ETSI GR ETI 006 V1.1.1 (2022-10)

Encrypted Traffic Integration (ETI); Implementation of the EU Council Resolution on Encryption

Disclaimer

The present document has been produced and approved by the Encrypted Traffic Integration (ETI) ETSI Industry Specification Group (ISG) and represents the views of those members who participated in this ISG.
It does not necessarily represent the views of the entire ETSI membership.

Reference
DGR/ETI-006

Keywords
cyber security, encryption

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 Group Report (GR) has been produced by ETSI Industry Specification Group (ISG) Encrypted Traffic Integration (ETI).

Modal verbs terminology

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

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

Executive summary

The EU Council Resolution on Encryption recognizes the complexity of the technology's application in ICT networks and the variety of needs it services. While in most circumstances, encryption of usefully enhances user security and privacy, it can also be used for an array of network harms and criminal purposes that requires visibility for both operational and law enforcement purposes.

The European Union has subsequently reflected these diverse needs in the European Parliament and of the Council on measures for a high common level of security of network and information systems across the Union (NIS_2 Directive) and other related enactments.

Introduction

On 14 December 2020, the Council of the EU adopted a new Resolution - through encryption and security despite encryption. The adoption represents the most significant statement of the EU on encrypted traffic integration - culminating drafting work begun in August 2020 with precursors going back many years. See Annex A. The action is especially relevant to ETSI because the Council undertook the action pursuant to 1-2 October 2020 (EUCO 13/20), asserting that "the EU will leverage its tools and regulatory powers to help shape global rules and standards". This contribution analyses the Resolution - especially examining what problems it missed - together with related additional EU actions, and provides guidance to support implementation.

Citing from the Resolution, the EU press release notes:

> *"Law enforcement authorities and the judiciary are increasingly dependent on access to electronic evidence to effectively fight terrorism, organized crime, child sexual abuse, and a range of other cybercrime and cyber-enabled crimes. Such access is essential to the success of law enforcement and criminal justice in cyberspace. However, there are instances where encryption renders access to and analysis of evidence extremely challenging or impossible in practice"* [i.1].

> *"The EU is striving to establish an active discussion with the technology industry, and with close involvement from research, academia, industry, civil society and other stakeholders, so as to strike the right balance between ensuring the continued use of strong encryption technology and guaranteeing the powers of law enforcement and the judiciary to operate on the same terms as in the offline world. Potential technical solutions will need to respect privacy and fundamental rights, and preserve the value that technological progress brings to society"* [i.2].

During the extensive Resolution legislation drafting and review period, on 11 May 2020, the European Commission laid down rules to prevent and combat child and sexual abuse by requiring tech companies to scan private messages for Child Sexual Abuse Material (CSAM) [i.15].

Following adoption of the Resolution, the EU Voluntary chatcontrol regulation was adopted on 6 July 2021 [i.16].
On 13 May 2022, to respond to the growing threats posed with digitalisation and the surge in cyber-attacks, the final version of the revised NIS Directive was agreed by the EU Parliament and Council [i.17]. During the months preceding its adoption, a significant set of Encryption Resolution related provisions were inserted in the Preamble, and two of the NIS_2 Articles - dealing with national cybersecurity strategy and cybersecurity risk management measures - were included. The first requires Member States adopt policies related to ICT products and services in public procurement on encryption requirements and the use of open-source cybersecurity products. The second requires Member States ensure essential and important entities take appropriate and proportionate technical, operational and organizational measures to manage the risks posed to the security of network and information systems which those entities use for their operations or for the provision of their services, including the policies and procedures regarding the use of cryptography and, where appropriate, encryption.

1 Scope

The present document provides guidance to support implementation of the EU "Council Resolution on Encryption Security through encryption and security despite encryption," adopted 14 December, 2020.

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] EU Council Resolution on Encryption Security through encryption and security despite encryption, adopted 14 December 2020.

NOTE: Available at https://data.consilium.europa.eu/doc/document/ST-13084-2020-REV-1/en/pdf.

[i.2] European Council, Press Release: "Encryption: Council adopts resolution on security through encryption and security despite encryption", 14 December 2020.

NOTE: Available at https://www.consilium.europa.eu/en/press/press-releases/2020/12/14/encryption-council-adopts-resolution-on-security-through-encryption-and-security-despite-encryption/.

