security needed for specific related security requirements.

Risk factor analysis of all appropriate risk factors can be combined to determine an overall risk of the product and label its risk as low, medium, or high. With this approach, each risk factor provides a description of high or low risk related to a particular aspect of the product and when combined a way to judge its overall security needs.

Each risk factor uses a three tier, low-medium-high risk structure. A set of risk factors is used to determine what requirements apply to the product in the later section [5 Requirements specifications](#).

Table 4.5-1: Determining risk level

Likelihood / impact	Low	High
Low	Low	Medium
High	Medium	High

4.5.1 List of Risk Factors

The risk factors identified by the risk assessment in Annex C are grouped into risk categories and assigned unique identifiers below.

4.5.1.1 Service requesting users

Number of affected Service Requesting Users [SRU]

Key: [SRU](#)

Rationale: Affected user base are a factor when determining risk.

[SRU](#)

risk **likelihood** is **low**, where:

- The NMS's managed network has well defined traffic.
- The NMS's managed network has only a small variety of traffic classes, for example: IoT network data collection and software updates.
- The NMS's managed network's SRUs are limited to other devices with well-known communication needs.

[SRU](#)

risk **likelihood** is **high**, if:

- The NMS's managed network network has arbitrary and poorly defined traffic.
- The NMS's managed network serves human users, each with multiple varied devices such as laptops and mobile phones.

[SRU](#)

risk **impact** is **low**, if:

- The NMS's managed network serves single household or a small business, small amount of SRUs.

[SRU](#)

risk **impact** is **high**, if:

- The NMS's managed network is a larger enterprise network with multiple sites connected to the same internal network structure.
- The NMS's managed network is a public telecommunication network provider, Internet service provider, or other network with a large amount of SRUs.

4.5.1.2 Complexity of managed network element implementation

Key: [Complexity](#)

Rationale: The complexity and number of devices, functions, and sites managed or performed by the NMS are a factor when determining risk.

Complexity

risk **likelihood** is **low**, if:

- The NMS has minimal features
- The NMS receives data only from simple devices, like a network of IoT devices that send basic availability metrics to the NMS
- The NMS also enables some simple features for basic networking functionalities like firewall, DHCP

Complexity

risk **likelihood** is **high**, if:

- NMS managed network is has exposed connectivity services like VPN and SDN.
- NMS provides a high number of network services.
- NMS managed network includes multiple interconnected sites

Complexity

risk **impact** is **low**, if:

- NMS managed devices have limited capabilities
- NMS uses idempotent design

Complexity

impact is **high**, if:

- NMS managed network performs dynamic routing table modifications
- NMS managed network is complex with sophisticated functions and supporting services
- NMS managed network includes multiple interconnected sites

4.5.1.3 Security expectations of the deployment context

Expectation is hard to describe as a sum of likelihood and impact. Therefore this risk factor is evaluated directly as perceived by the market the product is made available.

Key: [NIS2](#) **Rationale:** NIS2 identifies entities that require higher level of protection. The important and essential classifications are combined as the NIS2 doesn't make additional cybersecurity requirements based on classification. The additional mechanisms are often national level.

- The deployment context has other mechanisms that helps to identify and react to the security compromises

[NIS2](#) risk level is **low** if:

- NMS is intended for or foreseeably used to manage networks whose NIS2 status is undefined.
- NMS's intended deployment target is a household or a small business with under a thousand users.

[NIS2](#) risk level is **medium** if:

- NMS is intended for or foreseeably used to manage networks whose NIS2 status is undefined.
- The NMS product is intended or foreseeable used an audience of over a thousand users.
- The NMS managed network element is widely used and often used to store significant amounts of personal or financial data.

[NIS2](#) risk level is **high** if:

- - NMS is intended for or foreseeably used to manage networks whose NIS2 status is as important or essential entities

4.5.1.4 Deployment context network segmentation

Key: [Segment](#) **Rationale:** The level of segmentation and isolation of the NMS managed network are a factor when determining risk.

[Segment](#) **likelihood** is **low**, if:

- NMS managed network is physically isolated from public networks with strong physical access control procedures.

[Segment](#) **likelihood** is **high**, if:

- NMS managed network is connected with multiple entry points to public networks filtered by firewalls.
- NMS managed network uses no segmentation.

[Segment](#) **impact** is **low**, if:

- NMS managed network is segmented in a way that does not mix management traffic with payload data.
- NMS managed network uses single segment, but the number of connect devices in the network is low.

[Segment](#) **impact** is **high**, if:

- NMS managed network is segmented, and the segmentation is trusted to provide additional security.
- Traffic classes including control, management and payload shares the same segment on the NMS managed network.

4.5.2 Mapping of use cases to risk factors

The table below is an example, how the example use cases could be mapped to different risk factors.

Table 4.5.2-1: Example mapping of use cases

Use case	SR U	Complexity	NIS2	Segment
4.4.1.1 IoT network with monitoring data collection	low	low	TBD	high
4.4.1.2 Home network deployment	low	low	low	medium
4.4.2.1 Office network	TB D	high	TBD	TBD
4.4.2.2 Telecom network	high	high	high	TBD

The To Be Defined (TBD) represent manufacturer design choices and what market the product is intended to be used in. The product can be targeted to an audience, where the given risk factor evaluation is different. For example the [4.4.2.1 Office network](#) evaluation table could be expanded to all existing combinations of low, medium, and high, in the risk factors that has TBD in place. When the same product is provided to multiple different markets, highest risk factor shall be used.

4.6 Security Profile

In the present context a security profile is the identification and mapping of assets, threats, resulting risks, and mitigating objectives that are furthermore covered by security requirements. The mapping thereby ensures that all identified threats are repelled or mitigated.

All products with digital elements have a common set of requirements that shall be addressed regardless of the system design or of the intended market. These essential security requirements are defined in the CRA [i.1]. The present document tries also to identify risk factors that are not obvious in all scenarios.

4.7 Essential functions

Following list of essential functions keep the NMS self-secure and correct functioning during its operation in its intended environment.

- Network element configuration and change management
- The NMS will use the appropriate level of access control to maintain identity and actions each system actor can take
- Performance metrics assuring that the operation of the network is in the nominal levels
- Fault detection, reaction and recovery from fail state
- Functional resilience in terms of maintaining correct operation under abnormal network conditions, e.g., connection loss to managed elements.
- Functional resilience in case of
 1. loss of connectivity to connected managed elements totally or partially,
 2. to required network services for example time stamps and backup, and
 3. power off.
- Dynamic routing and switching control based on requests. Used extensively with Software Defined Networks.
- Device discovery, inventory building and depending on the use case topology map generation.
- Produce logs and traces for security and operational analysis

4.8 Operational Environment

The technical requirements of the present document apply under the environmental profile for operation of the product with digital elements, which shall be in accordance with its intended use. The product with digital elements shall comply with all the technical requirements of the present document at all times when operating within the boundary limits of the operational environmental profile defined by its intended use.

4.9 Users

Human users of the system are natural persons, trained and qualified as NMS administrators, and authorised to manage the NMS and the connected managed elements. Administrators typically access the system through a HTTPS GUI, console, or by VPN connection.

Machine users are servers or any other type of a computer that are identified and authenticated by communication protocols that protect the communication between the NMS and the machine user. Once the protected communication has been established, the machine user receives the according authorisation by the NMS.

Service Requesting Users do neither have a direct interface to, nor could they interact or login via other ways to the NMS. Nevertheless, SRUs rely on the correct functioning of the managed elements and therewith on the NMS.

