ETSI TR 119 404 V1.1.1 (2023-02)

Electronic Signatures and Infrastructures (ESI);
NIS2 and its impact on eIDAS standards

Reference
DTR/ESI-0019404

Keywords
trust services

ETSI

650 Route des Lucioles
F-06921 Sophia Antipolis Cedex - FRANCE

Tel.: +33 4 92 94 42 00 Fax: +33 4 93 65 47 16

Siret N° 348 623 562 00017 - APE 7112B
Association à but non lucratif enregistrée à la
Sous-Préfecture de Grasse (06) N° w061004871

Contents

Intellectual Property Rights

Essential patents

IPRs essential or potentially essential to normative deliverables may have been declared to ETSI. The declarations pertaining to these essential IPRs, if any, are publicly available for **ETSI members and non-members**, and can be found in ETSI SR 000 314: *"Intellectual Property Rights (IPRs); Essential, or potentially Essential, IPRs notified to ETSI in respect of ETSI standards"*, which is available from the ETSI Secretariat. Latest updates are available on the ETSI Web server (https://ipr.etsi.org/).

Pursuant to the ETSI Directives including the ETSI IPR Policy, no investigation regarding the essentiality of IPRs, including IPR searches, has been carried out by ETSI. No guarantee can be given as to the existence of other IPRs not referenced in ETSI SR 000 314 (or the updates on the ETSI Web server) which are, or may be, or may become, essential to the present document.

Trademarks

The present document may include trademarks and/or tradenames which are asserted and/or registered by their owners. ETSI claims no ownership of these except for any which are indicated as being the property of ETSI, and conveys no right to use or reproduce any trademark and/or tradename. Mention of those trademarks in the present document does not constitute an endorsement by ETSI of products, services or organizations associated with those trademarks.

DECT™, **PLUGTESTS™**, **UMTS™** and the ETSI logo are trademarks of ETSI registered for the benefit of its Members. **3GPP™** and **LTE™** are trademarks of ETSI registered for the benefit of its Members and of the 3GPP Organizational Partners. **oneM2M™** logo is a trademark of ETSI registered for the benefit of its Members and of the oneM2M Partners. **GSM**® and the GSM logo are trademarks registered and owned by the GSM Association.

Foreword

This Technical Report (TR) has been produced by ETSI Technical Committee Electronic Signatures and Infrastructures (ESI).

Modal verbs terminology

In the present document "**should**", "**should not**", "**may**", "**need not**", "**will**", "**will not**", "**can**" and "**cannot**" are to be interpreted as described in clause 3.2 of the ETSI Drafting Rules (Verbal forms for the expression of provisions).

"**must**" and "**must not**" are **NOT** allowed in ETSI deliverables except when used in direct citation.

Introduction

The cybersecurity of all essential digital services is vital for the digital transformation of Europe with digital services and electronic transactions. The provision of eIDAS trust services is identified as an essential element of Europe's digital infrastructure. The Directive (EU) 2022/2555 [i.2] of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive 2016/1148 (NIS2 Directive or NIS2) identifies requirements for cybersecurity risk management measures to be applied to providers of essential services including eIDAS trust services.

The existing ETSI EN 319 401 [i.7] defines General Policy Requirements for Trust Service Providers, including Qualified Trust Service Providers, which has been adopted as the basis for security of all ETSI standards for trust services. These ETSI standards for trust services have been adopted as the basis for assessing trust services compliance with the eIDAS Regulation across nearly all European Member States. ETSI EN 319 401 [i.7] already supports a large part of the cybersecurity requirements of the NIS2 Directive. However, detailed aspects of the NIS2 requirements, such as aspects of supply chain security, need to be incorporated into ETSI EN 319 401 [i.7]. Also, other ETSI standards for trust services may need updating to include additional references to the cybersecurity requirements specified in ETSI EN 319 401 [i.7] in order to fully comply with NIS2.

1 Scope

The present document:

- outlines the main requirements of NIS2;
- analyses the requirements of NIS2 Directive against the existing cybersecurity provisions of ETSI EN 319 401 [i.7] in order to identify areas where additional provisions are needed;
- takes into account the use of ISO 27002 general information security controls for cyber security used in support of ETSI EN 319 401 [i.7] including revisions to align with the major reorganisation to ISO 27002 from the 27002:2013 [i.5] to the 27002:2022 [i.6];
- establishes a methodology for aligning other ETSI standards with the NIS2 Directive.

2 References

2.1 Normative references

Normative references are not applicable in the present document.

2.2 Informative references

References are either specific (identified by date of publication and/or edition number or version number) or non-specific. For specific references, only the cited version applies. For non-specific references, the latest version of the referenced document (including any amendments) applies.