[i.3] EU COM(2020) 823 Final, 2020/0359 (COD): "Proposal for a Directive of the European Parliament and of the Council on measures for a high common level of cybersecurity across the Union, repealing Directive (EU) 2016/1148", Brussels, 16 December 2020.

NOTE: Available at https://eur-lex.europa.eu/resource.html?uri=cellar:be0b5038-3fa8-11eb-b27b-01aa75ed71a1.0001.02/DOC_1&format=PDF.

[i.4] U.S. Office of the Director of National Intelligence (ODNI): "Going Dark: Impact to intelligence and law enforcement and threat mitigation" (2017).

[i.5] IETF RFC 8404: "Effects of Pervasive Encryption on Operators".

[i.6] The SolarWinds Orion Hack: "The Basics You Need to Know", Foley Hoag LLP - Security, Privacy and the Law, JDSupra.

[i.7] Jordan Robertson and Michael Riley: "The Long Hack: How China Exploited a U.S. Tech Supplier", 12 February 2021.

[i.8] Additional Protocol to the Convention on Cybercrime, concerning the criminalisation of acts of a racist and xenophobic nature committed through computer systems.

[i.9] United Nations activity to fight racism.

NOTE: Available at https://www.un.org/en/fight-racism.

[i.10] ETSI TR 103 421: "CYBER; Network Gateway Cyber Defence".

[i.11] ETSI TS 103 523-1: "CYBER; Middlebox Security Protocol; Part 1: MSP Framework and Template Requirements".

[i.12] ETSI TS 103 523-2: "CYBER; Middlebox Security Protocol; Part 2: Transport layer MSP, profile for fine grained access control".

[i.13] ETSI TS 103 523-3: "CYBER; Middlebox Security Protocol; Part 3: Enterprise Transport Security".

[i.14] ETSI TS 103 523-5: "CYBER; Middlebox Security Protocol; Part 5: Enterprise Network Security".

[i.15] COM/2022/209 final: "Proposal for a Regulation of the European Parliament and of the Council laying down rules to prevent and combat child sexual abuse".

NOTE: Available at https://ec.europa.eu/home-affairs/proposal-regulation-laying-down-rules-prevent-and-combat-child-sexual-abuse_en.

[i.16] Regulation (EU) 2021/1232 of the European Parliament and of the Council of 14 July 2021 on a temporary derogation from certain provisions of Directive 2002/58/EC as regards the use of technologies by providers of number-independent interpersonal communications services for the processing of personal and other data for the purpose of combating online child sexual abuse.

NOTE: Available at https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32021R1232&from=PT.

[i.17] The NIS_2 Directive: "A high common level of cybersecurity in the EU".

NOTE: Available at https://www.europarl.europa.eu/thinktank/en/document/EPRS_BRI(2021)689333.

3 Definition of terms, symbols and abbreviations

3.1 Terms

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

going dark: inability for service operators or law enforcement officials to access or otherwise know required content of communication

3.2 Symbols

Void.

3.3 Abbreviations

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

5G	5th Generation (of mobile network technology)
AI	Artificial Intelligence
CATS	Community Alarm Telephone Services
CSAM	Child Sexual Abuse Material
CSIRT	Computer Security Incident Response Team
DNS	Domain Name System
ESI	Electronic Signatures and Infrastructures
ETI	Encrypted Traffic Integration
EU	European Union
ICT	Information and Computer Technology
IP	Internet Protocol
ISG	Industry Specification Group
LI	Lawful Interception

MSP	Middlebox Security Protocol
NFV	Network Functions Virtualisation
NIS	Network and Information Security
NIS_2	Network and Information Security 2nd edition
SAGE	Security Algorithm Group of Experts (ETSI specialist group)
SEC	SECurity
SPOC	Single Point of Contact
TC	Technical Committee
TLS	Transport Layer Security
UN	United Nations
URL	Uniform Resource Locator

4 The EU Resolution

4.1 Legislative History

The origins and legislative history underpinning the Resolution emerged in August 2020. Annex A provides the history of the present document sequence. The September note from the Council presidency mentions the inception of discussions in 2016 that were carried forward over the next four years "*in order to identify solutions that struck a balance between individual rights/citizens' security and privacy and allowing law enforcement agencies to do their work*".

This dialogue led to a consultation process and meetings from September until 24 November 2020 during which the text of the resolution was perfected. That text was circulated for approval among Council members - which occurred on 14 December and a press release was issued [i.2].

