ETSI TS 104 103 V1.1.1 (2025-09)

TECHNICAL SPECIFICATION

Cyber Security (CYBER);
Encrypted Traffic Integration (ETI);
Problem Statement review and requirements definition

Reference
DTS/CYBER-00140

Keywords
confidentiality, network measurement, network monitoring, network performance

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 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

This Technical Specification (TS) has been produced by ETSI Technical Committee Cyber Security (CYBER).

NOTE1: The present document is an update to ETSI GR ETI 001, merged with ETSI GR ETI 002, created by Industry Specification Group (ISG) Encrypted Traffic Inspection (ETI).

NOTE 2: The numbering of clauses in this edition of the document is intended to retain consistency with the foregoing ETSI GR ETI 001.

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.

1 Scope

The present document identifies and describes the problem arising from pervasive encrypted traffic in electronic/digital communications networks. In addition, the present document states the requirements for allowing Encrypted Traffic Integration (ETI) across an abstracted network architecture. The present document identifies the impact of encrypted traffic on a number of stakeholders and how the stakeholders' objectives work together. The characterization of traffic as either user generated content, user generated signalling, network signalling, and metadata, and the relative impact on stakeholders is considered. The present document also addresses the role of compliance obligations on the development and deployment of encrypted traffic and how it impacts different stakeholders.

The present document addresses the impact of pervasive encryption on stakeholders in order to assist future standards development activity in mitigating the negative impact on stakeholders whilst not adversely impacting the positive impacts of such a paradigm on stakeholders, including the regulatory and lawful dimensions.

The present document is structured as follows:

- Clause 4 outlines the role of encryption as it is being applied to networks from a mainly business perspective.
- Clause 5 outlines and provides a model of the ETI problem.
- Clause 6 presents the ETI model from a technical perspective.
- Clause 7 summarizes the risk of pervasive encryption.
- Clause 8 outlines the requirements for countering risks of pervasive encryption.
- Annex A (normative) provides a summary of the impact of pervasive encryption on various formal compliance obligations.
- Annex B (informative) gives an overview of the various common approaches to provide encryption in networks.
- Annex C (informative) offers a number of examples of the impact of pervasive encryption.
- Annex D (informative) addresses the application of the ETI requirements using the security controls approach.

The present document includes requirements that implement the role of Zero Trust (ZT) and Zero Trust Architecture (ZTA) [1] in ETI, in order to provide an explicitly trusted communications environment across all enabled layers of the Open Systems Interconnection (OSI) model. In addition, the present document describes a ZTA security model, that enforces transparency and explicability of the role of security functions, particularly encryption.

2 References

2.1 Normative 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.

Referenced documents which are not found to be publicly available in the expected location might be found in the ETSI docbox.

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] NIST Special Publication 800-207: "Zero Trust Architecture".

[2] ETSI TS 104 102: "Cyber Security (CYBER); Encrypted Traffic Integration (ETI); ZT-Kipling methodology".

[3] ETSI TS 103 532: "CYBER; Attribute Based Encryption for Attribute Based Access Control".

[4] Recommendation ITU-T X.800: "Security architecture for Open Systems Interconnection for CCITT applications".

[5] ETSI TS 101 331: "Lawful Interception (LI); Requirements of Law Enforcement Agencies".

[6] ETSI TS 102 656: "Lawful Interception (LI); Retained Data; Requirements of Law Enforcement Agencies for handling Retained Data".

[7] ETSI TS 102 165-1: "Cyber Security (CYBER); Methods and protocols; Part 1: Method and pro forma for Threat, Vulnerability, Risk Analysis (TVRA)".

[8] ETSI TS 102 165-2: "Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); Methods and protocols; Part 2: Protocol Framework Definition; Security Counter Measures". .

[9] ETSI TS 104 224: "Securing Artificial Intelligence (SAI); Explicability and transparency of AI processing".

[10] ETSI TS 104 223: "Securing Artificial Intelligence (SAI); Baseline Cyber Security Requirements for AI Models and Systems".

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 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] ISO/IEC 7498-1: "Information technology - Open Systems Interconnection - Basic Reference Model: The Basic Model".

NOTE: The same text is available as Recommendation ITU-T X.200.

[i.2] Directive 2014/53/EU of the European Parliament and of the Council of 16 April 2014 on the harmonisation of the laws of the Member States relating to the making available on the market of radio equipment and repealing Directive 1999/5/EC (Text with EEA relevance) (Radio Equipment Directive).

[i.3] COM/2017/010 final: "Proposal for a Regulation of the European Parliament and of the Council concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications)".

[i.4] Regulation (EU) 1025/2012 of the European Parliament and of the Council of 25 October 2012 on European standardisation, amending Council Directives 89/686/EEC and 93/15/EEC and Directives 94/9/EC, 94/25/EC, 95/16/EC, 97/23/EC, 98/34/EC, 2004/22/EC, 2007/23/EC, 2009/23/EC and 2009/105/EC of the European Parliament and of the Council and repealing Council Decision 87/95/EEC and Decision No 1673/2006/EC of the European Parliament and of the Council Text with EEA relevance.

[i.5] ETSI TR 103 456: "CYBER; Implementation of the Network and Information Security (NIS) Directive".

[i.6] ENISA: "Gaps in NIS standardisation Recommendations for improving NIS in EU standardisation policy" V.1.0, November 2016.

[i.7] ETSI TR 103 618: "CYBER; Quantum-Safe Identity-Based Encryption".

[i.8] ETSI TR 103 719: "Guide to Identity-Based Cryptography".

[i.9] ETSI TS 103 458: "CYBER; Application of Attribute Based Encryption (ABE) for PII and personal data protection on IoT devices, WLAN, cloud and mobile services - High level requirements".

[i.10] ETSI TR 103 369: "CYBER; Design requirements ecosystem".

[i.11] ETSI TR 103 421: "CYBER; Network Gateway Cyber Defence".

[i.12] IETF RFC 8404: "Effects of Pervasive Encryption on Operators".

[i.13] U.S. Office of the Director of National Intelligence (ODNI): "Going Dark: Impact to intelligence and law enforcement and threat mitigation" (2017).

[i.14] Tor project.

[i.15] A. Young, M. Yung: "Cryptovirology: Extortion-Based Security Threats and Countermeasures". IEEE Symposium on Security & Privacy, May 6-8, 1996. pp. 129-141. IEEE Explore: Cryptovirology: extortion-based security threats and countermeasures.

[i.16] ETSI TR 102 661: "Lawful Interception (LI); Security framework in Lawful Interception and Retained Data environment".

[i.17] ETSI TR 103 936: "Cyber Security (CYBER); Implementing Design practices to mitigate consumer IoT-enabled coercive control".

[i.18] ISO 7498-2: "Information processing systems -- Open Systems Interconnection -- Basic Reference Model -- Part 2: Security Architecture".

[i.19] ETSI TR 103 309: "CYBER; Secure by Default - platform security technology".

[i.20] ETSI TS 103 486: "CYBER; Identity Management and Discovery for IoT".

[i.21] GSMA: "FS.37 GTP-U Security".

[i.22] GSMA: "FS.40 5G Security Guide Version 3.0".

[i.23] NIST Special Publication 800-53, Revision 5: "Security and Privacy Controls for Information Systems and Organizations".

[i.24] ETSI TR 104 065: "Securing Artificial Intelligence (SAI); AI Act mapping and gap analysis to ETSI workplan".

[i.25] EN 18031-1: "Common security requirements for radio equipment - Part 1: Internet connected radio equipment" (produced by CEN).

[i.26] EN 18031-2: "Common security requirements for radio equipment - Part 2: radio equipment processing data, namely Internet connected radio equipment, childcare radio equipment, toys radio equipment and wearable radio equipment" (produced by CEN).

[i.27] EN 18031-3: "Common security requirements for radio equipment - Part 3: Internet connected radio equipment processing virtual money or monetary value" (produced by CEN).

[i.28] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation).

[i.29] 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 (NIS Directive).

[i.30] 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).

[i.31] Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence and amending Regulations (EC) No 300/2008, (EU) No 167/2013, (EU) No 168/2013, (EU) 2018/858, (EU) 2018/1139 and (EU) 2019/2144 and Directives 2014/90/EU, (EU) 2016/797 and (EU) 2020/1828 (Artificial Intelligence Act).

[i.32] Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act)".

[i.33] Council of the European Union: "Resolution on Encryption - Security through encryption and security despite encryption" No. 13084/1/20, Brussels, 24 Nov 2020.

[i.34] Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market For Digital Services and amending Directive 2000/31/EC (Digital Services Act).