4.10 Distribution of security functions

An NMS can be formed by a compilation or collaboration of different subsystems in a local distance but within the same management network and within the equal operational environment. The security functions may be implemented inside one or more of the subsystems that form the NMS. The NMS can thereby be operated by an OS package manager or other systems which also belong to the NMS and are in scope of the present standard.

The NMS documentation shall clarify whether a security requirement is

1. completed fulfilled by the NMS itself,
2. where it relies on support from external services and

3. to which extent it is dependent on an external service.

4.10.1 External security functions, not in scope of the present document

The following cybersecurity functionalities can be handled from components outside the product:

- From external provided updates on secured channels that the product uses to update the managed managed elements and also itself.
- **Identity management systems** that provide mechanisms for identification and authentication. The system can include also the lifecycle management for identity credentials [i.2]
- **Virtual Private Network** providing access to a physical or virtual established network of managed devices that have strictly controlled access to authorised functions of the product. [i.3] [i.4]
- **Provision of cryptographic keys** Public key infrastructure or other key management system for services of key generation, provision, establishment, and for certificate services such as generation, signing, verification, validation or withdrawal. [i.6]
- **Security information and event management systems** that collect data from multiple sources, analyse and correlate that data and present it as actionable information for security-related purposes unless it is considered to be integral part of the product features [i.7]
- **Physical and virtual network interfaces**
- **Operating systems** Operating systems that act as abstraction layer for the hardware system(s) that host the product and are else not involved in the internal functioning. [i.5]
- **Managed devices** Managed devices, including those that are managed by the product, such as routers, modems and switches. [i.8]
- **Antivirus**

Furthermore, it is essential to detail the generation and establishment of the trust relations between the NMS and the essential external services and systems.

4.10.2 Security functions provided to other products

The NMS shall provide the reliable availability of the operative network, while keeping control and providing traffic meta data and metrics for the administrator for verification of the correct network operation. Example: A listed managed element in the NMS can be enriched with traffic meta data. For example, and inconclusive, when and with what performance there was relevant traffic throughput, when/from/to there was a managed element managed traffic overload, received failure reporting or similar.

5 Requirements specifications

5.1 General

The following non-technical requirements shall be implemented by all products with digital elements evaluated with the present document.

- **[REQ-GEN-0]:** The product shall have technical documentation with what [Risk factors](#) the product shall be evaluated.
- **[REQ-GEN-1]:** The product shall have technical documentation a detailed enough systems architecture design description, that enables national bodies like MSA to evaluate and test the product design.
- **[REQ-GEN-2]:** The product dependencies to Operating System essential security capabilities are documented.
- **[REQ-GEN-3]:** The manufacturers technical documentation shall describe the external services and systems that are required for the product operation like mentioned in [4.10.1 External security functions, not in scope of the present document](#).

System operation is always an interplay of multiple components. Modern software design can rarely ignore impact of the changes to other components.

5.1.1 No known exploited vulnerabilities

If the deliverable contains or requires an operating system the operating system is expected to be regularly updated and maintained. Depending on the chosen delivery method, the maintenance of the operating system can be provided by the customer of the product. Note that a container has always an operating system.

If automateable and freely-usable vulnerability scanners are available the product shall satisfy the following with respect to the most comprehensive of such scanners.

- **[REQ-EXPLOIT-0a]** The product shall have no vulnerabilities discovered by scans.
- **[REQ-EXPLOIT-0b]** The product shall have only discoverable vulnerabilities whose age is consistent with the manufacturer's documentation of how long vulnerabilities may go unfixed after public disclosure.
- **[REQ-EXPLOIT-0c]** For each detected vulnerability, the product shall have publicly available documentation explaining how the risk has been mitigated.

Recognising that there may be vulnerabilities discovered between the time that a product is placed on the market and the time of that product's first use, and that the product should be free from known vulnerabilities both when first made available and when first used by a consumer, the manufacturer shall ensure that the product can be updated at the time of first use to address all known exploited vulnerabilities which were discovered after the product's placement on the market and before that first use.

- **[REQ-EXPLOIT-1a]** The product shall be accompanied by documentation describing how the product may be securely updated,
- **[REQ-EXPLOIT-1b]** including how to update the product prior to, or as part of, first use.
- **[REQ-EXPLOIT-2]** The product shall have OS and Application upgrade instructions which makes it possible to obtain the set High Availability targets.

More about [High Availability](#) in its dedicated chapter.

5.1.2 Secure design, development and production

This document will make normative reference to prEN 40000-1-2 "Principles for cyber resilience" [i.15], when available.

5.1.3 Product vulnerability management process

This document normatively references EN 40000-1-3 "Vulnerability Handling"[2] and doesn't currently add to the specified definitions.

5.2 Technical cybersecurity requirements specifications

This section contains technical cybersecurity requirements for the product. Each general technical requirement is objectively verifiable on an instance of a product. Each requirement has at least one concrete example that satisfies the requirements of the CRA. Later [Section 5.3 Risk Mitigations](#) combines these general requirements to [Section 4.5 Risk Factors](#). The Risk Mitigations can include additional topic specific requirements.

When evaluating the applicability of these requirements, the highest of following risk factors define the category to follow: [SRU](#), [Segment](#), [NIS2](#)

For low risk:

- **[REQ-TECH-0]** The product shall be shipped without undocumented interfaces.
- **[REQ-TECH-1]** The product shall implement [5.2.4 State-of-the-art cryptographic libraries](#) to allow the protection of the requirements of the foreseeable use.

- [REQ-TECH-2] When privileged information is transferred or accessed, a secure channel shall be used in transport [5.2.1 Secure channel](#).
- [REQ-TECH-3] All endpoints in a secure channel shall cryptographically verify others.

For medium risk:

- [REQ-TECH-4] The product shall be designed in a way that [5.2.2 Cryptographic key intialisation and rotation](#) is made possilbe.
- [REQ-TECH-5] All system components shall be synchronised to the same time.

For high risk:

- [REQ-TECH-6] All system clock drifts shall be monitored.
- [REQ-TECH-7] The product shall be designed in a way, that all cryptographic keys can be replaced with user controlled keys.

The listed requirement shall be implemented, if the risk of the given factor is defined as follows. When multiple factors define a different level, the lowest level shall be selected. A product which risk factor is evaluated to be medium, shall implement both low and medium requirements. A product which risk factor is evaluated to be high, shall implement all mapped requirements.

5.2.1 Secure channel

A **secure channel** referred in [REQ-TECH-2] and used in transportation is a cryptographically protected communication channel, that may be implemented with TLS. When TLS is used, manufacturer shall ensure that the channel uses appropriate cryptographic functions and configuration according to the requirements of the foreseeable use. Manufacturer shall ensure that the channel can not be impaired by downgrading it [i.10].

When TLS is not used to encrypt the traffic in the secure channel, manufacturer shall provide detailed description how the channel is secured in the technical documentation. The chosen method shall follow the intent in the CRA by protecting the data transfer, and protect the confidentiality and integrity of the data according to the requirements of the foreseeable use.

Mutual trust is in plural form not excluding IP Multicast or Anycast usage if implemented.



Figure 5.2.1-1: Secure channel example with TLS

The figure above is an illustration of a simple TLS protected communication between NMS and the managed device. The device initiates the connection towards reachable endpoint based on a DNS address configured into the managed device. The device validates the provided public certificate and logs in with machine credentials. NMS authorises the query based on the role and identity of the device.