NOTE: While any hyperlinks included in this clause were valid at the time of publication ETSI cannot guarantee their long term validity.

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

[i.1] Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union (NIS1).

[i.2] Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS2).

[i.3] Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC.

[i.4] Proposal for a Regulation of the European Parliament and of the Council amending Regulation (EU) No 910/2014 as regards establishing a framework for a European Digital Identity.

NOTE: The opinion of the council was published under 2021/0136(COD). The opinion of the Parliament was not yet published.

[i.5] ISO 27002:2013: "Information technology - Security techniques - Code of practice for information security controls".

[i.6] ISO 27002:2022: "Information technology - Security techniques - Code of practice for information security controls".

[i.7] ETSI EN 319 401: "Electronic Signatures and Infrastructures (ESI); General Policy Requirements for Trust Service Providers".

[i.8] ISO/IEC 27005: " Information technology - Security techniques - Information security risk management".

[i.9] ISO/IEC 27000: "Information technology - Security techniques - Information security management systems - Overview and vocabulary".

3 Definition of terms, symbols and abbreviations

3.1 Terms

For the purposes of the present document, the terms defined in NIS2 Directive [i.2] and the following apply:

cybersecurity: activities necessary to protect network and information systems, the users of such systems, and other persons affected by cyber threats

cyber threat: potential circumstance, event or action that could damage, disrupt or otherwise adversely impact network and information systems, the users of such systems and other persons

impact: harm that may be suffered when a threat compromises an information asset

incident: any event compromising the availability, authenticity, integrity or confidentiality of stored, transmitted or processed data or of the services offered by, or accessible via, network and information systems

incident handling: any actions and procedures aiming to prevent, detect, analyse, and contain or to respond to and recover from an incident

large-scale cybersecurity incident: incident whose disruption exceeds a Member State's capacity to respond to it or with a significant impact on at least two Member States

near miss: event that could have compromised the availability, authenticity, integrity or confidentiality of stored, transmitted or processed data or of the services offered by, or accessible via, network and information systems, but was successfully prevented from transpiring or did not materialise

qualified trust service provider: trust service provider who provides one or more qualified trust services and is granted the qualified status by the supervisory body

NOTE: As defined in eIDAS2 [i.4].

risk: potential for loss or disruption caused by an incident and is to be expressed as a combination of the magnitude of such loss or disruption and the likelihood of occurrence of that incident

risk analysis: process of estimating the likelihood that an event will create an impact and includes as necessary components, the foreseeability of a threat, the expected effectiveness of Safeguards, and an evaluated result

risk assessment: comprehensive project that evaluates the potential for harm to occur within a scope of information assets, controls, and threats

risk management: process for analysing, mitigating, overseeing, and reducing risk

security of network and information systems: ability of network and information systems to resist, at a given level of confidence, any event that may compromise the availability, authenticity, integrity or confidentiality of stored or transmitted or processed data or of the services offered by, or accessible via, those network and information systems

significant cyber threat: cyber threat which, based on its technical characteristics, can be assumed to have the potential to severely impact the network and information systems of an entity or its users by causing considerable material or non-material losses

trust service: 'trust service' means an electronic service normally provided for remuneration which consists of:

(a) the issuing of certificates for electronic signatures, of certificates for electronic seals, of certificates for website authentication or of certificates for the provision of other trust services;

(aa) the validation of certificates for electronic signatures, of certificates for electronic seals, of certificates for website authentication or of certificates for the provision of other trust services;

(b) the creation of electronic signatures or of electronic seals;

(c) the validation of electronic signatures or of electronic seals;

(d) the preservation of electronic signatures, of electronic seals, of certificates for electronic signatures or of certificates for electronic seals;

(e) the management of remote qualified electronic signature creation devices or of remote qualified electronic seal creation devices;

(f) the issuing of electronic attestations of attributes.

NOTE: As defined in eIDAS2 [i.4].

trust service provider: natural or a legal person who provides one or more trust services either as a qualified or as a non-qualified trust service provider

NOTE: As defined in eIDAS2 [i.4].

vulnerability: weakness, susceptibility or flaw of ICT products or ICT services that can be exploited by a cyber threat

3.2 Symbols

Void.