[i.35] ETSI TS 102 165-3: "Cyber Security (CYBER); Methods and Protocols for Security; Part 3: Vulnerability Assessment extension for TVRA".

3 Definition of terms, symbols and abbreviations

3.1 Terms

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

compliance obligations: requirements imposed on parties to network communication arising from: governmental statutory or regulatory provisions or directives; judicial decisions, rules and orders; contractual obligations among providers or users; and from legal exposure to tort claims

NOTE: As defined in ETSI TR 103 369 [i.10].

encryption: transformation of data by a cryptographic algorithm to produce a ciphertext

Going Dark: phenomenon by which an authorized user lacks the technical or practical ability to access data

NOTE: One result of going dark is the inability of an indirect party to network communication, e.g. the network operator or service provider, to meet a legal requirement or need because of pervasive encryption of the information transmitted or retained.

integrity: property that data has not been altered or destroyed in an unauthorized manner

perfect forward secrecy: property of an encryption system in which inspection of the data exchange that occurs during the key agreement phase of a session does not reveal the key used to encrypt the remainder of the session

NOTE: This definition is slightly at variance to that found in ETSI TR 102 661 [i.16] which, in referring to asymmetric cryptographic keys, states "*property that past confidentiality protected data will not be affected, if all certificates, concerning a specific time period, are revealed to an attacker*" although the general role of a session key to protect only for the associated session does not allow an attacker to infer any knowledge of any key used in any other session holds for both terms.

pervasive encryption: extensive encryption of data communicated "on the wire" or "at-rest" using transient techniques and practices among only a subset of the affected parties

trust: level of confidence in the reliability and integrity of an entity to fulfil specific responsibilities

Zero Trust Architecture (ZTA): cybersecurity model that seeks to eliminate implicit trust

NOTE: In NIST SP 800-207 [1], this term is extended to address the evolving set of cybersecurity paradigms that move defences from static, network-based perimeters to focus on users, assets, and resources.

3.2 Symbols

Void.

3.3 Abbreviations

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

A2ApoA	Application to Application point of Attachment
A2SpoA	Application to Service point of Attachment
ACL	Access Control List
AI	Artificial Intelligence
ApoA	Application point of Attachment
CapEx	Capital Expenditure
CEP	Communication End Point
CIA	Confidentiality Integrity Availability
CI/CD	Continuous Integration/ Continuous Delivery
CSP	Communications Service Provider
DSA	Digital Services Act
E2E	End to End
EDF	Ephemeral Diffie Helman
ENISA	European Network Information Security Agency
ETI	Encrypted Traffic Integration
EU	European Union
GDPR	General Data Protection Regulation
HSM	Hardware Security Module
ICT	Information and Communications Technologies
IoT	Internet of Things
IP	Internet Protocol
LI	Lawful Interception
MAC	Message Authentication Code
NIS	Network and Information Security
NIST	National Institute of Standards and Technology
NoO	Notice of Obligations
OpEx	Operational Expenditure
OS	Operating System
OSI	Open Systems Interconnection
PII	Person Identifying Information
QSC	Quantum Safe Cryptography
RED	Radio Equipment Directive
RTE	Run Time Explicability
S2SpoA	Service to Service point of Attachment
S2TpoA	Service to Transport point of Attachment
SA	Security Association
SAI	Securing Artificial Intelligence
SpoA	Service point of Attachment
T2TpoA	Transport to Transport point of Attachment
TE	Terminal Equipment
TFA	Technology Facilitated Abuse
TpoA	Transport point of Attachment
TVRA	Threat Vulnerability Risk Analysis
UE	User Equipment
VPN	Virtual Private Network
WPA-3	Wi-Fi® Protected Access 3
ZT	Zero Trust
ZTA	Zero Trust Architecture

4 Roles of encryption in networks

The role of encryption of information being transported between two end-points is perceived to have three widely recognized positive purposes depending on the context:

- confidentiality protection of the transferred information or content;
- enhanced trust in the identity of the parties associated with the information or content; and
- enhanced trust in the integrity of the information or content during transport.

The use of encryption as the default approach to enhance the security of communications has become increasingly common. While there are often benefits, in many scenarios the use of encryption as a default security approach exposes users and networks to threats from bad actors and malicious traffic which, if not caught in time by not being recognized as a result of being hidden behind encryption, can no longer be filtered out by the network operator to protect the network and its end users. Use of end-to-end encryption can restrict the ability of network management, anti-fraud, cyber security, and regulatory monitoring systems to manage data and communications flowing into, through, and out of networks. While encryption protects traffic flowing through a network from unauthorized inspection, encryption in itself does not protect the communicating end points from attack and reduces the ability of operators and their network management systems to remove malicious traffic by appropriate use of cybersecurity tools.

NOTE: Protecting privacy is often conflated with providing confidentiality where in practical terms the intersection of the 2 concepts is incomplete. Private information can be stored and transferred confidentiality but may leak from the endpoint

However, encryption may have a negative impact on third parties who do not have access to the encryption keys used and therefore do not have access to the content, but may have operational or legal responsibilities that require, or which are dependent on some level of knowledge of the information transported. Critical factors include how the keys were generated, who has knowledge of them, and how they are protected or shared.

In figurative terms the impact of encryption is to make the content of something obscured or impenetrable to anyone without the key.

EXAMPLE: There are many ways to describe how encryption works and one is to consider the analogy of a locked cabinet. The contents of the cabinet cannot be accessed without using the right key to unlock it. The network problem is that there are many such locked cabinets and the network cannot afford to get them mixed up. The network is also not in possession of the keys to open the cabinets to help them work out what to do with them. So conventionally each locked cabinet is marked on the outside in such a way that the network can identify who they belong to and make sure that Alice receives only her cabinets and Bob receives only his. Networks are somewhat complicated though and the reality is that, like the Russian nesting doll, cabinets are enclosed inside cabinets. In order to move cabinets to the correct destination each cabinet needs to be labelled and distinguished, and if those labels and distinguishing marks are themselves encrypted such that they cannot be easily read then their value is decreased. In the worst case scenario a Russian doll like model is tossed across a network between end points which take the subsequent dolls out of the package, if it is not for them they toss it back into the network.

Encryption is often confused with and used as a shorthand in referring to a number of cryptographic processes. For the purposes of the present document, the following relatively simple meanings are adopted:

- **Encryption** - where data is transformed by a cryptographic algorithm to produce a ciphertext with the intent to hide the information content of the data.
- **Trust** - a trusted network is able to fulfil its obligations, if obligations cannot be fulfilled because of the use of encrypted content, it will become less trusted.
- **Integrity** - in the social or business context integrity is closely aligned to trust that the data and the methods of handling the data cannot be altered or destroyed in an unauthorized manner.

Taking the terms above and the impact of pervasive encryption into account the result is a partial denial of service to the operator. In simple terms the expected trusted relationship of the operator is denied.

Encryption can be accomplished as a service by multiple parties as the information is moved between endpoints. In broad communications network terms, when some parties in the process choose to apply encryption, the other parties are no longer able to trust or view the information transported across the network to endpoints.

Making the operator and other stakeholders explicitly aware of the use and role of encryption, and other security techniques, in the system may allow mitigation of the negative effects of encryption whilst promoting their positive effects. The consequence for the present document is to make all security functions in a network explicit, with the further requirement to ensure that every transaction is made within a bounded set of Security Associations (SAs), while validating legitimacy of the transmitted data, that build to provide an explicit per transaction security model. The security model by being explicit shall then also be considered as making an explicit trust model for each transaction. The initial point shall be that the entire transaction and all the elements and data involved in the transaction are untrusted and insecure. The end point at which the transaction shall take place is that all elements and data in the connection are secured and trusted.

5 Model of ETI problem

The Going Dark challenge in which an authorized user lacks the technical or practical ability to access data has been exaggerated through the increasing use of pervasive encryption of traffic and signalling across networks - usually on an end-to-end basis. The adverse effects on cyber defence as well as a broad array of essential network operator functions are well recognized and documented (see references [i.11], [i.12] and [i.33]). Additionally, pervasive encryption poses significant difficulties for government authorities and imposition of requirements on communication service providers as documented in references [i.13] and [5].

In addition greater liability is being passed to providers of network and telecommunications services to manage access to certain forms of content which is made increasingly difficult if too much is encrypted and hidden from examination. This is addressed in part in Figure 2 with element C.

In the context of the telecommunication environment Going Dark includes the inability of a normally authorized party such as the CSP's network management entity to function because of the encryption by end-point users or third parties. For example, the intersection of the two elements, A, representing network capabilities that, when content and headers are encrypted, pose extreme challenges to network operation, and B, representing Network capabilities that are core to development of cyber/digital business, should be minimized, whilst always seeking to eliminate A (see Figure 1). In addition, the relative scale of B should always be significantly greater than A. See Figure 1.