5.2.2 Cryptographic key intialisation and rotation

Manufacturer shall design and implement support for on-demand rotation of cryptographic keys. The technical documentation shall include:

1. instructions on how to intialise trust
2. how to use the trust to accept managed elements to the network
3. how to the established trust to rotate all keys

5.2.3 Network segmentation

Network segmentation is encouraged to be used where applicable. The best practise is to use dedicated network segment for network management traffic. Management traffic can be configuration updates, encryption keys, software updates, and others alike.

ZeroTrust routing is also encouraged where applicable.

Editor's note: TODO: this should need to be coupled with Operative environment chapter

5.2.4 State-of-the-art cryptographic libraries

Cryptographic libraries, primitives and constructions shall follow ENISA's Agreed Cryptographic Mechanisms[1]. Manufacturer shall enable by default only the recommended designs that are fit for use-case. Any designs that are not fit for use-case may only be enabled after the user has been sufficiently informed of the security consequences in a manner that takes the use-case into account.

As an example, when using TLS to protect the transport, only TLS v1.3 shall be used with one of the three cipher suites: TLS_AES_256_GCM_SHA384, TLS_AES_128_GCM_SHA256 or TLS_AES_128_CCM_SHA256.

For backwards compatibility, use of other combinations of options other what is recommended[1] shall be implemented with the following details listed in the technical documentation:

- What component requires lesser cryptographical implementation
- Statement about why the backwards compatibility is in place
- Transition plan towards recommended cryptographical implementation
- Transition timeline

5.2.5 Software Bill of Materials

These requirements are generally binding, and there is no low-medium-high tiering available.

- **[REQ-SBOM-0]:** Operating system dependencies and application dependencies shall be clearly separated in the provided SBOM.
- **[REQ-SBOM-1a]:** Unique, unambiguous, and machine-readable identification of all components and dependencies shall be provided in the SBOM.
- **[REQ-SBOM-1b]:** The SBOM identifier format shall be consistent with common vulnerability handling standards.
- **[REQ-SBOM-2]:** The SBOM shall be consistent with [5.3.4 Secure updates](#) practices.

5.2.6 Role based authorisation

The identity management is an essential piece in the larger puzzle of cybersecurity. A secure product is required to confirm the identity and authority of all users performing an action. If the system fails to identify such actions and authority, or fails to track who executed commands, the system can easily fall into a state of chaos.

An identity management system provides for the authentication of each user. It provides the assurance of that an entity has authorization and has provided the correct information to the product to perform a specific action.[i.12] Only a well maintained trusted source list can provide functional authentication. If the source authentication is a company internal directory, the content needs to be up to date and reflect the status of persons granted current access.

These requirements apply to all network management systems, regardless of the product's use case and without variation for different tiers or risk.

- **[REQ-AUTH-0]:** The product shall be integrated into a state of the art identity management system.
- **[REQ-AUTH-1]:** 2-factor authentication shall be used to confirm the identity of a natural user.
- **[REQ-AUTH-2]:** Authorisation validity for authenticated natural users shall be no longer than a two days.

When the identity of a user is established, the system grants the user access rights based on the users' role. The system can have multiple distinct roles, each are tailored to the users' perceived needs. There are many possible roles, with examples such as: monitoring data reader, interconnectivity administrator, or administrator. If the product's deployment context calls for an all-powerful superuser, this can be accomplished either with a single role with numerous responsibilities or by aggregating many available roles to that single user. In many systems identity information includes a group assignment matched to a role inside the system.

Role Based Access Control design and depth is outside of the scope of this standard, but the product must use some form of RBAC. Both natural users, machine users, or equivalent structures need roles, despite often performing differently. Machine users can often have more exact limits on what functions they require. [i.13]

The product can serve traffic that is not meant to be identified. For example, an in-home router often trusts that the physical access to its port is enough to identify the subscriber line. In addition, the managed device can have a configuration port, management API, firmware update channel, or debugging access, which are classified as privileged.

- **[REQ-AUTH-3]:** RBAC design shall follow the best practices of the deployment context.
- **[REQ-AUTH-4]:** The RBAC design and application in the product shall be documented.
- **[REQ-AUTH-5]:** All privileged interfaces shall implement RBAC.
- **[REQ-AUTH-6]:** All access to administrative interfaces, control functions, and sensitive operations shall be subject to strong authentication of users, services, or integrated components.
- **[REQ-AUTH-7]:** Privileged interfaces shall be protected with [5.2.4 State-of-the-art cryptographic libraries](#).

TODO: define usage of machine credentials better, consider the cli over ssh controlled scenario

TODO: evaluate if a large enterprise needs to have 3rd. party IdP as an integrateable option

5.2.7 Remote Data Processing Systems

AMS: August and Daniel are working on this. Skip for now.

5.3 Risk Mitigations

The following sections describe how technical cybersecurity requirement in previous [Section 5.2](#) are mapped to the risk factors in [Section 4.5 Risk Factors](#). This section can include topic specific requirements.

5.3.1 Mitigations for user identity integrity

See [5.2.6 Role based authorisation](#)

5.3.2 Mitigations for ingested data integrity and confidentiality

When evaluating the applicability of these requirements, the highest of following risk factors define the category to follow: [SRU](#), [Complexity](#), [Segment](#), [NIS2](#)

For medium risk:

- **[REQ-INGEST-0]** The manufacturer shall protect the system against data poisoning or other adversarial attacks.
- **[REQ-INGEST-1]** The collected network element monitoring data shall be verifiable.

Every time a data is transported through an undefined connection, manufacturer shall take great care, that integrity and confidentiality of the data is not compromised.

Confidentiality can be achieved different ways in different scenarios. Reflecting to [List of Risk Factors](#) defined in this document, the following requirements shall be implemented.

Note that in a closed system, where the confidentiality doesn't require transport encryption, the data integrity does require at least signing of the data set with cryptographically good enough keying.

5.3.3 Mitigations for managed device configuration integrity and confidentiality

Push style configuration updates:

- **[REQ-CONF-0]** NMS signs the configuration in a way that managed device can verify the integrity of the content.
- **[REQ-CONF-1]** NMS sends the configuration only through [5.2.1 Secure channel](#).

Pull style configuration updates:

- **[REQ-CONF-2]** Connectible configuration update API enables managed device to verify the NMS authenticity.
- **[REQ-CONF-3]** Managed device credentials are valid.
- **[REQ-CONF-4]** Device role, place in the topology and function matches the requested configuration.

5.3.4 Secure updates

The update of a system has to be done often enough to keep the number of known vulnerabilities in minimum. A wide variety of threats related to secure update may appear both prior to an update and during the update process and the product shall mitigate both of these types of threat.

Pre-update acquisition & distribution secure update threats:

- Tampered update packages during storage or transmission
- Update retrieved from an untrusted or unauthenticated source
- Use of revoked or compromised signing keys

Threats to secure update during installation & execution:

- Authenticity or integrity verification bypass
- Downgrade to a vulnerable version
- Rollback protections bypass
- Loss of availability if update fails or is interrupted

Therefore, it is important to test all system upgrades and design the upgrade procedure in a way, that keeps the system within the set [5.3.8 High Availability](#) targets.

Requirements:

- **[REQ-UPDATES-0]:** The product shall verify the authenticity and integrity of update packages using a cryptographic digital signature verification prior to installation.
- **[REQ-UPDATES-1]:** The product shall maintain a monotonic version counter or equivalent mechanism to prevent installation of updates with an older vulnerable version.
- **[REQ-UPDATES-2]:** If the product supports intentional rollback, this action shall require explicit authorisation and shall be based on separately versioned and signed rollback metadata.
- **[REQ-UPDATES-3]:** The product shall apply updates in an atomic manner such that incomplete or failed updates do not result in a partially updated state. In the event that an update cannot be completed successfully, the product shall automatically restore a previously operational software state, ensuring the product remains functional.