3.3 Abbreviations

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

eIDAS1	Regulation (EU) No 910/2014 [i.3]
eIDAS2	Proposal for a Regulation [i.4]
NIS1	Directive (EU) 2016/1148 [i.1]
NIS2	Directive (EU) 2022/2555 [i.2]
QTSP	Qualified Trust Service Provider
TSP	Trust Service Provider

4 Overview

4.1 Introduction

The NIS2 Directive [i.2], unlike the NIS1 Directive [i.1], includes TSPs within its scope of application and refers to them in various parts of its provisions. In addition, the draft eIDAS2 Regulation refers to the NIS2 Directive in terms of the security requirements that TSPs have to comply with.

Until the final text of the eIDAS2 Regulation [i.4] is approved, it is uncertain whether the reference is made for all TSPs' Information security measures or those relating to cybersecurity only.

In any case, in the present document it will be taken into consideration the state of the art in relation to the security requirements of TSPs a per eIDAS1 Regulation, ETSI EN 319 401 [i.7] as well as the specific standards of each trust service.

The division of Information security and cybersecurity requirements into two documents, eIDAS2 Regulation [i.4] and NIS2 Directive [i.2], with different scopes of application and normative force creates the following challenges:

- The eIDAS2 Regulation is directly applicable in the Member States as soon as it is published or the date of entry into force set therein without the need for national applications even if the implementing acts are still pending. The NIS2 Directive, however, by its very nature, requires national implementation into domestic law of each Member State, which may not be homogeneous.

- National rules implementing the NIS2 Directive and the application of these rules to TSPs based on their territory may pose a risk to the European market for TSPs as per the eIDAS1 Regulation. Now, a QTSP only needs to be assessed in a Member State under the control of the national supervisor to be able to provide services in the EU without further regulatory constraint. However, following the applicability of the NIS2 Directive to TSPs, and thus the obligation to abide different national rules adopted in its implementation, there is a risk that QTSPs need more than a single assessment if they are to provide services in more than one Member State. Article 26(1) states that entities fall under the restriction of the member state in which they are established. However, in case the transposition of the directive in a member states requires that all services used by an entity falling under NIS2 fulfill the requirements of NIS2 this might lead to complication if a service from another member state is used.

- The NIS2 Directive establishes a system of supervision that, if not properly articulated at national level, could lead to a TSPs duplicated supervision.

The present document, then, is aimed at analysing the IT and cybersecurity requirements for TSPs in the light of this new regulatory environment, proposing, as far as possible, solutions that allow, firstly, to standardise an adequate level of cybersecurity for all TSPs regardless of the country in which they provide services and, furthermore, to fully comply with the NIS2 Directive.

4.2 General obligations under the NIS2 Directive

Irrespectively of the specific cybersecurity and Information security requirements referred to in clause 5 of the present document, TSPs are subject to the following general obligations of the NIS2 Directive [i.2], which are referred to throughout its provisions:

1) Article 3 paragraph 4 establishes a list of information that TSPs, as subject to NIS2, have to provide to Member States' competent authorities: the name of the entity; the address and up-to-date contact details, including email addresses, IP ranges and telephone numbers; where applicable, the relevant sector and subsector referred to in Annex I or II; and where applicable, a list of the Member States where they provide services falling within the scope of this Directive.

2) **Cybersecurity risk management and critical supply chain** (Arts. 20 to 24)

3) **European cybersecurity certification scheme** (Art. 24). Article 24 states that Member States may require entities to use particular ICT products, services and processes certified under specific European cybersecurity certification schemes. It further notes that the Commission may adopt implementing acts specifying which categories of essential or important entities are required to use certain certified ICT products, services and processes or obtain a certificate under which European cybersecurity certification schemes, and may request ENISA to prepare a candidate scheme or to review an existing European cybersecurity certification scheme in cases where no appropriate European cybersecurity certification scheme is available.

4) **Standardisation** (Art. 25). In accordance with Article 25 of the NIS2 Directive, Member States are encouraged to use European or internationally accepted standards and specifications relevant to the security of network and information systems. ENISA, in collaboration with Member States, advices and provides guidelines regarding technical areas to be considered and any existing standards, including Member States' national standards, which would allow these areas to be covered. To promote the convergent implementation of Article 21(1) and (2), Member States are encouraged to use European and international standards and technical specifications relevant to the security of network and information systems, without imposing or discriminating in favour of a particular type of technology. ENISA, in cooperation with Member States, and after consulting relevant stakeholders when appropriate, will also draw up advice and guidelines regarding technical areas to be considered, and any existing standards, including national standards, which would allow these areas to be covered.