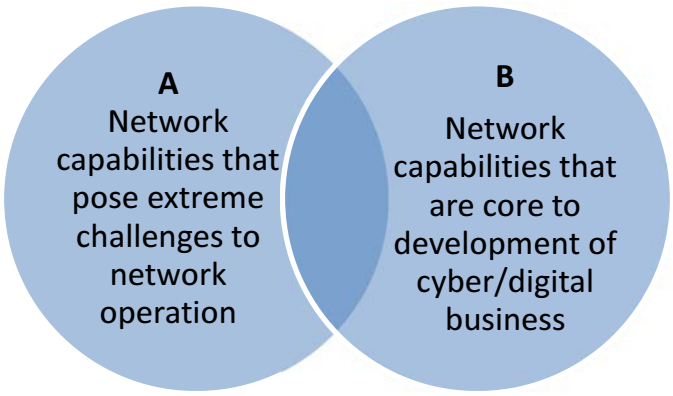


Figure 1: Representation of encrypted content fostering the Going Dark in networks

One consequence of pervasive encryption is that some of the obligations placed on operators and suppliers with respect to regulation, law or convention, or operator security policy, may be difficult to meet. These additional constraints on networks, may be viewed as a third dimension of the simplified Venn Diagram and are shown in Figure 2.

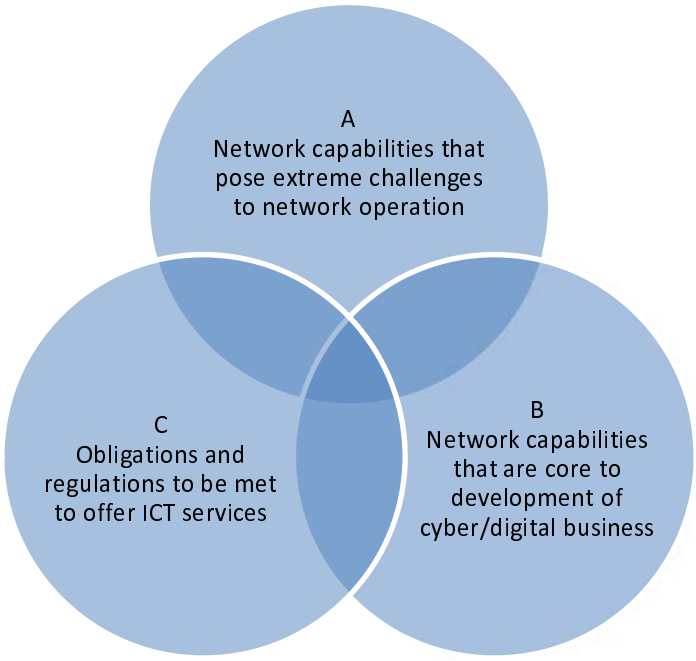


Figure 2: Refinement of the Going Dark by addition of externally imposed obligations

It is recognized that in many cases the content of encrypted data should never be exposed to an ICT operator. Thus, the definition of an authorized user is made with respect to the content and the necessary header information required to transfer that content. It should be assumed that a single authorized entity is unlikely to exist for the entire distribution of data from source to destination, rather it should be assumed that distinct authorized entities exist at each layer of the normal OSI stack. In the scope of the "C" entity from Figure 2 are such things as ensuring the obligations to support Lawful Interception ETSI TS 102 656 [6], ETSI TS 101 331 [5], the GDPR [i.28], obligations under the NIS2 [i.29] directive, the Cyber Resilience Act [i.30], the AI Act [i.31] and the Cyber Security Act [i.32], and any national or regional requirements to be able to offer services.

NOTE: A short summary of the impact of regulation or compliance obligations, as in element "C" of Figure 2, can be found in Annex A of the present document.

6 Technical view of the problem of ETI

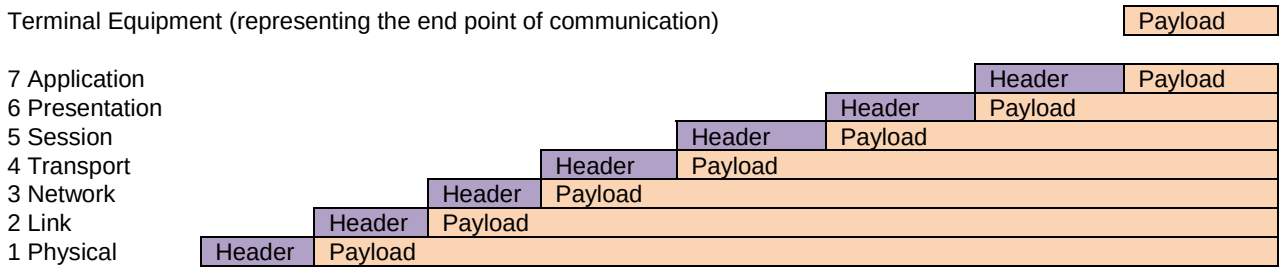
6.1 Simplified network model

There are a very large number of ways of presenting a telecommunications network depending on the level of abstraction to be presented. The purpose of the network model in the present document is to identify the impact of encrypted traffic on network function.

Assumption#1: The present document considers packet-based communications where packets are considered within a layered communications model.

Assumption#2: In a layered model of communication (e.g. the OSI 7 layer model [i.1]) the payload of layer N is not intended to be available to layer N-1 (layer N-1 is agnostic of layer N).

Assumption#3: In a layered model of communication (e.g. the OSI 7 layer model [i.1]) the header of layer N informs the content of the header of layer N-1, and layer N+1.



NOTE: Whilst every layer is indicated as having a header and payload it is recognized that in some implementations the header element is not explicit (e.g. a physical layer header is unusual).

Figure 3: Layering model showing data hiding layer-by-layer

In general, it is only the content of the header at layer N that is required to allow layer N to perform at its optimal level.

For simplicity the network is presented as an entity that allows a Communication End Point (CEP) to connect to its peer CEP. From the point of view of the application in the CEP the network should not be visible. In broad terms if the payload is opaque, it can be encrypted. However, in some instances the nature of the payload may need to be examined in order to validate the content of the header. If the payload is encrypted, and the key to decrypt is known only to the peer (i.e. the key for an encrypted payload at layer N is known only to the layer N peer and is not available to any layer N-1 entity), then it is not possible to verify the header against the content of the payload.

NOTE: In end-to-end communication the terms Terminal Equipment (TE) or User Equipment (UE) are often used to refer to the end-point and may be considered as a synonym for the more general Communication End Point (CEP).

If the CEP encrypts content before submission to the network stack it may be possible for the user to send prohibited information across a network. An examination of this is given in Annex C.

6.2 Layer obfuscation

The term layer obfuscation is used in the ETI context to address one of the many problems wherein a packet is "re-networked" such as found in most tunnelling protocols. For the Internet Protocol (IP) stack this is a case of inserting one IP packet (the inner packet) into another IP packet (the outer packet), the outer packet is visible to the network and all the network functionality is performed on the outer packet with the inner packet being carried transparently across the network. Most tunnelling protocols will encrypt the inner packet. In a VPN environment the intention is to present a remote IP packet as if it were local.

In the most extreme case this form of layering within layers becomes "onion" like, and often referred to as onion-routing, as is used in the Tor project [i.14]. The Tor project further complicates onion-routing as each connection between CEPs is encrypted across a randomized set of relay points, with each relay leg having a different encryption key.