These requirements are generally binding, and there is no low-medium-high tiering available.

Editor's Note: Consider making [REQ-UPDATES-3] applicable only for high tier.

5.3.5 Logging

The monitoring requirements becomes more demanding, when the security expectation of the deployment context is more strict. When evaluating the applicability of these requirements, the highest of following risk factors define the category to follow: [NIS2](#)

For low risk:

- **[REQ-LOG-0a]:** The log file of events shall be protected from unauthorised access, modification,
- **[REQ-LOG-0b]:** and is confidentiality protected.
- **[REQ-LOG-1a]:** The product shall generate auditable events for: successful and failed authentication attempts,
- **[REQ-LOG-1b]:** session establishment attempts with source details,
- **[REQ-LOG-1c]:** session termination events with reason,
- **[REQ-LOG-1d]:** session validation checks like number of concurrent sessions,
- **[REQ-LOG-1e]:** and privilege escalation.
- **[REQ-LOG-2a]:** The product shall log boot or initialisation events: timestamped boot stage progression,
- **[REQ-LOG-2b]:** component verification and initialisation actions,
- **[REQ-LOG-2c]:** and recovery mode activations if in use.
- **[REQ-LOG-3a]:** The product shall log: update availability,
- **[REQ-LOG-3b]:** start and finish of the update download,
- **[REQ-LOG-3c]:** events described by [5.3.4 Secure updates](#),
- **[REQ-LOG-3d]:** and installation successes and failures.

For medium risk:

- **[REQ-LOG-4]:** The log information shall have an active backup scheduled.
- **[REQ-LOG-5]:** Administrative actions like logs, traces and events shall be recorded into a write only service or endpoint.

For high risk:

- **[REQ-LOG-6]:** The write only log or tracing storage shall be deployed outside of the system deployment context.
- **[REQ-LOG-7]:** The system reports relevant administrative operations shall be forwarded to an external SIEM system.
- **[REQ-LOG-8]:** SIEM transfer format, field attributes and event descriptions shall made available as part of the technical documentation.

5.3.6 Metrics

Reasoning for metrics requirements is often justified by data integrity protection. Faults can not be detected, if an attacker can hide it's existense.

These requirements are generally binding, and there is no low-medium-high tiering available.

General requirements:

- **[REQ-METRICS-0]** The product shall be designed in a way that collected and stored metrics data can not be altered.

- [REQ-METRICS-1] Historical metrics data import overwriting an existing data point shall be noticed.
- [REQ-METRICS-2] Metrics name, purpose, and value interpretation shall be described for the user.
- [REQ-METRICS-3] Metrics cadence, accuracy and storage time shall be described for the user.

NOTE: [REQ-MON-1], [REQ-MON-2] and [REQ-MON-3] requirements apply to all collected metrics.

Availability and uptime requirements:

- [REQ-METRICS-4] Relevant system and connected element metrics like CPU, memory, disk utilisation shall be tracked and reported.
- [REQ-METRICS-5a] System process and service crashes and restarts shall be tracked and reported.
- [REQ-METRICS-5b] Managed element process and service crashes and restarts shall be tracked and reported.
- [REQ-METRICS-6] Managed elements and system nodes and provided services availabilities and statuses shall be tracked and reported.
- [REQ-METRICS-7a] Relevant system database and storage health metrics like queries per second, latency and throughput shall be tracked and reported.
- [REQ-METRICS-7b] Relevant managed element database and storage health metrics like queries per second, latency and throughput shall be tracked and reported.
- [REQ-METRICS-8] Relevant networking metrics like throughput and protocol errors shall be tracked and reported.

Application metrics requirements:

- [REQ-METRICS-9] GUI and API latencies and error rates shall be tracked and reported.

Matching tests for these requirements are listed in [6.3.6 Metrics tests](#).

[6.3.6 Metrics tests](#): #636-metrics-tests

5.3.7 Data minimisation

These requirements are generally binding, and there is no low-medium-high tiering available.

- [REQ-MINIMI-0] Metrics name, purpose, and value interpretation shall be described for the user.
- [REQ-MINIMI-1] Metrics cadence, accuracy and storage time shall be described for the user.

5.3.8 High Availability

High availability starts from the running process. In a modern cluster runtime environment used in large system deployments, the process rarely can control the loss of underlying resources. Administrative actions can shutdown the node without pre seeding announcement unexpectedly. It is up to the software design to tolerate these interruptions.

Modern design is often distributed, but depending on the implementation and runtime context, a singular process can also provide the targetted service availability if implemented correctly and self healing system can launch a replacement within the given time window.

When evaluating the applicability of these requirements, the highest of following risk factors define the category to follow: [SRU](#), [Complexity](#), [Segment](#), [NIS2](#)

For low risk:

- [REQ-HA-0] Expected availability shall be defined for each relevant system component.
- [REQ-HA-1] System updates and changes shall be included in the availability time definition.

For medium risk:

- [REQ-HA-2] System shall tolerate loss of resources within the limits of the defined availability.
- [REQ-HA-3] Recovery capabilities shall be made available in the technical documentation and are sufficient to implement the expected availability.

How to include protections against DDoS or similar?

6 Conformity assessments and tests

There are three different types of assessments used in this document.

Conceptual assessment, where documentation on the products assets and external capabilities and claimed mechanisms is compared with the applicability requirement's text. This style of assesment is kept in minimum.

Functional completeness assessment, where verification that the claimed mechanisms cover all interfaces and functions where the feature is required by the standard and the product's use case. Often the output is required to show proof of the implementation exactness.

Functional sufficiency assessment, where it is addressed in the assessment of appropriateness to evaluate whether the requirement implementation is adequate for their intended purpose. This is used with for example system architecture description, where using quantitative metrics would be unreasonable.

6.1 General requirements assessments

6.1.0.0 REQ-GEN-0

Requirement: The product shall have technical documentation with what [Risk factors](#) the product shall be evaluated.

Objective: Manufacturer declares the targeted market what is considered to be foreseeable use of the product.

Preparation: None

Activities:

1. Study the technical documentation.

Verdict:

1. Pass if all risk factors are included
2. and the reasoning why a given level was selected is presented.
3. Fail otherwise.

Supporting Evidence:

1. References to to documentation sections.

6.1.0.1 REQ-GEN-1

Requirement: The product shall have technical documentation a detailed enough systems architecture design description, that enables national bodies like MSA to evaluate and test the product design. **Objective:** MSA and other related parties can examine the product without installing it into a test or production environment.

Preparation: None

Activities:

1. Study the technical documentation.

Verdict:

1. Pass documentation has a detailed enough systems architecture design description.
2. Fail otherwise.

Supporting Evidence:

1. References to to documentation sections.

6.1.0.2 REQ-GEN-2

Requirement: The product dependencies to Operating System essential security capabilities are documented.

Objective: Dependencies to OS capabilities are documented and understood.

Preparation: None

Activities:

1. Study the technical documentation.

Verdict:

1. Pass if important and essential OS services and concepts are named
2. and their usage to run the application workload is clearly expressed as part of the architecture description.
3. Fail otherwise.

Supporting Evidence:

1. References to to documentation sections.

6.1.1 No known exploited vulnerabilities tests

6.1.1.0 REQ-EXPLOIT-0

Requirement a: The product shall have no vulnerabilities discovered by scans.