5) **Reporting and information-sharing** (Arts. 2, 26 and 27). Article 20 requires Member States establish an extensive array of reporting and sharing obligations concerning any incident having a significant impact on the provision of services and mitigation measures. Article 29 requires Member States ensure that essential and important entities may exchange on a voluntary basis relevant cybersecurity information among themselves including information relating to cyber threats, near misses, vulnerabilities, indicators of compromise, tactics, techniques and procedures, cybersecurity alerts and configuration tools. Article 30 requires Member States that essential and important entities may notify, on a voluntary basis, to the competent authorities or the CSIRTs any relevant incidents, cyber threats or near misses.

6) **Supervisory and enforcement measures in relation to essential entities** (Arts. 32 and 33)

Other obligations set out under the NIS2 Directive [i.2] are:

1) Article 7 requires each Member State to adopt a national cybersecurity strategy defining the strategic objectives and appropriate policy and regulatory measures, with a view to achieving and maintaining a high level of cybersecurity.

2) Coordinated vulnerability disclosure. Article 12 requires each Member State designate one of its CSIRTs as a coordinator for the purpose of coordinated vulnerability disclosure. It additionally requires ENISA develop and maintain a European vulnerability registry database, in consultation with the Cooperation Group.

3) Crisis management, CSIRT, Member States cooperation, international cooperation and peer review. Article 9 requires each Member State designate one or more competent authorities responsible for the management of large-scale cybersecurity incidents and crises to identify capabilities, assets and procedures that can be deployed in case of a crisis and adopt a national cybersecurity incident and crisis response plan. Articles 9 to 19 describe the implementation, requirements, task and cooperation of national CSIRTs, an EU CSIRTs network, and the European cyber crises liaison organisation network (EU - CyCLONe).

5 Provisions related to eIDAS and Trust Service Providers: eIDAS2

5.1 Introduction

The NIS2 Directive [i.2] applies to TSPs, public or private, regardless of their size (Arts. 2.1 and 2.2). The NIS2 Directive apply where public administration entities that carry out their activities in the areas of national security, public security, defence or law enforcement, including the prevention, investigation, detection and prosecution of criminal offences acts as a trust service provider (Article 2.7 in relation to 2.9). QTSPs are considered essential entities (Article 3.1.b) and Annex i. sectors of high criticality. 8. Digital infrastructure Trust service providers). Non-qualified TSPs are considered important entities.

eIDAS2 Regulation [i.4], on its side, sets out the following obligations in relation to the NIS2 Directive:

- Articles 17 and 18 of the eIDAS2 Regulation sets out the obligation for national authorities with supervisory functions under the Regulation to cooperate with supervisory authorities under the NIS2 Directive in case of any significant breaches of security or loss of integrity of which they are aware. Article 18 confers on supervisors under the NIS2 the ability to verify whether the TSPs comply with the requirements under NIS2 Directive, to require the trust service providers to remedy any failure to comply with those requirements, to provide timely the results of any supervisory activities linked to trust service providers and to inform the supervisory bodies about relevant incidents notifying them of any such breaches.

- Article 19a requires non-qualified TSPs to comply with the requirements of Article 18 of NIS2 Directive, now Article 21, and in particular to have appropriate policies and take corresponding measures to manage legal, business, operational and other direct or indirect risks to the provision of the service. The following security measures are to be included: measures related to registration and on-boarding procedures to a service; measures related to procedural or administrative checks; and measures related to the management and implementation of services.

- The amendment of Article 20 includes within the obligation of QTSPs to be audited against the eIDAS Regulation [i.4] but also against the requirements of Article 18 of NIS2 Directive [i.2], now Article 21. The result of the audit is forwarded to the eIDAS2 Supervisory authority. The eIDAS supervisory authority, if it receives notification that a QTSP fails to fulfil any of the requirements set out by former Article 18 of the NIS2 Directive, taking into account in particular, the extent, duration and consequences of that failure, may withdraw the qualified status of that provider or of the affected service it provides.

- The new paragraph of Article 21 of eIDAS2 [i.4] states that for the verification of the requirements of Article 18, now Article 21 of NIS2 Directive, the eIDAS supervisory body *"shall request the competent authorities referred to in Dir XXXX [NIS2] to carry out supervisory actions in that regard and to provide information about the outcome without undue delay, and no later than two months from the receipt of this request by the competent authorities referred to in Dir XXXX [NIS2]. If the verification is not concluded within two months of the notification, the competent authorities referred to in Dir XXXX [NIS2] shall inform the supervisory body specifying the reasons for the delay and the period within which the verification is to be concluded. Where the supervisory body concludes that the trust service provider and the trust services provided by it comply with the requirements laid down in this Regulation, the supervisory body shall grant qualified status to the trust service provider and the trust services it provides and inform the body referred to in Article 22(3) for the purposes of updating the trusted lists referred to in Article 22(1), not later than three months after notification in accordance with paragraph 1 of this Article".*

5.2 Risk of fragmentation of the internal market

NIS2 Directive [i.2] sets out the baseline for cybersecurity risk-management measures and reporting obligations across the sectors that fall within its scope but its application to certain services/sectors implies a risk of fragmentation of the internal market.