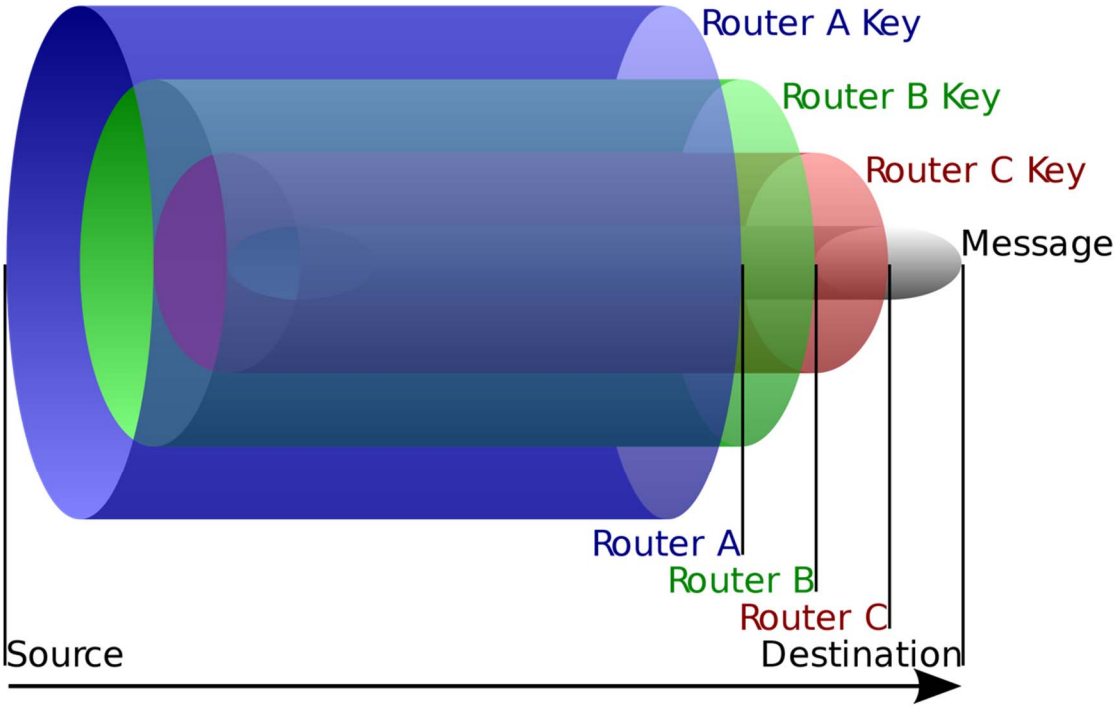


Figure 4: Layer overlaid on layer model as seen in VPNs and onion-routing

In addition to layer obfuscation the more general model is that of layer violations. Many layer violations are designed in as part of network optimization and whilst the theoretical basis of layering is very much against layer violations the reality is that they exist and are often essential. Any dependence on layering violations is broken by extending data hiding to data encryption.

6.3 Stakeholder model

6.3.0 General view

Stakeholders can be defined with respect to their relationship to the data, and to the nature of that relationship as one of owner, trusted party (each of these is considered as non-adversarial stakeholder), or adversary.

6.3.1 Adversarial stakeholders

The viewpoint of an adversarial stakeholder is to use pervasive encryption with an explicit intent to avoid any form of oversight (i.e. to explicitly act against the interests of parties in group A and C of the Venn diagram from Figure 2).

6.3.2 Non-adversarial stakeholders

A non-adversarial stakeholder uses encryption as offered by legitimate parties in order to ensure that privileged information is only made visible to authorized parties.

6.3.3 Network management stakeholders

Network managers are a special case of non-adversarial stakeholders that are network-resident and who aim to optimize availability of networks to serve the other non-adversarial stakeholders. In particular, one of the roles of network management stakeholders is to be able to inhibit the actions of adversarial stakeholders. The ability to validate traffic and signalling is critical to the success of network management.

7 Quantitative risk assessment

7.1 Overview

The TVRA approach defined in ETSI TS 102 165-1 [7], and expanded on in ETSI TS 102 165-3 [i.35] for continuous vulnerability assessment in the context of the CSA [i.32], identifies risk as the product of the impact and likelihood of an attack. For assessment of likelihood a number of metrics are considered that determine the level of expertise, time and equipment required by the attacker to conduct the attack. In addition the method addresses how the motivation of an attacker may determine the willingness to achieve an appropriate level of technical knowledge to mount an attack.

7.2 Impact and likelihood assessment

The core concern of pervasive encryption has been outlined in clauses 4, 5 and 6 of the present document. In order to express the problem more quantitatively the risk calculation approach defined in ETSI TS 102 165-1 [7] is applied below.

Risk is assessed as the weighted product of the likelihood of a threat, and the impact of that threat. As outlined in previous clauses of the present document the impact of pervasive encryption is scenario, or use case, dependent. In contrast the ease of deploying strong encryption indicates that, in general technical terms, the likelihood of deploying encryption is very high. This is shown in the assignment of the likelihood factors from ETSI TS 102 165-1 [7] to the deployment of end-to-end or pervasive encryption in Table 1 and the resulting assessment of attack potential as basic shown in Table 1 and Table 2.

Table 1: Quantization of attack potential for application of encryption

Factor	Range (assigned file)	Value	Scoring rationale
Time (elapsed time)	≤ 1 day	0	The level of detail widely available for applying encryption suggests that an attack can be planned and deployed in less than 1 day.
Expertise	Layman	0	Tools exist to easily switch encryption on without having to have detailed knowledge of the cryptography that underpins it. In part this is because most computers and their operating systems include basic capabilities to apply encryption.
Knowledge	Public	0	There is widespread publicly available data to guide a non-expert to apply encryption at end points on a public connection.
Opportunity	Easy	1	Most of the tools for applying encryption exist by default in common ICT platforms.
Equipment	Specialized	4	There may be a requirement for slightly more advanced software than comes bundled with a computer and its operating system. As with the gathering of expertise and knowledge however most of this equipment is readily available with some effort to search it out.

From ETSI TS 102 165-1 [7] the attack potential is translated into natural English terms as in Table 2.

Table 2: Quantization of attack resistance to application of encryption

Attack potential values	Attack potential required to exploit attack	Resistant to attacker with attack potential of
0 to 9	Basic	No rating

With the assumption that the impact from random application of encryption is non-negligible the likelihood of attack is considered as at least "possible" and often "very likely" as described in ETSI TS 102 165-1 [7].

Depending on the use case (see clauses 4 and 5, and Annex B for an overview of some use cases where pervasive or maliciously applied encryption is deployed) the level of risk measured using the approach described in ETSI TS 102 165-1 [7] is either Major or Critical in most cases.

EXAMPLE 1: A ransomware attack in which assets are encrypted by an attacker using symmetric keying with the key released on payment of the ransom, or simply destroyed if the ransom is not paid, may result in critical and irrecoverable loss of essential assets. Overall risk assessment of ransomware should be that it is a critical risk.

EXAMPLE 2: Masking of essential routing data by use of layer masking (a Tor like network or a simple lower layer VPN) may result in continuous reinjection of traffic to the network without it terminating efficiently and thus lowering network efficiency. In the extreme cases this may lead to over investment in devices (CapEx) and raise operational costs (OpEx) to cope with maliciously formed traffic and could place the network organization at critical risk levels.

As indicated in the examples pervasive encryption can give rise to increases in both Capital Expenditure (CapEx) and Operational Expenditure (OpEx) by reducing the achievable efficiency of networks and services.

7.3 Motivation assessment

It can be suggested that the application of encryption to user content is somewhat benign and is motivated by a reasonable desire on behalf of the user applying the encryption to satisfy the security tenet of least privilege. Thus it is reasonable to encrypt the details of a bank transaction as the network provider is not a privileged user of that content.

7.4 Countermeasure considerations

The guiding principle of countering ETI problems is visibility, transparency, and the provision of a trust architecture.

The general model of countermeasure identified in ETSI TS 102 165-1 [7] is that they (the countermeasures) are assets that are added to the system to reduce the weighted risk to the system. The purpose of countermeasures is to reduce either the likelihood of an attack or the attack impact. The general security model can be summarized in the triplets shown below for each of the model (i.e. the general ETI concern) and its implementation (i.e. means to address the ETI concern):

- Model: {threat, security-dimension, countermeasure}
- Implementation (for ETI): {pervasive encryption, integrity, transparency and explicability}

The specific threat considered in the present document is "pervasive encryption". In this case the security dimension most impacted is integrity, in that the threat may not allow managed operation of the network, and may allow for prohibited content to be distributed. The latter threat in particular impacts the level of trust afforded to the network by its users and therefore impacts the security dimension of integrity.

NOTE 1: The meaning given to integrity in this instance is that a trusted network acts honestly and without masking its behaviour from its stakeholders.

NOTE 2: A framework of security countermeasures is described in ETSI TS 102 165-2 [8].

Whilst the present document identifies that in order to counter the threat to integrity from pervasive encryption the network and is constituent elements shall be both transparent and explicable it is recognized that there may be several alternative countermeasures and these should first be identified, then evaluated and compared to identify the costs and benefits of each so that an informed decision can be made of which countermeasures to select.

The model of static and run-time transparency and explicability given in ETSI TS 104 224 [9], and the application of the ZT-Kipling method (in ETSI TS 104 102 [2]) in the context of ETSI TS 102 165-1 [7] may be used to provide the required countermeasure to the threat of pervasive encryption (see also clause 8.2).