Requirement b: The product shall have only discoverable vulnerabilities whose age is consistent with the manufacturer's documentation of how long vulnerabilities may go unfixed after public disclosure.

Requirement c: For each detected vulnerability, the product shall have publicly available documentation explaining how the risk has been mitigated.

Objective: Disclosure of new vulnerabilities in the product and its dependencies are proactively monitored.

Preparation:

1. Select up to three vulnerability scanners meeting the requirements

Activities:

1. On a new product, carry out a secure update, run the selected scanners on the product, and examine the documentation for any reported vulnerabilities

Verdict:

1. Pass if manufacturer process to track new vulnerabilities is documented
2. and how existing vulnerabilities are tracked in the already released products is described.
3. and no vulnerabilities found, or all reported vulnerabilities satisfy either the age or documentation requirement.

4. Fail otherwise.

Supporting Evidence:

1. References to to documentation sections.
2. Documented vulnerability handling policy.
3. List of vulnerability scanners selected.
4. Reports from each scanner.
5. Correlation of reports of discovered vulnerabilities with documentation of mitigations.

6.1.1.1 REQ-EXPLOIT-1

Requirement a: The product shall be accompanied by documentation describing how the product may be securely updated,

Requirement b: including how to update the product prior to, or as part of, first use.

Objective: Prevent exploitation of known exploited vulnerabilities

Preparation:

1. Examine public or private vulnerability information sources and select a recently fixed vulnerability (preferably the most recently fixed).

Activities:

1. On a new product, carry out the initial secure update, scan the product to see if a recently fixed vulnerability has been fixed on the product, and examine the documentation for the required info.

Verdict:

1. Pass if the secure update completes successfully
2. and the most recently fixed vulnerability is fixed
3. and the documentation includes all the required information
4. and the instructions are noting the custom requirements of the application, if any.
5. Fail otherwise.

Supporting Evidence:

1. Documentation of vulnerability handling
2. Documentation of how to securely update the product
3. The report for the selected vulnerability
4. Description of how to scan for the vulnerability
5. Log of vulnerability scan results

6.1.1.2 REQ-EXPLOIT-2

Requirement: The product shall have OS and Application upgrade instructions which makes it possible to obtain the set High Availability targets.

Objective: Responsibility of OS level upgrades can be elsewhere outside of the system control.

Preparation: None

Activities:

1. Study the technical documentation.

Verdict:

1. Pass if cross referencing OS and Application upgrade instructions makes it possible to maintain High Availability requirements defined in the technical documentation.
2. Fail otherwise.

Supporting Evidence:

1. References to to documentation sections.

6.2 Technical cybersecurity requirement tests and assessments

6.2.0.0 REQ-TECH-0

Requirement: The product shall be shipped without undocumented interfaces.

Objective: How the product communicates is understood and documented.

Preparation:

1. Have the product initialised and available with the default configuration and required credentials.

Activities:

1. Study the technical documentation.
2. Study the listed documented communication endpoints.
3. List all the interfaces the product is listening.
4. Cross-reference the open interfaces to the documentation.

Verdict:

1. Pass, if all interfaces used for communication are documented.
2. Fail otherwise.

Supporting Evidence:

1. References to to documentation sections.

6.2.0.1 REQ-TECH-1

Requirement: A network management system shall implement [5.2.4 State-of-the-art cryptographic libraries](#) to allow the protection of the requirements of the foreseeable use.

Objective: Agreed Cryptographic Mechanisms specification is followed and the product shows it does that.

Preparation:

1. Have the product initialised and available with the default configuration and required credentials.

Activities:

1. Study the technical documentation.
2. Identify the patterns from architectural documentation where encryption is required.
3. Study the implementation from the product or from the technical documentation.

Verdict:

1. Pass if the documentation describes with enough details how and where the encryption is used,
2. and handling of PII and privileged information is identified and protected with [5.2.4 State-of-the-art cryptographic libraries](#).
3. Fail otherwise.

Supporting Evidence:

1. References to to documentation sections.

6.2.0.2 REQ-TECH-2

Requirement: When privileged information is transferred or accessed, a secure channel shall be used in transport [5.2.1 Secure channel](#).

Objective: Protect the integrity of the data.

Preparation: None

Activities:

1. Study the technical documentation.
2. Identify the structures where administrative, PII or otherwise privileged information is transferred.
3. Study the implementation from the product and from the technical documentation.

Verdict:

1. Pass, if the flow of privileged information is identifiable from the documentation,
2. and testing the implementation of interfaces matches the documentation.
3. Fail otherwise.

Supporting Evidence:

1. Listing of tested interfaces and the protocol replies that show what encryption is used.

6.2.0.3 REQ-TECH-3

Requirement: All endpoints in a secure channel shall cryptographically verify others.

Objective: Mutual authentication ensures that blind trust is not part of the system design.

Preparation: None

Activities:

1. Study the technical documentation.
2. Identify the structures where administrative, PII or otherwise privileged information is transferred.

3. Study the implementation from the product and from the technical documentation.

Verdict:

1. Pass, if the described system implements mechanism for mutual authentication,
2. and, there is no debug mode or equivalent activated on by default.
3. Fail otherwise.

Supporting Evidence:

1. References to to documentation sections.

6.2.0.4 REQ-TECH-4

Requirement: The product shall be designed in a way that [5.2.2 Cryptographic key intialisation and rotation](#) is made possilbe.

Objective: Ensure product that allows and encourages users to change keys when necessary for product security reasons, such as when employees and administrators roles change..

Preparation: None

Activities:

1. Study the technical documentation.
2. Cross reference the instuctions how and how often to do rotation of important keys to industry state-of-the art policies..

Verdict:

1. Pass, if key rotation can be made on demand,
2. and the instructed rotation policy is fit for the foreseeable use of the product.
3. Fail otherwise.

Supporting Evidence:

1. References to to documentation sections.

6.2.0.5 REQ-TECH-5

Requirement: All system components shall be synchronized to the same time.

Objective: Prevent errors and innaccuracvy in logging, metrics, and traces, due to unsynchronized component clocks.

Preparation:

1. Have the product initialised and available with the default configuration and required credentials.

Activities:

1. Dump all clock from all participating systems and nodes.
2. Ensure that the clock deviation is within limits specified in the techinal documentation.
3. If unsure, verify that the clock synchronisation mechanism is in use and functioning in the default installation.

Verdict:

1. Pass, if the clock deviation is under the specified limit in the technical documentation.
2. Fail otherwise.

Supporting Evidence:

1. Log output from the test.

6.2.0.6 REQ-TECH-6

Requirement: All system clock drifts shall be monitored.

Objective: Where multiple monitoring sources all operate they shall have consistent clocks where any drift or lack of synchronization shall be accurately documented and notification provided to administrator.

Preparation:

1. Have the product initialised and available with the default configuration and required credentials.

Activities:

1. Set a node or a system to a wrong time that is off by at least an hour.

Verdict:

1. Pass, if system notices the drift,
2. and creates a notification about the event.
3. Fail otherwise.

Supporting Evidence:

1. System notification from the logs.

6.2.0.7 REQ-TECH-7

Requirement: The product shall be designed in a way, that all cryptographic keys can be replaced with user controlled keys.

Objective: Product shall provide users with data management capabilities and ability to verify the integrity of the stored data in the NMS.

Preparation: None

Activities:

1. Study the technical documentation.
2. Cross reference to the architectural description of how the encryption is used in different parts of the system.