4.2 Critical challenges treated

The Resolution appropriately notes at the outset that "*encryption is a necessary means of protecting fundamental rights and the digital security of governments, industry and society*". However, it then also recognizes that encryption creates difficulties in enabling "*law enforcement and judicial authorities to exercise their lawful powers, both online and offline protecting our societies and citizens*". It also notes that "*criminals can include readily available, off-the-shelf encryption solutions designed for legitimate purposes in their modi operandi*". The referenced encryption solutions increasingly include ever more sophisticated techniques for pervasive promiscuous encryption whose collective effects are known as *Going Dark* [i.4].

Unfortunately, the Resolution's concept of the encryption ecosystem and the associated problems evidences a very constrained treatment of the subject - focusing only on the adverse effects on law enforcement and judicial authorities. The Resolution also makes statements like "*encryption is an anchor of confidence in digitalisation and in protection of fundamental rights and should be promoted and developed*" and "*it is evident that all parties benefit from encryption technology*". It then paints the problems as only those of law enforcement, when in fact there are a vast array of *Going Dark* problems, and many parties and business and legal systems are seriously impeded if not devastated by some encryption technology implementations.

The Resolution is a start at recognizing the "*downsides*" of encryption technology, and that now "*strives to establish an active discussion with the technology industry*". However, more than just "*competent authorities must be able to get access to data in a lawful and targeted manner*". The full array of stakeholder parties pursuant to multiple compliance obligations and essential network operations need be able to avoid *Going Dark* and get access as well. The "*regulatory framework*" called for in the Resolution is actually a broad legal framework for compliance obligations that includes requirements imposed on parties to network communication arising from: governmental and intergovernmental agreements, statutory or regulatory provisions or directives; judicial decisions, rules and orders; contractual obligations among providers or users; and from legal exposure to tort claims.

The Resolution does recognize a broader array of stakeholders by calling for "*possible solutions…developed in a transparent manner in cooperation with national and international communication service providers and other relevant stakeholders [through] technical solutions and standards*". Action is also called for through the efforts of EU Member States and "*…institutions and bodies*" for "*defining and establishing innovative approaches in view of new technologies; [and] analysing appropriate technical and operational solutions…*".

The Resolution maps closely to the Terms of Reference of the ETI ISG as well as additional activity in TC CYBER. As the designated EU standards body for addressing this subject matter, ETSI should undertake responsive work and establish a continuing, close collaborative relationship that is recognized and relied upon by the EU Council in implementing the Resolution. A start is providing insight into the critical problems missed as well as the innovative Middlebox Security Protocol (MSP) specifications that balance the compliance requirements of the respective stakeholders.

4.3 Pervasive loss of communication network controls

One of the more significant encryption-related developments occurring in the past several years is the so-called pervasive encryption movement which has been manifested in the marketplace to progressively harm the ability of network providers to perform essential operations and meeting an array of compliance responsibilities - especially related to cybersecurity, infrastructure protection, and supply chain security [i.5].

Increasingly, not only communications content, but all manner of signalling and support services like DNS, are being encrypted, and promiscuous techniques such as ephemeral encryption (e.g. TLS 1.3) are being deployed. Network operators - especially those for enterprise networks who implement security at network gateways not only to prevent the distribution of malware and surreptitious remote control of computers, but also for exfiltration of protected information - are going completely dark.

The use of these capabilities has become prominent over the past several years in mounting attacks on election systems and effecting hostile social media-based disinformation campaigns extraterritorially. Over the past several months awareness of the attack capabilities has been extended to facilitating massive enterprise and government monitoring attacks such as the SolarWinds Orion security breach worldwide [i.6]. Even more recently the SuperMicro hack of supply chain hardware platforms in widespread use worldwide - presumably to exfiltrate data - underscores how everyone has become critically dependent on the ability to continuously monitor and analyse network traffic to have any chance at achieving cybersecurity [i.7]. *Going Dark* is one the greatest network communication existential threats today, and getting worse.

Another critical network control that is lost by *Going Dark* is the ability for networks to support their National Security/Emergency Preparedness and public safety obligations that require the ability to prioritize or restrict network resource access and use during national or local emergencies. During any manner of emergencies arising from natural or other causes, it is necessary for network operators and service providers to implement these capabilities at the peril of the public.

4.4 Pervasive loss of legal controls

In addition to the loss of network controls, an array of legal controls essential to society are also lost through *Going Dark*. Some of these controls in recent years have become significantly more important.