8 Requirements to counter the ETI problem

8.1 Introduction and overview of means to counter ETI

An ETI conformant network shall be able to demonstrate that for each connection there is an established trust contract, and an associated security contract. The present document identifies the role of Zero Trust Architecture (ZTA) [1] and its close association to an active (rather than static) implementation of the secure by default paradigm [i.19] in providing the transparency and explicability of the use of encryption, while adhering to ZTA principles within related technologies to mitigate the ETI problem. Thus the core requirements to counter the ETI problem are transparency and explicability of the role and purpose of every element in the network.

NOTE: Whilst the present document uses the ZT and ZTA paradigm to achieve the transparency and explicability requirements other approaches may be used to achieve the same objectives.

In a broad interpretation of the ETI problem statement addressed in clauses 4, 5 and 6, and specifically in clause 7.4 above of the present document, it is surmised that making the operator and other stakeholders explicitly aware of the use and role of encryption, and other security techniques, in the system will allow mitigation of the negative effects of encryption whilst promoting their positive effects. The consequence for the recommendations in the form of requirements outlined in the present document is to make all security functions in a network explicit, with the further requirement to ensure that every transaction is made within a bounded set of Security Associations (SAs), while validating legitimacy of the transmitted data, that build to provide an explicit per transaction security model. The security model by being explicit should then also be considered as making an explicit trust model for each transaction. The initial point should be that the entire transaction and all the elements and data involved in the transaction are untrusted and insecure. The end point at which the transaction should take place is that all elements and data in the connection are secured and trusted.

As stated above, to support ETI the operator and other stakeholders should be explicitly aware of the use and role of encryption, and other security techniques, in the system. Thus all security functions in the ICT system or network that is ETI compliant shall be explicit. In practical terms this requires that each security function is transparent and the rationale for each function is explicable.

8.2 Transparency

It shall be possible for an authorized entity to request the encryption state of any connection or data at any involved, identifiable, and addressable object (hereinafter referred to as an entity), in the ICT system by direct interrogation of the entities participating in the connection. The requesting entity should be within the same trusted environment of the target entity (the one whose state is being interrogated) and therefore has to be identified and authenticated before being allowed to operate on the entity. The encryption state of any connection shall be reported as one of: encryption applied; encryption not applied; or unknown.

In order to enable the transparency requirement, all entities in the communication chain shall have a well-defined (i.e. standardized) point of inspection, and a standardized query interface should be used.

As part of the goal of achieving transparency the sub-goals of accountability and explicability are considered. For this to be achieved the base requirement of transparency above shall apply to the connection as a whole and the context in which encryption is applied.

NOTE: A number of means exist that attempt to verify and provide proof of the path any packet has taken across a network by addition of data to the packet header for 3rd party verification. The approach in the present document is to develop a trust and security contract for the connection that provides an alternative approach to achieve such proofs.

The model for explicability and transparency is identified below and summarized in Figure 5.

Figure 5: Components required in element documentation for transparency

Every element shall be identified and able to explain its purpose in the system. Every element shall identify the forms of security association it supports, and for each security association the root of trust (as the point of liability) shall be identifiable.

The general approach to static and run-time explicability identified in ETSI TS 104 224 [9] should be augmented by application of the ZT-Kipling method (ETSI TS 104 102) [2]. Table 3, Table 4, Table 5 and Table 6 below act as examples of the application of each of ETSI TS 104 102 [2] and ETSI TS 104 224 [9] to the pervasive encryption problem.

Table 3: Application of ETSI TS 104 102 [2] in the ETI context

Question form	Question text example
What	What is being encrypted? (e.g. data at rest, data in transit, consumer data, signalling data)
Why	Why is encryption being applied (to that asset/data/signalling)?
When	When is the encryption applied (and removed)?
How	How is the encryption applied? (e.g. symmetrically, asymmetrically, transparently to the end-user, with the collusion of one or more other parties)
Where	Where is the encryption applied? (logically (say the OSI layer) and geographically)?
Who	Who applies the encryption? (i.e. who has the keys for the operation?)

Table 4: Static explicability statement for ETI and the role of encryption (from ETSI TS 104 224 [9])

Documentation Element	Element
1	Statement of system purpose
2a	Identification of data source(s)
2b	Purpose of data source(s) (in support of system purpose)
2c	Method(s) used to determine data quality
3	Identity of liable party

The purpose of explicability is to allow a lay person (i.e. not a professional programmer or system analyst) to gain a reasonable understanding of the main data flows and processing steps in the program.

Table 5: Run time explicability statement ETI and the role of encryption (from ETSI TS 104 224 [9])

Documentation Element	Element
RTE-1	Static explicability statement
RTE-2	What process does data undergo between acquisition and curation?
RTE-3	What are the metrics that determine change in the learning/weighting of data?
RTE-4	Identification of events to be logged
RTE-5	Identification of performance target and associated metrics
RTE-6	Identification of liable party (if different from that identified in the static explicability documentation)

Table 6: Transparency statement for ETI and the role of encryption (from ETSI TS 104 224 [9])

Documentation Element	Element
T-1	Static explicability statement
T-2	Run time explicability statement
For each data source	
T-3a	Verified identification of source of data
T-3b	Verified proof of liability of data source
T-3c	Verified proof of consent to use

8.3 Management of cryptographic keys

The trend in cryptographic protection is towards perfect forward secrecy in which session keys cannot be compromised even if the root key from which the session keys are derived is itself made known. Ephemeral keys are a consequence or attribute closely associated with trying to achieve forward secrecy. A key is described as ephemeral when it is created uniquely for each key establishment process. The assurance of forward secrecy requires that the ephemeral session key is discarded after use.

For the purposes of ETI the legitimate use of forward secrecy should be maintained for each Security Association (SA) in a transaction. However the form of key agreement should be visible to authorized parties.

8.4 Identification of authorized parties

The encryption state of any connection of an ETI conformant system shall only be disclosed to authorized parties. An authorized party shall be unambiguously identified and that identity shall be authenticated. The identity of the authorized party may take a number of forms including those defined in ETSI TS 103 486 [i.20] and using forms of attribute rich identity coupled to attribute based authentication modes as described in ETSI TS 103 486 [i.20].

8.5 Trust architecture for ETI

A layered communications architecture, as defined for OSI in ISO/IEC 7498-1 [i.1], has implicit trust relationships at each layer determined by the functional model of each layer. The present document extends the OSI model to a wider concept of ZTA as in NIST SP 800-207 [1] beyond the enterprise network to a full public telecommunications network addressing the particular model described in clause 3.1.3 of [1] (ZTA Using Network Infrastructure and Software Defined Perimeters) to the entirety of the OSI stack.

ZT a security strategy (or approach) is designed to detect and prevent breaches, while consistently (or better continuously) verifying all users, all devices, all layers (e.g. OSI layers, signalling, data, management, etc.), all applications across all locations in the real time (run time), and applying Continuous Integration and Continuous Delivery (CI/CD) pipeline security, resulting in preventative security from all attack vectors at all stages of the attacks.

The rationale of the ZTA is that there should be no assumptions as to what happens before or after each hop in and across the infrastructure, starting with the source and ending with the destination of a particular data flow. Every device, application, microservice, and user shall be validated and verified in real time. With each step a user (or the proxy for the user) makes through the infrastructure, the following two aspects provide adherence to ZTA:

- ETI conformant systems shall provide means to validate, authenticate, and apply threat prevention capabilities across all locations consistently.
- ETI conformant systems shall provide means to validate, authenticate and verify all users, all devices, and all applications, and apply threat prevention capabilities across all locations to protect against all attack vectors consistently.
- ETI conformant systems shall be able to validate the "who", the "what", the "where", the "when", the "why", and the "how" across all traffic flows throughout the lifecycle of those flows.

NOTE: Applying the ZT-Kipling method defined in [2] addresses the means to do the "who", "what", "where", "when", "why", and "how" validation.

Whilst the abstracted model from ETSI TS 102 165-2 [8] is recommended for addressing the ETI problem it is recognized that the managed security of networks is broadly addressed by the following services as defined by the OSI 7-layer security model (see table 2 of Recommendation ITU-T X.800 [4] and its mirror ISO 7498-2 [i.18]) and the aspects of ZTA [1]:

- At layer 7:
  - Identity Assertion ("who").
  - Application Validation ("what").
  - To-be-accessed Targeted Resources Destination ("where").
  - Data Flow Time-stamping ("when").
  - Data Classification ("why").
  - Identity Assertion of the Targeted Resources Access ("how").
  - Peer Entity Authentication.
  - Data Origin Authentication.
  - etc.
- At layer 6:
  - Facilities provided by the presentation layer offer support to the provision of security services by the application layer to the application process.
  - The facilities provided by the presentation layer rely on mechanisms which can only operate on a transfer syntax encoding of data.
  - Security mechanisms in the presentation layer operate as the final stage of transformation to the transfer syntax on transmission, and as the initial stage of the transformation process on receipt.
- At layer 5: No security services are provided in the session layer.
- At layer 4:
  - Peer Entity Authentication;
  - Data Origin Authentication;
  - Access Control service;
  - Connection Confidentiality;
  - Connectionless Confidentiality;
  - Connection Integrity with Recovery;
  - Connection Integrity without Recovery; and
  - Connectionless Integrity.
- At layer 3:
  - Peer entity authentication.
  - Data origin authentication.
  - Access Control List (ACL).
  - Connection confidentiality.
  - Connectionless confidentiality.