Verdict:

1. Pass, if customer has a ability to change all cyptographic keys in the system.
2. Fail otherwise.

Supporting Evidence:

1. References to to documentation sections.

6.2.5.0 REQ-SBOM-0

Requirement: Operating system dependencies and application dependencies shall be clearly separated in the provided SBOM.

Objective: To make clear what part of the system to upgrade, the source of the dependency should be understandable.

Preparation: None

Activities:

1. Study the technical documentation.

Verdict:

1. Pass if system dependencies and application dependencies are clearly separated.
2. Fail otherwise.

Supporting Evidence:

1. References to to documentation sections.

6.2.5.1 REQ-SBOM-1

Requirement a: Unique, unambiguous, and machine-readable identification of all components and dependencies are provided in the SBOM.

Requirement b: The SBOM identifier format is consistent with common vulnerability handling standards.

Objective: A linux kernel version can be 6.18, but what it contains? A referable and exact pointer is needed.

Preparation: None

Activities:

1. Study the technical documentation.
2. Study the SBOM.

Verdict:

1. Pass if provided SBOM identifiers are unique
2. and recognised in the industry
3. and cross referable to known vulnerability databases.
4. Fail otherwise.

Supporting Evidence:

1. References to to documentation sections.

6.2.5.2 REQ-SBOM-2

Requirement: The SBOM shall be consistent with [5.3.4 Secure updates](#) practices.

Objective: The deliverable erodes over time. The SBOM is one of the sources for the motivation to upgrade.

Preparation: None

Activities:

1. Study the technical documentation.
2. Study the SBOM.
3. Cross reference to upgrade instructions.

Verdict:

1. Pass if instructions are operatively consistent.
2. Fail otherwise.

Supporting Evidence:

1. References to to documentation sections.

6.3 Risk mitigations tests

6.3.6 Metrics tests

6.3.6.0 REQ-METRICS-0

Requirement: The product shall be designed in a way that collected and stored metrics data can not be altered.

Objective: An attacker wants to hide its operations. System should prepare for that.

Preparation: None

Activities:

1. Study the technical documentation.

Verdict:

1. Pass if no unauthorised process before ingestion of collected metrics data can alter the metrics before storage,
2. and the storage can not be altered outside of regular cleaning cycles.
3. Fail otherwise.

Supporting Evidence:

1. References to to documentation sections.

6.3.6.1 REQ-METRICS-1

Requirement: Historical metrics data import overwriting an existing data point shall be noticed.

Objective: Prevent compromised managed element to hide its behaviour.

Preparation:

1. Have the product initialised and available with the default configuration.

2. Create required authentication credentials for the test.
3. Prepare an import data set, that represents natural collected values from the target.
4. Create a copy of the import data set and modify the values.

Activities:

1. Begin timeseries data collection.
2. Restart the collection of timeseries data with the modified data set.

Verdict: Pass if systems detects the modified data set.

Supporting Evidence:

1. Collect output showing the whether the current metrics data is being handled by the normal flow as expected.
2. Collect output showing how the modified data set was accepted or discarded.

6.3.6.2 REQ-METRICS-2

Requirement: Metrics name, purpose, and value interpretation shall be described for the user.

Objective: Understanding what is collected helps user to understand what happens, but also is needed for data minimisation validation.

Preparation:

1. Have the product initialised and available with the default configuration and required credentials.

Activities:

1. Study the monitoring data GUI.
2. Study the provided documentation.
3. Investigate the metrics storage.

Verdict:

1. Pass if there are no unknown metrics displayed or collected.
2. Pass if the metric well-known, like CPU usage, but undocumented.
3. Pass if the metric is recognised and pointer to the documentation is provided (managed element manufacturer's reference documentation e.g.).
4. Fail otherwise.

Supporting Evidence:

1. The technical documentation.
2. Screenshot of the GUI displaying how the data is displayed.

6.3.6.3 REQ-METRICS-3

Requirement: Metrics cadence, accuracy and storage time shall be described for the user.

Objective: Metrics storage consumes a lot of storage, and also affects persons privacy as rarely the data is deleted on demand.

Preparation:

1. Have the product initialised and available with the default configuration and required credentials.

Activities:

1. Study the monitoring data GUI.
2. Study the provided documentation.
3. Investigate the metrics storage.

Verdict:

1. Pass if the metrics collection cadence, accuracy and storage time matches the described use.
2. Fail otherwise.

Supporting Evidence:

1. The technical documentation.
2. Metrics storage plan.

6.3.6.4 REQ-METRICS-4

Requirement: Relevant system and connected element metrics such as CPU, memory, disk utilisation shall be tracked and reported.

Objective: Support users or administrators ability to detect compromised, misconfigured, or harmful connected elements through unusual, excessive, or risky patterns of use.

Preparation:

1. Have the product initialised and available with the default configuration and required credentials.
2. Have at least one managed element as part of the system the product operates

Activities:

1. Study the provided technical documentation to interpret the monitoring data GUI.
2. Simulate unnormal behaviour by intentionally cutting the connection with a managed element and observe the monitoring data.
3. Restart the managed element.

Verdict:

1. Pass if basic administrative metrics are tracked and displayed.
2. Pass if the connection loss to the managed element is recognized.
3. Pass if by observing the metrics a baseline can be established.
4. Pass if anomalies like load spikes after a restart can be observed.
5. Fail otherwise.

Supporting Evidence:

1. The technical documentation of the monitoring data.
2. Screenshot of the GUI displaying how the data is displayed the normal operation and the detection of the unnormal behaviour.

6.3.6.5 REQ-METRICS-5

Requirement a: System process and service crashes and restarts shall be tracked and reported.

Requirement b: Managed element process and service crashes and restarts shall be tracked and reported.

Objective: Crashes are used to modify the program state. Abnormal crashes can be an indication of upcoming compromise.

Preparation:

1. Have the product initialised and available with the default configuration and required credentials.
2. Have the managed element initialised and available with the default configuration and required credentials.

Activities:

1. Purposefully crash a process or restart a connected element.
2. Study the metrics output.

Verdict:

1. Pass if process or device specific counter is iterated.
2. Fail otherwise.

Supporting Evidence: Log or and metrics output showing detected system or managed element crash or restart with the reported cause.

6.3.6.6 REQ-METRICS-6

Requirement: Managed elements and system nodes and provided services availabilities and statuses shall be tracked and reported.

Objective: Bad availability can be a indication of compromise.

Preparation:

1. Have the product initialised and available with the default configuration and required credentials.
2. Have the managed element initialised and available with the default configuration and required credentials.

Activities:

1. Study the monitoring data GUI.
2. Study the provided documentation.

Verdict:

1. Pass if Service Level Indicator defines and implements expected operation availability per connected element and relevant system processes.
2. Fail otherwise.

Supporting Evidence:

1. The technical documentation.
2. Screenshot of the GUI displaying how the data is displayed.

6.3.6.7 REQ-METRICS-7

Requirement a: Relevant system database and storage health metrics like queries per second, latency and throughput shall be tracked and reported.

Requirement b: Relevant managed element database and storage health metrics like queries per second, latency and throughput shall be tracked and reported.

Objective: Bad service quality can be a indication of compromise.

Preparation:

1. Have the product initialised and available with the default configuration and required credentials.
2. Have the managed element initialised and available with the default configuration and required credentials.

Activities:

1. Study the monitoring data GUI.
2. Study the provided documentation.

Verdict:

1. Pass if Service Level Indicator defines and implements expected operation
 - success rate
 - operation failure rate
 - query execution time
 - response size where applicable.
2. Fail otherwise.