Online Hate Crime. Forty-two nations are signatories to the Online Hate Crime Protocol [i.8]. The Protocol has its origins both in the European Commission against Racism and Intolerance, but also the UN Convention that and follows from the domestic laws of many countries. There are also related UN instruments and initiatives that have existed for more than a half century [i.9]. Although in the past, those treaty-based legal obligations and initiatives have been subordinated or ignored, the speed and nation-threatening effects of on-line hate are producing realization that corrective actions are necessary. Much of this activity has significantly aided by encryption technologies, and *Going Dark* presents significant challenges in meeting international and regional legal obligations.

Domestic terrorism. Domestic terrorism is some prominent countries has grown to constitute the primary national existential threat and are ripping at the fabric of democracy [i.9]. In large measure, such domestic terrorism activities are scaled and coordinated using so-called Over-the-Top encrypted messaging services. *Going Dark* significantly exacerbates the challenges faced by authorities to monitor these activities and prevent major attacks on government infrastructure, activities, and personnel.

Intellectual property theft. One of the known principal uses of *Going Dark* technologies and platforms is the unauthorized distribution of copyrighted material. This material includes both audio and multimedia productions, as well as software - often with embedded malware. Some recent encryption platforms have even been optimized to facilitate such activity.

eDiscovery. As the evidence in civil litigation has become increasingly manifested in digital form in recent decades, the judicial systems in many countries have established mandatory rules for discovery and availability. The requirements and standards are collectively referred to as eDiscovery. *Going Dark* technologies significantly impair the ability of the parties to eDiscovery to meet their rights and obligations, as well as the juridical systems that rely on them.

Tort liability. In many countries, tort liability is an essential component of juridical systems in bringing about acceptable societal conduct and penalizing wrongdoers for their conduct which harms third parties. It is related to eDiscovery requirements. In some countries, the providers of *Going Dark* products and services have indirectly received grants of tort immunity (known in the U.S. as Sec. 230 protection) as a secondary consequence of legacy law intended to encourage on-line services, and the protection is now being eliminated. The ability to impose tort liability as a legal control should not be lost as a consequence of *Going Dark*.

Trusted identity. The quest to achieve *Going Dark* has driven a vast market for free, zero cost, Let's Encrypt™ including those digital certificates that only identify the hosting website, but which unbeknownst to the user at the other end, provide no trust in the entity responsible for the site. The certificates are "untrusted" by design solely for the purpose of *Going Dark*. The result has devastated the X.509 trusted identity marketplace.

antitrust enforcement. Because *Going Dark* technologies and services are typically implemented through network and application platforms such as browsers that are widely deployed, those technologies can be leveraged in the marketplace achieve and leverage unlawful marketplace dominance. In other words, *Going Dark* significantly impairs enforcement of antitrust controls. The removal of governmental oversight and regulation of the trusted identity industry described above, has enabled widespread anticompetitive behaviour.

4.5 Exacerbating effects of virtualisation and 5G

One of the most significant paradigms in the history of electronic communication technology is now unfolding. It is represented in the ubiquitous deployment of virtualised architectures, services, protocols, and devices that are instantiated on demand from cloud data centres worldwide, and known as Network Functions Virtualisation (NFV). The marketplace drivers are multiple 5G manifestations: radio, fixed, cable, and satellite.

In this new virtualisation ecosystem, security is not possible with pervasive promiscuous encryption because continuous monitoring is the only means to mitigate the threat. Cybersecurity in this ecosystem necessitates thorough vetting of hardware compliance with rigorous trust requirements prior to service in the infrastructure. However, as all the subsequent functionality is manifested by NFV software scripts that are run by the device, continuous monitoring of its behaviours and signatures is essential. Enabling and allowing promiscuous encryption communication to and from the device or its orchestrations creates fundamental unacceptable risk. In a virtualisation world, *Going Dark* is the ultimate cybersecurity peril from which there is no escape. The EU Resolution inexplicably seems to ignore this critically important reality.

4.6 Middlebox Security Protocols

For the past four years, ETSI TC CYBER has been engaged with the assistance of cybersecurity experts in industry, the academic community, and government in identifying best-of-breed solutions to the tension between the desirable attributes of encrypted communication and inherent risks posed. The work on middlebox security protocols in ETSI TC CYBER began with an extensive study of the cybersecurity requirements at network gateways that included a survey of all the discoverable research and development activity underway, and similar work occurring in other industry bodies [i.10].