  - Packet flow confidentiality.
  - Connection integrity without recovery.
  - Connectionless integrity.
- At layer 2:
  - Connection confidentiality.
  - Connectionless confidentiality.
- At layer 1:
  - Connection confidentiality.
  - Traffic flow confidentiality.

Each security service in the OSI model exists as a peer to peer service, i.e. network layer to network layer, application layer to application layer. Each layer has an implicit security association determined by the key used to protect the services at that layer. The model in the present document extends the OSI peer-to-peer model with the ZTA defined in [1] and addresses the identity management requirements as an instance of the model for ZTA Using Enhanced Identity Governance ([1], clause 3.1.1).

To be considered as ETI layers shall be developed as independent trust zones with clear visibility (see clause 8.2 Transparency) of the services offered. By the term independent trust zone it is intended that each layer should have autonomy from any other layer.

As Figure 2 illustrates, ZTA adds the following attributes to each of the OSI layers:

- Layer 7: Data Validation and Integrity check, Threat Intelligence, Microsegmentation of Services; Identity Assertion.
- Layer 6: This is folded into Layer 7.
- Layer 5: This is folded into Layer 7.
- Layer 4: Pure Access Control Lists do not guarantee ZTA, hence this is folded into Layer 7.
- Layer 3: Microsegmentation, Data Source validation, Data Destination validation, Data Destination Authentication.
- Layer 2: This is folded into Layer 3.
- Layer 1: Authenticity and validation checks of all hardware and software components.

In summary, ZTA follows the principle of "never trust, always verify".

The model of trust, on the other hand, is that whilst content of user communication may view the network as untrusted and the user may choose to apply application plane services to ensure confidentiality of user content, the lower layers are themselves contained in layer specific trust relationships. In this way all data required to enable layer operations should be visible to that layer.

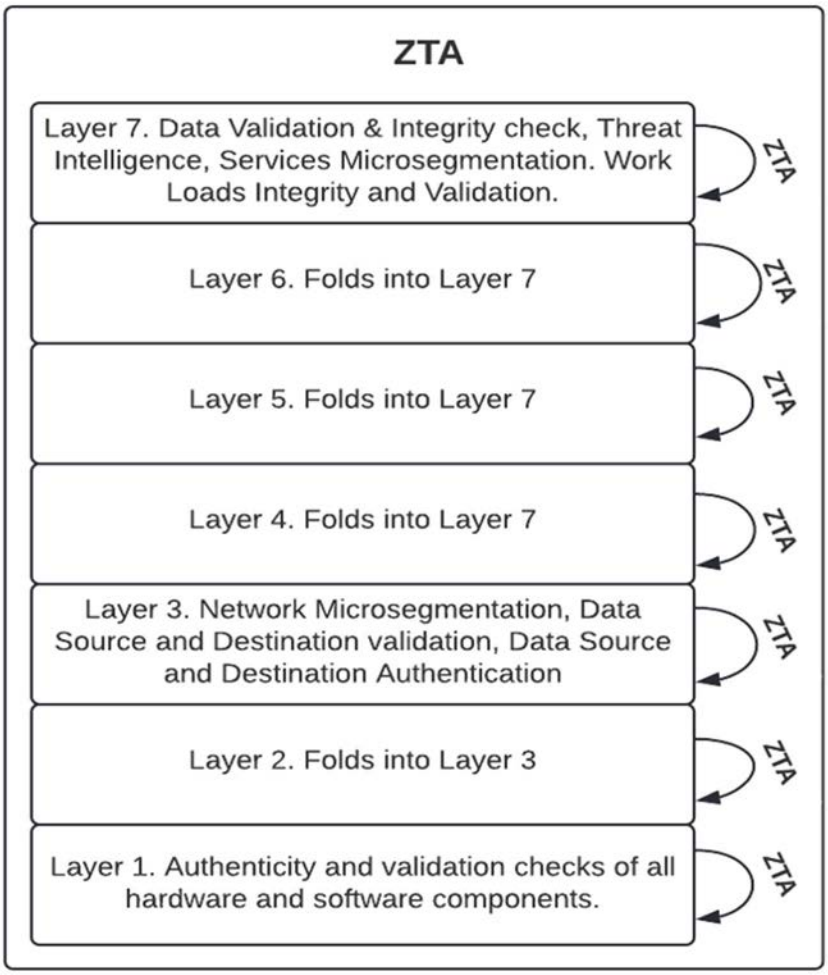


Figure 6: Representation of ZTA mapping to OSI layers

In general, whereas trust can be defined in spoken and written English as "*firm belief in the reliability, truth, or ability of someone or something*" this has to be translated into something more tangible and exact for ICT systems and has often been simplified into the assertion of integrity of an object where that assertion is made, or attested to, by a known entity. A number of forms of integrity assertion exist, summarized in ETSI TS 102 165-2 [8], including the use of Message Authentication Codes (MACs), Hash functions, and digital signatures. The present document suggests that security association is used as a synonym for trust association.

An end-to-end connection is composed of at least one and more likely an indeterminate, but finite, number of security associations. E2E security is thus not just an end-point issue but a composition of SAs issue. Each security association is also a representation of a trust association and for the purposes of the present document trust is a weighting that applies to a security association.

$$\sum Trust.SA$$

Each security association should be protected by a unique key. For compositions of security associations, where one security association is dependent on another security association within the overall composition, they should be protected by different (*and also unique*) keys. The nature of an SA, one-to-one, one-to-many (including broadcast), many-to-one and many-to-many, has a significant influence on the selection of keying strategy to protect to the SA, details of keying strategies are addressed in ETSI TS 102 165-2 [8].

NOTE 1: An SA does not imply encryption but rather explicitly identifies the nature of the security association, e.g. an SA and key for each of integrity/confidentiality/availability. Therefore SA should not be read as shorthand for encrypted link.

In the ETI model each link shall represent trust for each attribute of the CIA paradigm:

- How is data encrypted and decrypted? Who establishes the keys?

- Source authentication → as a prerequisite for the other attributes.
- How is data integrity preserved?
- How is the identity of the asset and link assured?
- How is access control to data and services related to the link assured?

When the ZTA model is completed the result is a trust contract between end points that details the form of security association on each link and at each layer.

NOTE 2: Not all links will be explicit as some links will essentially be passive (layer 1 and 2 links often have no complex security associations).

The role of trust contracts is addressed in part by obligation of trust protocols (see ETSI TS 103 486 [i.20] and also ETSI TR 103 719 [i.8]).

8.6 Reference model of an ICT network for ETI

The security model for ETI is developed from that found in ETSI TS 102 165-2 [8] and copied below for convenience. In this latter model the OSI model [i.1] is simplified to 3 planes: Transport; Service and Application. Between planes both horizontally and vertically are "points of attachment" and it is at these points of attachment that the security services lie. The transport plane approximates to the lower layers of the OSI model, the service plane approximates to the higher layers of the OSI model, with the application plane addressing the user level application.

NOTE 1: The specific terminology from ETSI TS 102 165-2 [8] is drawn from a traditional telecoms consideration but with a relaxed interpretation can be mapped to non-telecoms environments, including those of conventional programming, to business practices and similar.