Supporting Evidence:

1. The technical documentation.
2. Screenshot of the GUI displaying how the data is displayed.

6.3.6.8 REQ-METRICS-8

Requirement: Relevant networking metrics like throughput and protocol errors shall be tracked and reported.

Objective: When the errors stop and the throughput returns to nominal levels, the damage has already been done.

Preparation:

1. Have the product initialised and available with the default configuration and required credentials.
2. Have the managed element initialised and available with the default configuration and required credentials.

Activities:

1. Study the monitoring data GUI.
2. Study the provided documentation.
3. Generate large amount of traffic in random location.

Verdict:

1. Pass if corresponding metrics matches the generated traffic.
2. Fail otherwise.

Supporting Evidence:

1. The technical documentation.
2. Screenshot of the GUI displaying how the data is displayed.

6.3.6.9 REQ-METRICS-9

Requirement: GUI and API latencies and error rates shall be tracked and reported.

Objective: Wrong calls to the endpoints is an indication of compromise attempt.

Preparation:

1. Have the product initialised and available with the default configuration and required credentials.
2. Have the managed element initialised and available with the default configuration and required credentials.

Activities:

1. Send a correct API request towards each system API endpoint.

Verdict:

1. Pass if all API endpoints responds as expected
2. and the response latency is recorded in defined accuracy
3. and tracks the number of successfull requests.
4. Fail otherwise.

Supporting Evidence:

1. Relevant metrics described in the technical documentation.

6.3.8 High availability tests**6.3.8.0 REQ-HA-0**

Requirement: Expected availability shall be defined for each relevant system component.

Objective: Preparation:

1. Have the product initialised and available with the default configuration and required credentials.

Activities:

1. Study the metrics for availability information

Verdict:

1. Pass all relevant components availability is defined and tracked
2. Fail otherwise.

Supporting Evidence:

1. Relevant metrics described in the technical documentation.

2. Screen shots of metrics being visualised in the dashboards.

6.3.8.1 REQ-HA-1

Requirement: System updates and changes shall be included in the availability time definition.

Objective:

Preparation:

1. Have the product initialised and available with the default configuration and required credentials.

Activities:

1. Kill a random process, processing node or simulate a loss of a datacenter.
2. Repeat first step enough of times with varying scopes to demonstrate conformance.

Verdict:

1. Pass if loss of a resource matching the availability and distribution description doesn't exceed the availability definition.
2. Fail otherwise.

Supporting Evidence:

1. Structured log output or other documentation that shows made actions and perceived operative response.

Objective: System updates and changes are included in the availability definition.

Preparation: None

Activities:

1. Study the availability definition and the presented metrics.

Verdict:

1. Pass if system changes, updates and upgrades are not considered to be outside of the availability definition and tracking.
2. Fail otherwise.

Supporting Evidence:

1. Pointers to the documentation.

6.3.8.2 REQ-HA-2

Requirement: System shall tolerate loss of resources within the limits of the defined availability.

Objective: The customer understands how the system behaves under different conditions and can make a disaster recovery plan for the operation.

Preparation:

1. Have the product initialised and available with the default configuration and required credentials.

Activities:

1. Study the availability definition from the documentation.

2. Delete or make unavailable: service, compute node, rack, or datacenter based on the what the system design tolerates.
3. Wait for stability.
4. Return the resrouce taken away in previous step.
5. Wait for stability.

Verdict:

1. Pass if recovery expectations are clearly defined,
2. and the system returns to stability after removal of the largest resource in the toleration description,
3. and the deleted or removed resources returns operation after they are reintroduced to the system,
4. and the defined high availability is hold.
5. Fail otherwise.

Supporting Evidence:

1. Pointers to the documentation.
2. Description of the test procedure and relevant bits of log showing the phases.

6.3.8.3 REQ-HA-3

Requirement: Recovery capabilities shall be made available in the technical documentation and are sufficient to implement the expected availability.

Objective: The customer understands how the sytem behaves undre different conditions and can make a disaster recovery plan for the operation.

Preparation: None

Activities:

1. Cross-reference the recovery capabilities with the distribution description.
2. Cross-reference the recovery capabilities with the deployment plan and system architecture.

Verdict:

1. Pass if recovery expectations are clearly defined
2. and the distribution of the system operation is within reasonable scope in regards of the production size.
3. Fail otherwise.

Supporting Evidence:

1. Pointers to the documentation.

Annex A (informative): Mapping with essential requirements of the CRA

Table mapping technical cybersecurity requirements from Section 5 of the present document to essential cybersecurity requirements in Annex I of the CRA. The purpose of this is to help identify missing technical cybersecurity requirements.

Table A-1: Essential requirements mapping

CRA requirement	Technical cybersecurity requirements
No known exploitable vulnerabilities	5.1.1 No known exploited vulnerabilities
Secure design, development, production	5.1.2 Secure design, development and production
Secure by default configuration	5.2.4 State-of-the-art cryptographic libraries
Secure updates	5.3.4 Secure updates
Authentication and access control mechanisms	5.2.6 Role based authorisation
Confidentiality protection	5.3.2 Mitigations for ingested data integrity and confidentiality
Integrity protection for data and configuration	5.3.2, 5.3.3, 5.3.6 Metrics
Data minimisation	5.3.7 Data minimisation
Availability protection	5.3.8 High Availability
Minimise impact on other devices or services	5.3.8 High Availability
Limit attack surface	5.1.3 Product vulnerability management process
Exploit mitigation by limiting incident impact	5.2.6 Role based authorisation
Logging and monitoring mechanisms	5.3.5 Logging, 5.3.6 Metrics
Secure deletion and data transfer	[REQ-METRICS-3], 5.2.1 Secure channel

Table mapping status of cybersecurity requirements in each section. Will be removed from the finalised standard.

Table A-2: Cybersecurity requirements mapping to sections

Section	Content status	Tests status
5.1 General	done	done
5.1.1 No known exploited vulnerabilities	done	done
5.1.2 Secure design, development and production	done	n/a
5.1.3 Product vulnerability management process	done	n/a
5.2 Technical cybersecurity requirements specifications	done	done
5.2.1 Secure channel	done	n/a
5.2.2 Cryptographic key intialisation and rotation	done	
5.2.3 Network segmentation	idea would need refinement	
5.2.4 State-of-the-art cryptographic libraries	done	n/a
5.2.5 Software Bill of Materials	done	
5.2.6 Role based authorisation	done	
5.2.7 Remote Data Processing Systems	waits for AMS input	
5.3.1 Mitigations for user identity integrity	done	
5.3.2	done	
5.3.3	done	
5.3.4 Secure updates	done	
5.3.5 Logging	done	
5.3.6 Metrics	done	done
5.3.7 Data minimisation	done	
5.3.8 High Availability	done	done

Annex B (informative): Relationship between the present document and any related ETSI standards (if any)

List any related ETSI standards and how they interact with the present document.

- 3gpp <https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=3973>

Annex C (informative): Risk acceptance criteria and risk management methodology

Ref. (PT1 6.3) Table mapping the identified risks to requirements

C.1 Risk acceptance and risk management methodology

Describe how to decide if residual risks are tolerable.

C.2 Risk assessment methodology

Risk levels for each factors are determined by reading the descriptions for each risk factor and choosing the one that most accurately represents the highest risk for the intended purpose and reasonably foreseeable use and misuse of the product, as specified by the manufacturer.

The risks can be divided to likelihood and impact, but they can also be presented as a whole. When likelihood and impact is presented, only high and low evaluation is available. Risk is considered to be medium, when one of the likelihood and impact is low, and the other one is high.