The acquired knowledge base from the initial work was then used to create a set of Middlebox Security Protocol (MSP) Technical specifications that enable users and network service providers to provide an effective balance of the privacy, compliance, and security requirements. The various specification parts include:

1) a generic MSP requirements and threat model [i.11];

2) a transport layer protocol controlled jointly by the end user and network operator [i.12];

3) a transport layer protocol controlled by an enterprise network operator [i.13]; and

4) a network layer protocol controlled an enterprise network operator [i.14].

The solutions have been the subject of hackathons and running code made available by ETSI. Global network object identifiers and common names were acquired for the specifications. Collaboration has been underway with industry user communities - especially global financial institutions who have a critical need. Further improvements and extensions are also being planned for the constantly evolving challenges of encryption technology represented by the EU Resolution.

4.7 ETSI Responsive Actions

As both a global leader as well as the European Union's principal designated standards body in the sector, ETSI has for decades served as the repository for expertise and developer of industry encryption specifications. ETSI's responsive actions are manifested though ongoing work in several Technical Committees and Industry Specification Groups, as well as continuing collaboration with other relevant standards bodies and expert communities.

The principal relevant ETSI groups are TCs CYBER, ESI, LI, and SAGE, and ISGs ETI and NFV SEC. The EU Resolution calls for three actions for which ETSI is not only highly competent and has ongoing work for two of them, but is also the principal body within the EU. For the third action relating to a regulatory framework, ETSI can play an important collaborative role - as it has done for many security Directives.

a) defining and establishing innovative approaches in view of new technologies;

b) analysing appropriate technical and operational solutions; and

c) develop a regulatory framework across the EU that would allow competent authorities to carry out their operational tasks effectively while protecting privacy.

The next needed steps are for the ETSI groups either individually or collectively identifying appropriate EU body contacts for implementing the Resolution - conveying existing relevant work and an intent to assist them as the development of ETSI's responsive actions moves forward.

4.8 Guidance

The clauses above provide an enumeration of guidance activities within ETSI that support implementation of the EU "Council Resolution on Encryption Security through encryption and security despite encryption". The clauses below provide guidance emerging from actions being taken by EU institutions which also support implementation of the Resolution. The most important of the EU actions is NIS_2 - for which ETSI groups will continue work to support.

5 Related EU actions

5.1 EU Proposal laying down rules to prevent and combat Child Sexual Abuse Material (CSAM)

On 11 May 2020, the European Commission laid down rules to prevent and combat child and sexual abuse by requiring tech companies to scan private messages for Child Sexual Abuse Material (CSAM) and evidence of grooming, even when those messages are supposed to be protected by end-to-end encryption [i.15]. Online services that receive detection orders under the proposed regulation would have "obligations concerning the detection, reporting, removal and blocking of known and new child sexual abuse material, as well as solicitation of children, regardless of the technology used in the online exchanges". Mirroring the Resolution on Encryption, the proposal notes that although end-to-end encryption is an important security tool, providers are not to allow encryption to be used to enable child sexual abuse.

In order to ensure the effectiveness of those measures, allow for tailored solutions, remain technologically neutral, and avoid circumvention of the detection obligations, those measures should be taken regardless of the technologies used by the providers concerned in connection to the provision of their services. Therefore, this Regulation leaves to the provider concerned the choice of the technologies to be operated to comply effectively with detection orders and should not be understood as incentivising or disincentivising the use of any given technology, provided that the technologies and accompanying measures meet the requirements of this Regulation.

That includes the use of end-to-end encryption technology, which is an important tool to guarantee the security and confidentiality of the communications of users, including those of children. When executing the detection order, providers should take all available safeguard measures to ensure that the technologies employed by them cannot be used by them or their employees for purposes other than compliance with this Regulation, nor by third parties, and thus to avoid undermining the security and confidentiality of the communications of users.

5.2 EU Voluntary chatcontrol regulation

On 6 July 2021, Members of the European Parliament approved the ePrivacy Derogation, allowing providers of e-mail and messaging services to automatically search all personal messages of each citizen for presumed suspect content and report suspected cases to the police [i.16].

Envisaged are chat control, network blocking, mandatory age verification for communication and storage apps, age verification for app stores and exclusion of minors from installing many apps. The communication services affected include telephony, e-mail, messenger, chats (also as part of games, on part of games, on dating portals, etc.), videoconferencing. End-to-end encrypted messenger services are not excluded from the scope. Hosting, services affected include web hosting, social media, video streaming services, file hosting and cloud services.