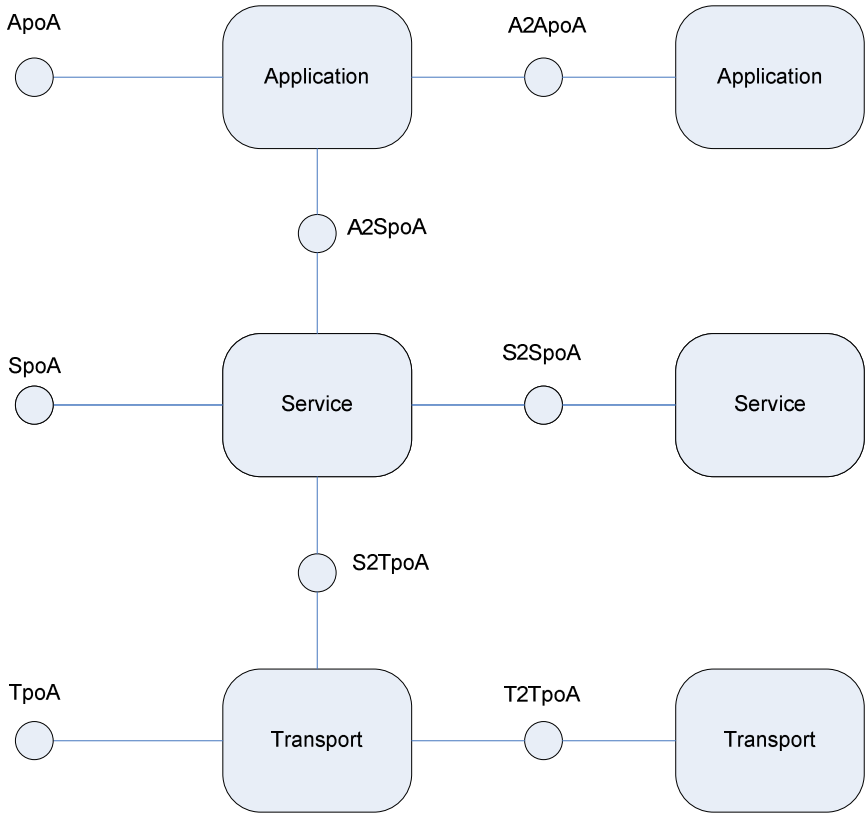


Figure 7: Abstract architecture for security countermeasure application from ETSI TS 102 165-2 [8]

The user connects to each layer using a layer specific point of Attachment (poA):

- TpoA Transport point of Attachment (TpoA reference point).

- SpoA Service point of Attachment (SpoA reference point).
- ApoA Application point of Attachment (ApoA reference point).

The countermeasures are described with respect to the user interaction with each layer:

- Inbound authentication at TpoA/SpoA/ApoA.
- Outbound authentication at TpoA/SpoA/ApoA.

NOTE 2: If an authentication exchange nests inbound and outbound authentication, it is termed mutual authentication. However if the exchanges are discrete and with different lifetimes the term mutual authentication is inappropriate.

- Integrity of communication at TpoA/SpoA/ApoA.
- Confidentiality of communication at TpoA/SpoA/ApoA.

Within the system the countermeasures are extended to cover interactions between layers both vertically and horizontally. The set of countermeasures thus include:

- Service to Service authentication.
- Integrity of communication from Service to Service.
- Confidentiality of communication from Service to Service.

NOTE 3: The term Service is used as a synonym for any of the three abstract layers of the ICT architecture.

The services apply to the following points on Figure 4:

- A2SpoA Application to Service reference point.
- S2TpoA Service to Transport reference point.
- A2ApoA Application to Application reference point.
- S2SpoA Service to Service reference point.
- T2TpoA Transport to Transport reference point.

NOTE 4: The model does not show a specific reference point between Application and Transport on the assumption that a Service layer always exists.

In addition to the countermeasures provided at the identified reference points a secure system may have to deploy other countermeasures to protect their assets. Such countermeasures may include billing controls, system auditing and event logging.

Annex A (informative): Considerations for Compliance Obligation

A.1 Overview

The compliance obligations described in this annex are examples and do not imply that these are the only obligations that apply to communication networks, or that these are the only obligations affected by pervasive encryption in networks.

NOTE: A full enumeration of compliance obligations for communication networks is provided in ETSI TR 103 369 [i.10].

A.2 EU GDPR

The General Data Protection Regulation (GDPR) [i.28] suggests the use of encryption several times across several articles. For example, Articles 6.4e, 32.1a, 34.3a all suggest use of encryption.

It is possible that an over enthusiastic interpretation of these articles leads to a data controller recommending that everything is encrypted at all times. However, such an interpretation does not eliminate the data protection responsibility, as the end points of the communication would normally decrypt the data that has been encrypted whilst in transit. This happens especially with the reception of Personal Identifying Information (PII). Once everything has been decrypted (even if only for temporary processing) obligations for data protection apply in regard to that content.

A.3 EU NIS2 Directive

The Network and Information Security Directive (NIS Directive) [i.29] applies in particular to two forms of commercial entity:

1) Operators of essential services

2) Digital service providers

In ETSI TR 103 456 [i.5] and in the ENISA report on gaps in NIS standardization [i.6] a wide overview of the impact of the NIS Directive [i.29] on networks and on standardization is given. These reports however have not fully addressed the impact on network management from the forms of pervasive encryption addressed by the present document.

Many of the goals of the NIS Directive [i.29] may be thwarted, e.g. Article 7 requires this capability as part of a national strategy "*defining the strategic objectives and appropriate policy and regulatory measures with a view to achieving and maintaining a high level of security of network and information systems*". Many risks may be invisible as a result of the application of end-to-end encryption. Where risks impact essential services provided at the network edge, there is a clear risk of being unable to conform to the core requirements of the NIS Directive [i.29] when end-to-end encryption is deployed.

In broad outline the purpose of the NIS Directive [i.29] is to enable EU Member states to provide legal measures that in turn invoke a set of common cyber security technical requirements that include:

- structured sharing of information on risks and incidents;
- notification of incidents;
- outcomes-focused cybersecurity risk management practices and controls to identify and protect assets, detect anomalous analyses and potential incidents, and respond to and recover from incidents that may impact network and information systems;
- international cooperation to improve security standards and information exchange, and promote a common global approach to NIS issues through harmonised standards.

The impact of end-to-end encryption of both content and signalling on management of the NIS Directive [i.29] may be such that the necessary analysis to allow information sharing may be severely impeded.

A.4 Council of the EU Resolution on Encryption

The EU has adopted the "Council Resolution on Encryption - Security through encryption and security despite encryption" [i.33]. The resolution contains several clauses describing objectives, the current use/state of encryption, challenges for ensuring security, striking a right balance, joining forces with the tech industry, a need for a regulatory framework, and innovative investigative examples.

Concerning a regulatory framework, the resolution notes:

- The need to develop a regulatory framework across the EU that would allow competent authorities to carry out their operational tasks effectively while protecting privacy, fundamental rights and the security of communication could be further assessed.
- Potential technical solutions will have to enable authorities to use their investigative powers which are subject to proportionality, necessity and judicial oversight under their domestic legislation, while respecting common European values and upholding fundamental rights and preserving the advantages of encryption. Possible solutions should be developed in a transparent manner in cooperation with national and international communication service providers and other relevant stakeholders. Such technical solutions and standards - and the fast development of technology in general - would also require continually improving the technical and operational skills and expertise of competent authorities to effectively address the challenges of digitalization in their work on a global scale.

The present document, and any follow-on work undertaken, may in part address the requirements for further assessment and the transparent development of solutions, outlined in the resolution.

A.5 EU Cybersecurity Act

The EU Cybersecurity Act [i.32] adopted in April 2019 provides "*a framework for the establishment of European cybersecurity certification schemes for the purpose of ensuring an adequate level of cybersecurity for ICT products, ICT services and ICT processes in the Union, as well as for the purpose of avoiding the fragmentation of the internal market with regard to cybersecurity certification schemes in the Union*". It tasks ENISA with numerous related functions.

The Cybersecurity Act does not, however, explicitly mention or treat encryption except in a legislative history paragraph encouraging ENISA "to promote basic multifactor authentication, patching, encryption, anonymization and data protection advice".

A.6 ePrivacy Regulation

In 2017, a draft proposal referred to as ePrivacy Regulation [i.3] was introduced in the European Parliament and the Council. Its many provisions lay down rules regarding the protection of fundamental rights and freedoms of natural and legal persons in the provision and use of electronic communications services, and in particular, the rights to respect for private life and communications and the protection of natural persons with regard to the processing of personal data. It has not, however, further progressed. It also has no specific provisions related to encryption except in a legislative history paragraph that mentions that "*Service providers who offer electronic communications services should inform end- users of measures they can take to protect the security of their communications for instance by using specific types of software or encryption technologies*".

A.7 Radio Equipment Directive

The Radio Equipment Directive 2014/53/EU ("RED") [i.2] ensures a single market for radio equipment. In particular, it requires that, before being placed on the market, radio equipment has to incorporate safeguards to ensure that the personal data and privacy of the user are protected. Under the RED [i.2] and the European Standardization Regulation (EU) 1025/2012 [i.4], the Commission is empowered to adopt measures that determine access to markets.

For the bulk of the RED [i.2] only radio aspects are considered and the test conditions are specified in Harmonised ENs. However, there are aspects of the RED [i.2] in Article 3.3d/e/f that address security and privacy that may be impacted by end-to-end encryption. The specific impact of persistent and pervasive encryption as addressing RED Article 3.3d/e/f are outlined as follows.