As recognized in Recital 4 of NIS2 Directive "*The cybersecurity requirements imposed on entities providing services or carrying out activities which are economically significant vary considerably among Member States in terms of type of requirement, their level of detail and the method of supervision. Those disparities* ***entail additional costs and create difficulties for entities that offer goods or services across borders****. **Requirements** imposed* ***by one Member State*** *that are* ***different from, or even in conflict with, those imposed by another Member State, may substantially affect such cross-border activities****. Furthermore, the possibility of the inadequate design or implementation of cybersecurity requirements in one Member State is likely to have repercussions at the level of cybersecurity of other Member States, in particular given the intensity of cross-border exchanges.* ***The review of Directive (EU) 2016/1148 has shown a wide divergence in its implementation by Member States****, including in relation to its scope, the delimitation of which was very largely left to the discretion of the Member States" As per Recital 5 of NIS2 Directive "All those divergences entail a fragmentation of the internal market and can have a prejudicial effect on its functioning, affecting in particular the cross-border provision of services and the level of cyber resilience due to the application of a variety of measures. Ultimately, those divergences could lead to the higher vulnerability of some Member States to cyber threats, with potential spill-over effects across the Union".*

In order to avoid the fragmentation of cybersecurity provisions of Union legal acts, where further sector-specific Union legal acts pertaining to cybersecurity risk-management measures and reporting obligations are considered to be necessary to ensure a high level of cybersecurity across the Union, the NIS2 Directives proposes:

- either the issuance by the Commission of implementing acts under this Directive; or in accordance with Recital 84 of NIS 2 Directive, taking into account their cross-border nature the implementation of cybersecurity risk-management measures, TSPs "*should be subject to a high degree of harmonisation at Union level*" that "*should be facilitated by an implementing act*".

- sector-specific Union legal acts, when considered equivalent, could contribute to ensuring a high level of cybersecurity across the Union, while taking full account of the specificities and complexities of the sectors concerned.

5.3 Risk assessment and risk management

NIS2 Directive [i.2] states that is a TSPs' obligation taking all appropriate and proportionate measures to manage the risks posed to their services, including in relation to customers and relying third parties, and to report incidents. Such cybersecurity and reporting obligations should also concern the physical protection of the services provided.

The requirements for qualified trust service providers laid down in Article 24 of Regulation (EU) No 910/2014 [i.4] continue to apply.

5.4 Cybersecurity risk-management measures

5.4.1 Risk mitigation and cybersecurity measures

As threats to the security of network and information systems can have different origins, NIS2 Directive mandates to base cybersecurity risk-management measures on an all-hazards approach, which aims to protect network and information systems and the physical environment of those systems from events such as theft, fire, flood, telecommunication or power failures, or unauthorised physical access and damage to, and interference with, an essential or important entity's information and information processing facilities, which could compromise the availability, authenticity, integrity or confidentiality of stored, transmitted or processed data or of the services offered by, or accessible via, network and information systems.

The cybersecurity measures sets out in Article 21 are meant to address the physical and environmental security of network and information systems by including measures to protect such systems from system failures, human error, malicious acts or natural phenomena, in line with European and international standards, such as those included in the ISO/IEC 27000 [i.9] family.

Cybersecurity measures are meant to mitigate the TSPs' exposure to risks and to the societal and economic impact that an incident would have. When establishing cybersecurity risk-management measures the following are to be taken into account, such as:

- the criticality of the entity;
- the risks, including societal risks, to which it is exposed;
- the entity's size; and
- the likelihood of occurrence of incidents and their severity, including their societal and economic impact.

According to the Recital 93 of the NIS2 Directive [i.2] the cybersecurity obligations laid down in the NIS2 Directive "should be considered to be complementary to the requirements imposed on trust service providers" under eIDAS Regulation [i.4].

5.4.2 Cyber hygiene policies, cybersecurity awareness, and innovative technology

NIS2 Directive [i.2] requires that cyber hygiene policies be established in order to protect network and information system infrastructures, hardware, software and online applications, as well as business or end-user data. These policies include common baseline practices such as software and hardware updates, password changes, the management of new installs, the limitation of administrator-level access accounts, and the backing-up of data. ENISA is entitled to monitor and analyse Member States' cyber hygiene policies, as well as efforts to raise awareness of risks related to connected devices. Additionally, Article 21.2.g) NIS2 Directive sets outs TSPs obligations to adopt a wide range of basic cyber hygiene practices, such as:

- zero-trust principles;
- software updates;
- device configuration;
- network segmentation;
- identity and access management or user awareness;
- organise training for their staff and raise awareness concerning cyber threats, phishing or social engineering techniques.