5.3 NIS_2 Directive

On 16 June 2020, the European Parliament provided a briefing on the agreement between Parliament and the Council on NIS_2 Directive [i.3] that was reached on 13 May 2022 [i.17]. To respond to the growing threats posed with digitalisation and the surge in cyber-attacks, the revised NIS Directive strengthens the security requirements, address the security of supply chains, streamline reporting obligations, and introduce more stringent supervisory measures and stricter enforcement requirements, including harmonised sanctions across the EU. The proposed expansion of the scope covered by NIS_2, by effectively obliging more entities and sectors to take measures, would assist in increasing the level of cybersecurity in Europe in the longer term. The Council Resolution on Encryption was reflected in numerous provisions in the preamble and provisions.

Preamble

*"**(26c) Member States should encourage the use of any innovative technology, including artificial intelligence (AI), the use of which could improve the detection and prevention of attacks against network and information systems, enabling resources to be diverted towards cyber attacks more effectively. Member States should therefore encourage in their national strategies activities in research and development to facilitate the use of such technologies, in particular relating to (semi-)automated tools in cybersecurity and where relevant the sharing of data needed to train and improve them. The use of any innovative technology, including artificial intelligence (AI) should be used in full respect of EU data protection law, including on the data protection principles of data accuracy, data minimisation, fairness and transparency, data security, such as state-of-the-art encryption. The requirements of data protection by design and by default laid down in Regulation (EU) 2016/679 should be fully exploited.***

*(53) Providers of public electronic communications networks or publicly available electronic communications services, should **implement security by design and by default, and** inform the service recipients of particular and significant cyber threats and of measures they can take to protect the security of their **devices and** communications, for instance by using specific types of software or encryption technologies.*

*(54) In order to safeguard the security of electronic communications networks and services, the use of encryption **technologies**, in particular end-to-end encryption **as well as data-centric security concepts, such as cartography, segmentation, tagging, access policy and access management, and automated access decisions**, should be promoted**.** Where necessary, **the use of encryption and in particular end-to-end encryption** should be mandatory for **the** providers of **electronic communications networks and** services in accordance with the principles of security and privacy by default and by design for the purposes of Article 18. The use of end-to-end encryption should be reconciled with the Member States' powers to ensure the protection of their essential security interests and public security, and to permit the investigation, detection and prosecution of criminal offences in compliance with Union law. **However, this should not weaken** end-to-end encryption**, which is a critical technology for effective data protection and** privacy and security of communications.*

(69) The processing of personal data, to the extent strictly necessary and proportionate for the purposes of ensuring network and information security by ***essential and important*** *entities,* ***could be considered legitimate to comply with legal obligation subject to the requirements of Article 6(1)(c) and (3) of Regulation (EU) 2016/679,*** *of the data controller concerned as referred to in Regulation (EU) 2016/679.* ***Processing of personal data might also be necessary for legitimate interests pursued by essential and important entities, as well as providers of security technologies and services acting on behalf of these entities, pursuant to Article 6(1)(f) of Regulation (EU) 2016/679, including where such processing is necessary for cybersecurity information sharing arrangements or the voluntary notification of relevant information as laid down in this Directive.*** *Measures related to the prevention, detection****, identification, containment****, analysis and response to incidents, measures to raise awareness in relation to specific cyber threats, exchange of information in the context of vulnerability remediation and coordinated disclosure, as well as the voluntary exchange of information on those incidents, as well as cyber threats and vulnerabilities, indicators of compromise, tactics, techniques and procedures, cybersecurity alerts and configuration tools may require the processing of* ***certain categories*** *of personal data****, such as*** *IP addresses, uniform resources locators (URLs), domain names,* ***email addresses, time stamps - where those reveal personal data. Processing of personal data by competent authorities, SPOCs and CSIRTs, could be considered necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the data controller or could constitute a legal obligation, pursuant to Article 6(1) point (c) or (e) and Article 6(3) of Regulation (EU) 2016/679 or for pursuing a legitimate interest of the essential and important entities, as referred to in Article 6(1)(f) of Regulation (EU) 2016. Furthermore, Member States' laws may lay down rules allowing competent authorities, SPOCs and CSIRTs, to the extent that is strictly necessary and proportionate for the purpose of ensuring the security of network and information systems of essential and important entities, to process special categories of personal data in accordance with Article 9 of Regulation (EU) 2016/679, in particular by providing for suitable and specific measures to safeguard the fundamental rights and interests of natural persons, including technical limitations on the re-use of such data and the use of state-of-the-art security and privacy-preserving measures, such as pseudonymisation, or encryption where anonymisation may significantly affect the purpose pursued****.***