When both likelihood and impact are low, the requirements defined in the chapter [5 Requirements specifications](#) defined for low category sets the minimum required features for any product within the category subject to this document.

When multiple risk factors are combined in a single requirement applicability, the highest risk level determines what is required from the product.

To be able to map the product requirements applicability:

1. Document a comprehensive range of foreseeable use cases for products of this type.
2. Define the product risk levels evaluating the risk factors as low-mid-high based on the instructions.
3. Cross reference to [5 Requirements specifications](#) requirements.
4. See from [6 Conformity assessments and tests](#) how to show conformity of the product.

C.2.1 Assets

NMS protects systems that are relying on network connectivity to perform its daily operations.

Business continuity

- market information
- business-critical processes
 - manufacturing
 - finances
- compliance evidence if form of logs and reports

Incident response capability

- ability to detect, diagnose, and remediate outages

Network configuration

- network configuration
- network inventory

- network topology
- network segmentation policies
- firewall rules

Connected devices

- management traffic
- access to the management interface
- connected devices updates, patches
- CORBA access, grpc
- keys can be generated or imported through the key management modules

C.2.1.1 Data assets

The stored data depends on what functions the NMS has available and what the intend use is. The stored data can be, but is not limited to:

- System audit data
 - authentication data
 - syslogs
- cryptographic data like encryption keys
- Backups
- Device monitoring data
- Sensitive monitoring data
 - NetFlow information
 - Packet captures
 - Protocol analysis information
- Network configuration data

C.2.2 Threats

Based on the assets, what are the threats during:

- Use for intended purpose or reasonably foreseeable use
- When integrated into another product

Example threats can be found in the same documents suggested in the section on cybersecurity requirements.

[Recital 58] [i.1]

- economic espionage
- irresponsible state behaviour in cyberspace and its legislation allows
- arbitrary access to any kind of company operations or data
- commercially sensitive data
- impose obligations for intelligence purposes without democratic checks and balances

- oversight mechanisms
- due process or the right to appeal

Table C.2.2-1: Threats

What	How?	More?
CVE-2025-6763	Unauthorised configuration modification	
CVE-2024-5245	Default Credentials Local Privilege Escalation	CVE-2024-5245 PoC
CVE-2025-46274	Hard-coded credentials	
CVE-2025-46271	Command injection before auth	more in cybersecurity news
CVE-2025-24937	Local file modification and privilege escalation	
CVE-2024-25010	Improper input validation leading to arbitrary code execution	
CVE-2022-48469	There is a traffic hijacking vulnerability in routers	
CVE-2025-27212	Device command injection	

- [Nokia's advisories](#)
- [Ericsson's security bulletins](#)
- [Huawei's vulns](#)
- Samsung: no publicly available vulnerability database.

C.3 Assumptions

- Proper operating system
 - **Rationale:** A network management system requires a trustworthy operating system to perform its functions.
- Proper administrator
 - **Rationale:** A network management system requires effective administration to perform its functions.
- Not being attacked by a state actor
- Not using sophisticated or expensive hardware snooping techniques
- No secret hardware backdoors

Annex D (informative): Risk evaluation guidance

For each network management system placed on the market, the manufacturer shall develop a threat model and risk profile of the foreseeable use of the system, and shall consider the interplay between:

- Complexity of foreseeable use
- Likelihood of an incident, given the foreseeable use
- Impact of an incident, given the foreseeable use

Attack vectors that are the responsibility of the network management system:

- Arbitrary commands from outside the system control boundaries
 - Through APIs
 - From GUI
 - Context manipulation (DNS, TLS)
 - Ingested data manipulation
- Unprivileged actors inside the system control boundaries
 - Malicious networking node
 - Malicious 3rd. party integration
- Privileged actors inside the system control boundaries
 - Credential missuse

Out of scope attack vectors:

- Anything the OS is responsible for
 - Direct bit twiddling of registers

Refer to normative standards:

- Device driver attack vectors
- Physical interface specific attack vectors?

Annex L (informative): Relationship between the present document and the requirements of EU Regulation 2024/2847

DRAFT ANNEX L - DO NOT CONSIDER THE CONTENT

The present document has been prepared under the Commission's standardisation request C(2025) 618 final to provide one voluntary means of conforming to the requirements of Regulation (EU) No 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) No 2019/1020 and Directive (EU) 2020/1828 (Cyber Resilience Act). Once the present document is cited in the Official Journal of the European Union under that Regulation, compliance with the normative clauses of the present document given in table A.1 confers, within the limits of the scope of the present document, a presumption of conformity with the corresponding requirements of that Regulation and associated EFTA regulations.

NOTE: The above paragraphs have to be repeated in the Foreword.

The annex shall have a table for a clear indication of correspondence between normative clauses of the standard and the legal requirements aimed to be covered.

It should be evaluated - on the basis of the legal requirements supported and other information given in a harmonised standard - how detailed correspondence can be indicated between the normative elements of the harmonised standard and the legal requirements aimed to be covered. However, where this correspondence is expressed in too general terms, it could lead to a situation where the Commission cannot assess whether the Harmonised Standard satisfies the requirements, which it aims to cover, and subsequently publication of its references in the OJEU according to Article 10(6) of the Regulation is significantly delayed or is not possible at all.

EXAMPLE: EXAMPLE: EXAMPLE for a table:

Table A.1: Relationship between the present document and the requirements of EU Regulation 2024/2847

Requirement		Requirement Conditionality			
No	Description	Requirements of Regulation	Clause(s) of the present document	Use case	Condition
1					
2					
3					
...					

Key to columns:

Requirement:

No A unique identifier for one row of the table which may be used to identify a requirement.

Description A textual reference to the requirement.

Requirements of Regulation Identification of article(s) defining the requirement in the Regulation.

Clause(s) of the present document Identification of clause(s) defining the requirement in the present document unless another document is referenced explicitly.

Requirement Conditionality:

Use case Indicates whether the requirement is unconditionally applicable (U) or is conditional upon the manufacturer's claimed functionality of the equipment (C).

Condition Explains the conditions when the requirement is or is not applicable for a requirement which is classified "conditional".

NOTE 1: The table cannot indicate direct relationship between the relevant legal requirement and other standards or normative clauses contained in other standards.

NOTE 2: The order of the first and the second columns can be changed.

NOTE 3: The title of this column can be adapted on the basis of specific needs

The annex shall have at least the following two warnings.

A warning stating that presumption of conformity is effective only as long as the reference is maintained in the OJEU by the Commission. The following URL-address https://ec.europa.eu/growth/single-market/european-standards/harmonised-standards_en to consult the latest list of Harmonised Standards published in the OJEU should be provided.

Presumption of conformity stays valid only as long as a reference to the present document is maintained in the list published in the Official Journal of the European Union. Users of the present document should consult frequently the latest list published in the Official Journal of the European Union.

A warning stating that those products or services which are within the scope of a relevant standard may be also subject to other Union legislation.

Other Union legislation may be applicable to the product(s) falling within the scope of the present document.

Annex <L+3> (informative): Bibliography

<Publication>: "<Title>".<Edition>. <Year>, <Issue designation>, <Page location>.

Annex <L+4> (informative): Change history

The "Change history/Change request (history)" annex shall be included in every revised or amended harmonised standard and shall contain information concerning significant changes that have been introduced by it. It shall be presented as a table.

Document history		
Month year	Version	Milestone (Changes made)

History

The following table will automatically be filled in by the ETSI Secretariat.

Document history		
Version	Month year	Milestone (Changes made)