5.4.3 Supply chain

As sets out in NIS2 Directive [i.2]: *"Addressing risks stemming from an entity's supply chain and its relationship with its suppliers, such as providers of data storage and processing services or managed security service providers and software editors, is particularly important given the prevalence of incidents where entities have been the victim of cyberattacks and where malicious perpetrators were able to compromise the security of an entity's network and information systems by exploiting vulnerabilities affecting third-party products and services. Essential and important entities should therefore assess and take into account the overall quality and resilience of products and services, the cybersecurity risk-management measures embedded in them, and the cybersecurity practices of their suppliers and service providers, including their secure development procedures. Essential and important entities should in particular be encouraged to incorporate cybersecurity risk-management measures into contractual arrangements with their direct suppliers and service providers. Those entities could consider risks stemming from other levels of suppliers and service providers*" (recital 85).

Supply chain security controls, including security-related aspects concerning the relationships between each entity and its direct suppliers or service providers, is partially covered by ETSI EN 319 401 [i.7] in areas such as "overall responsibility of TSP", "outsourcer's liability", "contractual relationship" "interface of third party components", or "trustworthy systems and products". However, its provision it is not sufficient and need to be developed.

Under the NIS2 Directive, TSPs' have to make sure that their cooperation with academic and research institutions takes place in line with their cybersecurity policies and follows good practices as regards secure access and dissemination of information in general and the protection of intellectual property in particular. Similarly, given the importance and value of data, third parties providing services on data transformation and data analytics to TSPs' are subject to the appropriate cybersecurity measures.

References to be taking into account:

- ISO/IEC 27002:2022 [i.6], sections 5.19 to 5.22
- MITRE: https://www.mitre.org/news-insights/news-release/mitres-new-system-trust-protects-vulnerable-supply-chains
- NSA: https://www.nsa.gov/About/Cybersecurity-Collaboration-Center/Cybersecurity-Partnerships/ESF/
- NIST: https://csrc.nist.gov/Projects/cyber-supply-chain-risk-management/publications

5.5 Supervision

NIS2 Directive [i.2] proposes in Recital 94 that Member States assign the role of the competent NIS2 authorities for TSPs "to the supervisory bodies under eIDAS Regulation in order to ensure the continuation of current practices and to build on the knowledge and experience gained in the application of that Regulation". In such a case, close cooperation is expected between both supervisory authorities, by exchanging relevant information in order to ensure effective supervision and compliance of TSPs with the NIS2 and eIDAS2 requirements.

6 TSPs' NIS2 Cybersecurity obligations

6.1 Analysis of NIS2 vs ETSI EN 319 401 controls

Much of ETSI EN 319 401 [i.7] is based around general requirements for information security management such as specified in ISO 27002:2013 [i.5]. Many of the concepts and security controls defined for information security are also applicable to the wider concept of cybersecurity.

NIS2 Directive requires management bodies of essential and important entities to approve the cybersecurity risk management measures taken by those entities, oversee its implementation and holding them accountable for the non-compliance. This is already well address in ISO 27002:2013 [i.5] and associated standards for information security management.

Article 21, on its side, requires Member States to ensure that essential and important entities take appropriate and proportionate technical and organisational measures to manage the risks posed to the security of network, and information systems which those entities use in the provision of their services. This is already well address in ISO 27002:2013 [i.5] and other associated standards for information security management.

Table 1 analyses the requirements from the NIS2 Directive and the degree to which they are addressed by existing requirements in ETSI EN 319 401 [i.7].