(70c) When exercising their supervisory tasks in relation to essential and important entities, competent authorities should ensure that these tasks are conducted by trained professionals. Trained professionals should have the necessary skills to carry out the tasks conferred on competent authorities by this Directive, in particular in regards to conducting on-site and off-site inspections including the identification of weaknesses in databases, hardware, firewalls, encryption and networks. Inspections should be conducted in an objective manner."

NIS_2 Provisions

"Article 5 National cybersecurity strategy

2. As part of the national cybersecurity strategy, Member States shall in particular adopt the following policies:

(a) a policy addressing cybersecurity in the supply chain for ICT products and services used by entities for the provision of their services;

(b) a policy regarding the inclusion and specification of cybersecurity-related requirements for ICT products and services in public procurement, including cybersecurity certification as well as encryption requirements and the use of open-source cybersecurity products;

Article 18 Cybersecurity risk management measures

2. The measures referred to in paragraph 1 shall be based on an all-hazards approach aiming to protect network and information systems and their physical environment from incidents, and shall include at least the following:

(g) policies and procedures regarding the use of cryptography and, where appropriate, encryption;"

Annex A: Bibliography

Council Resolution on Encryption - Proceeding Docket

- CM 5286 2020 INIT - WRITTEN PROCEDURE 14/12/2020
  END OF WRITTEN PROCEDURE Council Resolution on Encryption - Approval.
- CM 5222 2020 INIT - WRITTEN PROCEDURE 09/12/2020
  Council Resolution on Encryption - Approval - Initiation of written procedure.
- ST 13550 2020 INIT - NOTE 01/12/2020
  Recommendations for a way forward on the topic of encryption
  Subject matter: CYBER, IXIM, CATS, JAI, DATAPROTECT, COPEN, ENFOPOL, COSI
  Originator: Presidency
- ST 13084 2020 REV 1 - NOTE 24/11/2020
  Council Resolution on Encryption - Security through encryption and security despite encryption.
- ST 13085 2020 REV 1 - 'I' ITEM NOTE 24/11/2020
  Council Resolution on Encryption.
- ST 13085 2020 INIT - 'I' ITEM NOTE 23/11/2020
  Draft Council Resolution on Encryption.
- ST 13084 2020 INIT - NOTE 20/11/2020
  Draft Council Resolution on Encryption - Security through encryption and security despite encryption.
- ST 12863 2020 INIT - NOTE 16/11/2020
  Draft Council Resolution on Encryption - Security through encryption and security despite encryption.
- ST 12864 2020 INIT - NOTE 16/11/2020
  Recommendations for a way forward on the topic of encryption
  Subject matter: CYBER, IXIM, CATS, JAI, DATAPROTECT, COPEN, ENFOPOL, COSI
  Originator: Presidency
  Date of meeting: 19/11/2020
- ST 12143 2020 REV 1 - NOTE 06/11/2020
  Draft Council Resolution on Encryption - Security through encryption and security despite encryption.
- CM 4195 2020 INIT - NOTICE OF MEETING AND PROVISIONAL AGENDA 29/10/2020
  Informal videoconference of the members of JHA Counsellors (All) (Encryption).
- ST 12143 2020 INIT - NOTE 21/10/2020
  Draft Council Declaration on Encryption - Security through encryption and security despite encryption
- ST 10728 2020 INIT - NOTE 18/09/2020
  Security through encryption and security despite encryption
- ST 10730 2020 INIT - NOTE 18/09/2020
  End-to-end encryption in criminal investigations and prosecution
- ST 7675 2020 ADD 1 - NOTE 08/05/2020
  Law enforcement and judicial aspects of encryption: The various forms of encryption
  Subject matter: CYBER, CT, IXIM, CATS, JAI, ENFOPOL, COSI, TELECOM.
- ST 7675 2020 INIT - NOTE 08/05/2020
  Law enforcement and judicial aspects of encryption
  Subject matter: CYBER, CT, IXIM, CATS, JAI, ENFOPOL, COSI, TELECOM.

History

Document history		
V1.1.1	October 2022	Publication