Table 1

Domain	Sub-domains	NIS2 Directive	ETSI EN 319 401 [i.7]	NIS2 Requirement met by ETSI EN 319 401 [i.7]
Risk analysis		21.2. a) risk analysis	5 Risk Assessment	The risk analysis requirement is included with non-normative reference to ISO/IEC 27005 [i.8]. It needs further work in NWI that has to be risk oriented
Information system security policies		21.2. a) information system security policies	6.3 Information security policy	Fully
ISMS policies and procedures		21.2. f) policies and procedures to assess the effectiveness of cybersecurity risk management measures	Controls and policies included in clause 7. Need to link clause 6 with the controls and procedures of clause 7. The legal provision also reflects the need to review risk assessment and policies on a regular basis	Need to provide cross links separate requirements in ETSI EN 319 401 [i.7]
Internal organization	Organization reliability		7.1.1 Organization reliability	Additional to NIS2
	Segregation of duties		7.1.2 Segregation of duties	Additional to NIS2
Human resources	General	21.2 (i) human resources security, access control policies and asset management	7.2 Human resources	Fully
	Training and awareness	21.2. (g) basic cyber hygiene practices and cybersecurity training;	REQ-7.2-02, REQ-7.2-03, REQ-7.2-04, REQ-7.2-13	Fully
Asset management	General requirements	21.2. (e) security in information systems acquisition, development and maintenance, including vulnerability handling and disclosure 21.2 (i) …asset management	7.3.1 General requirements	Fully
	Media handling		7.3.2 Media handling	Additional to NIS2
Vulnerability management		21.2. (e) security in information systems acquisition, development and maintenance, including vulnerability handling and disclosure	Included but not as a specific topic	Need to provide cross links to separate requirements in ETSI EN 319 401 [i.7]

Domain	Sub-domains	NIS2 Directive	ETSI EN 319 401 [i.7]	NIS2 Requirement met by ETSI EN 319 401 [i.7]
Access control		21.2 (i) …. access control policies...; 21.2. (j) the use of multi-factor authentication or continuous authentication solutions, secured voice, video and text communications and secured emergency communications systems within the entity, where appropriate	7.4 Access control It is to be notice that this clause does not deal with multi-factor authentication or other specific types of authentication but with more abstract aspects of access management, e.g. the principle of least privilege and controls for the separation of trusted roles. In my opinion, there is a need for additional controls in the standard	Need development
	System and application access control		Included but not as a specific topic	Need to provide cross links to separate requirements in ETSI EN 319 401 [i.7]
Cryptographic controls		21.2. (g) policies and procedures regarding the use of cryptography and, where appropriate, encryption	7.5 Cryptographic controls	Fully
Physical and environmental security		See recital 93 "Such cybersecurity and reporting obligations should also concern the physical protection of the services provided" Not specifically included, see 21.2. f)	7.6 Physical and environmental security	Included
Supply chain		21.2. (d) supply chain security including security-related aspects concerning the relationships between each entity and its direct suppliers or service providers	REQ-6.3-05 REQ-6.3-06 REQ-7.1.1-07 REQ-7.1.1-08 REQ-7.1.1-09 REQ-7.7-01	Partially
Operation security			7.7 Operation security	Additional to NIS2
Network security		21.2. (e) security in network	7.8 Network security REQ-7.9-07, REQ-7.9-10, REQ-7.9-11 REQ-7.11-02 information systems acquisition REQ-7.7-01 REQ-7.7-02 REQ-7.7-03 REQ-7.7-04 REQ-7.7-05 REQ-7.7-08 REQ-7.7-09	Fully
Incident management		21.2. (b) incident handling	7.9 Incident management	Fully
	Reporting	Under NIS2 (CERT) and eIDAS regulation Recital 48a NIS2 Directive Article 24 eIDAS Regulation	Included but not as a specific topic	Need to provide cross links to separate requirements in ETSI EN 319 401 [i.7]
Collection of evidence			7.10 Collection of evidence	Additional to NIS2

Domain	Sub-domains	NIS2 Directive	ETSI EN 319 401 [i.7]	NIS2 Requirement met by ETSI EN 319 401 [i.7]
Business continuity management		21.2. (c) business continuity, such as backup management and disaster recovery, and crisis management	7.11 Business continuity management	Fully
Compliance			7.13 Compliance	Additional to NIS2

6.2 ETSI EN 319 401 and ISO/IEC 27002 control mapping

As described in clause 6.1 many of the ETSI EN 319 401 requirements build on ISO/IEC 27002:2013 requirements. When revising ETSI EN 319 401 [i.7] this use of ISO/IEC 27002:2013 control will need to be updated to reference the new organisation of information system management controls in ISO/IEC 27002:2022 as illustrated in table 2.

Table 2

ETSI EN 319 401 [i.7]	ISO/IEC 27002:2013 [i.5] references in ETSI EN 319 401 [i.7]	ISO/IEC 27002:2022 [i.6] Information security, cybersecurity and privacy protection - Information security controls
5 Risk Assessment		
6.3 Information security policy	Clause 5.1.1	5.1 Policies for information security
Controls and policies included in clause 7. Need to link clause 6 with the controls and procedures of clause 7		
7.1.1 Organization reliability		5.2 Information security roles and responsibilities
7.1.2 Segregation of duties		5.3 Segregation of duties
7.2 Human resources	Clauses 6.1.1, 6.1.2 Clauses 7, 7.2.1, 7.2.3	5.4 Management responsibilities; 6.1 Screening 6.2 Terms and conditions of employment 6.3 Information security awareness, education and training 6.4 Disciplinary process 6.5 Responsibilities after termination or change of employment 6.6 Confidentiality or non-disclosure agreements 6.7 Remote working
REQ-7.2-02, REQ-7.2-03, REQ-7.2-04, REQ-7.2-13		6.3 Information security awareness, education and training
7.3.1 General requirements	Clauses 8, 8.1.1	5.9 Inventory of information and other associated assets 5.10 Acceptable use of information and other associated assets 5.11 Return of assets
7.3.2 Media handling	Clause 8.3	7.10 Storage media
		5.8 Information security in project management 8.26 Application security requirements 8.7 Protection against malware 8.8 Management of technical vulnerabilities 8.9 Configuration management 8.15 Logging 8.16 Monitoring activities 8.17 Clock synchronization 8.18 Use of privileged utility programs 8.19 Installation of software on operational systems
7.4 Access control	Clause 9	5.15 Access control 5.16 Identity management 5.17 Authentication information 5.18 Access rights 8.2 Privileged access rights 8.3 Information access restriction

ETSI EN 319 401 [i.7]	ISO/IEC 27002:2013 [i.5] references in ETSI EN 319 401 [i.7]	ISO/IEC 27002:2022 [i.6] Information security, cybersecurity and privacy protection - Information security controls
		8.4 Access to source code 8.5 Secure authentication 8.18 Use of privileged utility programs
7.5 Cryptographic controls	Clause 10	8.24 Use of cryptography
7.6 Physical and environmental security	Clauses 11, 11.1	7.1 Physical security perimeters 7.2 Physical entry 7.3 Securing offices, rooms and facilities 7.4 New Physical security monitoring 7.5 Protecting against physical and environmental threats 7.6 Working in secure areas 7.7 Clear desk and clear screen 7.8 Equipment siting and protection 7.9 Security of assets off-premises 8.1 User endpoint devices
Not included		5.19 Information security in supplier relationships 5.20 Addressing information security within supplier agreements 5.21 Managing information security in the ICT supply chain 5.22 Monitoring, review and change management of supplier services 5.23 Information security for use of cloud services
7.7 Operation security	Clauses 12, 14, 15	5.37 Documented operating procedures 8.6 Capacity management 8.31 Separation of development, test and production environments 8.32 Change management
7.8 Network security		8.20 Networks security 8.21 Security of network services 8.22 Segregation of networks 8.23 Web filtering
7.9 Incident management	Clause 16	5.24 Information security incident management planning and preparation 5.25 Assessment and decision on information security events 5.26 Response to information security incidents 5.27 Learning from information security incidents 5.28 Collection of evidence 6.8 Information security event reporting
7.10 Collection of evidence		5.28 Collection of evidence
7.11 Business continuity management	Clause 17	8.13 Information backup 5.29 Information security during disruption 5.29 Information security during disruption 5.30 ICT readiness for business continuity
7.13 Compliance		5.31 Legislation, regulations and statutory and contractual requirements 5.32 Intellectual property rights 5.33 Protection of records 5.34 Privacy and protection of PII 5.35 Independent review of information security

7 Methodology in Aligning ETSI Standards with NIS2

There are many existing ETSI standards for trust services that use ETSI EN 319 401 [i.7] referencing specific clauses for particular aspects of information security management based around ISO/IEC 27002:2013 [i.5]. As far as possible the structure and existing content of ETSI EN 319 401 [i.7] will be maintained thereby minimising the impact on other standards referencing ETSI EN 319 401 [i.7]. Thus, rather than changing the structure of ETSI EN 319 401 [i.7] to match the topics of NIS2, a mapping table will be provided, probably in an annex, to map the NIS2 requirements to ETSI EN 319 401 [i.7] clauses based around the table 1 provided in clause 6.1. Where there new requirements, such as for as supply chain, these will placed wherever possible within the existing ETSI EN 319 401 [i.7] clause structure.

Unless absolutely essential, existing trust service standards will not be changed on the assumption that the additional requirements included in ETSI EN 319 401 [i.7] can be applied through the existing ETSI EN 319 401 [i.7] references. If additional requirements are necessary not linked existing clauses referenced from the other trust service standards these will be clearly identified in ETSI EN 319 401 [i.7] as additional requirements to be applied to standards referencing ETSI EN 319 401 [i.7] when requiring compliance to NIS2.

History

Document history		
V1.1.1	February 2023	Publication