"3. Radio equipment within certain categories or classes shall be so constructed that it complies with the following essential requirements:

(d) radio equipment does not harm the network or its functioning nor misuse network resources, thereby causing an unacceptable degradation of service;".

In this instance the problem statement given in respect of network management stakeholders (see clause 6.3.3 of the present document) applies.

"(e) radio equipment incorporates safeguards to ensure that the personal data and privacy of the user and of the subscriber are protected;".

Here it may be argued that applying encryption will achieve this.

"(f) radio equipment supports certain features ensuring protection from fraud".

The following publications address the security aspects of the RED: EN 18031-1 [i.25], EN 18031-2 [i.26], and EN 18031-3 [i.27].

A.8 Lawful access to communication and communications data

ETSI TS 102 656 [6] and ETSI TS 101 331 [5] define the broad set of requirements from law enforcement to telecommunications. The expectation is that data is provided en-clair where keys are known to the provider, or in native format when keys are not available. The obvious impact of end-to-end encryption is that less content can be offered en-clair, and if the imposition of end-to-end encryption extends to signalling that too cannot be offered en-clair.

A.9 Digital Services Act

The DSA [i.34] provides a set of rules regulating the responsibilities of digital services that act as intermediaries within the EU to connect consumers with goods, services and content. In this context, 'digital services' refers to online platforms, such as marketplaces and social media networks, it can also be extended to consider apps that implement such services. The DSA sets out clear due diligence obligations for online platforms and other online intermediaries. This is a different dimension of security than much of existing telecommunications in that it looks at content and its legitimacy under the law. The DSA addresses the requirement to ensure platforms remove fraudulent products and content from being distributed and gives tools to ensure that users can flag illegal or disturbing content, and will also have a clear means of contesting platforms' content moderation.

A.10 Cyber Resilience Act

The Cyber Resilience Act [i.30] identifies a number of essential requirements to be met prior to placement of things with digital elements on the market (for the EU). The approach and requirements outlined in the present document provide a baseline for achieving the essential requirements for the run-time security of networks, services and applications.

A.11 Artificial Intelligence Act

The Artificial Intelligence Act (EU AI Act) [i.31] lays out the foundations for regulating AI in the EU. The AI Act classifies AI according to its risk, as follows: prohibited unacceptable risk; regulated high-risk; limited risk, where deployers and developers are required to ensure that end-users are aware that they are interacting with AI; and unregulated minimal risk.

ETSI TS 104 223 [10] defines a set of 13 principles for the provision of secure AI, in addition ETSI TR 104 065 [i.24] maps the requirements of the AI Act [i.31] to the wider output of ETSI.

Whilst AI, and the AI Act, do not require data sources or algorithms to be encrypted there is a risk that by abusing encryption maliciously formed data may not be identified and may lead to unintended consequences.

Annex B (informative): Encryption tools

B.1 Architectures and schemes

To a limited extent the form of encryption used by actors will influence the strategies used to mitigate the worst impacts of encrypted traffic and signalling on network operation. In simple terms the success of cryptography is in the management of keys, on the assumption that the underlying algorithms have been tested and proven to achieve their intended security strength. Key management strategies and the matching algorithms fall into a small set of classes:

- Symmetric encryption:
  - Only the end points have access to the key.
- Asymmetric encryption:
  - One key to lock, a matching key to unlock. Often termed public key encryption in that one key of the pair can be made public with close to zero likelihood of an adversary determining the private key.
  - Widely used in e-commerce and large parts of the internet to protect the content of transactions, and widely built into core protocols.
- Functional encryption:
  - Functional encryption is a generalization of asymmetric encryption. It is seen in two primary forms where the public key element has semantic meaning (e.g. an email address):
    - Identity based encryption (see ETSI TR 103 618 [i.7], ETSI TR 103 719 [i.8]).
    - Attribute based encryption (see ETSI TS 103 532 [3], ETSI TS 103 458 [i.9]).
- Homomorphic encryption:
  - A form of encryption that allows operations on encrypted data without decrypting it first. The result of the computation is in an encrypted form, when decrypted the output is the same as if the operations had been performed on the unencrypted data.

In addition, due attention should be paid to the evolution of the above strategies to mitigate the threat from Quantum Computing and to the development of algorithms resistant to Quantum Computing attacks, as defined in the output of ETSI TC CYBER QSC (Quantum Safe Cryptography).

B.2 Additional key management issues

From the outline of clause B.1 above, there are two forms of keying, symmetric where both parties have the same key, and asymmetric where the keys are paired with one key used for encryption and one for decryption. A general rule of thumb is that symmetric encryption is fast, and asymmetric encryption is slow. A second rule of thumb is not to over expose a key, so in the same way that users are recommended to use different passwords for every site or purpose, it is conventional practice to use a "session key" for every session. If a new session key is used, and if the new session key cannot be linked to any other session key from the same user, then even if the key for a single session is compromised only that session is compromised, this is common practice in cellular radio. The means by which a session key is derived is an important consideration, recognizing weaknesses that may lead to a loss of perfect forward security has seen a move to ephemeral key agreement schemes.

With some key exchange methods identical keys will be generated if the same parameters are used on either side. The role of ephemeral methods is to guarantee that a different key is used for each connection, with the addition of protection against a store and extract attack. Therefore, an attack on any long-term key would not cause all the associated session keys to be breached, halting the attempt to recover data encrypted with those session keys (this offers a guarantee of perfect forward secrecy). Due to the promise of ephemeral keys giving guarantees of perfect forward secrecy they are being embedded in many of the commonly used network protocols. This includes TSLv1.3 for protection of IP traffic, WPA-3 for Wi-Fi® networks, and use of Ephemeral Diffie Helman (EDF) in key exchanges.

Annex C (informative): Case analysis of impact of end-to-end encryption

C.1 Criminal activity - general

The term **Going Dark** has been used by law enforcement authorities for several decades and was specifically cited by the U.S. Office of the Director of National Intelligence [i.13] as a major concern for law enforcement.

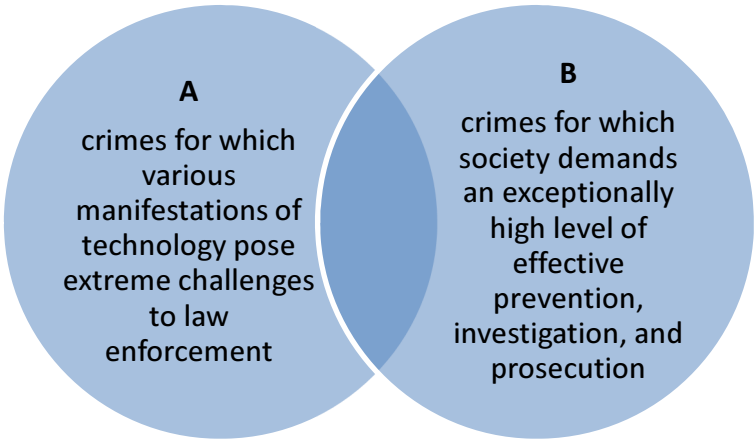


Figure C.1: Law enforcement view of Going Dark

Figure C.1 shows the "classic" Going Dark Venn diagram, where A and B intersect, society gets worried. Crimes that fall into the intersection include drug crimes, terrorism and child sexual exploitation.

When using telecommunications in aid of criminal activity the criminals effectively hide in plain sight and use technology to mask their activity. The problem of "Going Dark" is that law enforcement are always playing catch up, and the inherent danger is that the gap between what is feasible to gather evidence on and the ability of the criminal to mask their activity is one of many unknown unknowns (the existence of crime is a known unknown, it is known to be going on, but it is often unknown who is involved and where and how to stop the criminal having a technological advantage).

The problem that ETI is faced with, is to enable reasonable legal access to data, such as images, to make a value judgement on the content without violating privacy or denying legitimate use of certain data. This is in addition to having reasonable access to each protocol layer's header to allow for network capabilities to be optimized (in practice this is giving some access to Layer N+1, i.e. to the layer above, which means some restricted override of data hiding).

If criminal extortion over telecommunications takes place it is unlikely to be limited to a single channel, rather it is more likely to occur over multiple channels belonging to the victim (e.g. social media channels, direct telecommunications links). The problem of pervasive end-to-end encryption makes discovery and investigation hard.

C.2 Cryptovirology

At one extreme of the rise of pervasive encryption is the specific application of cryptography to malicious ends. The insight that encryption could be used to skirt the protections provided by the network has led to the creation of a new field of study: cryptovirology. This field is devoted to studying the methods in which cryptography may be used to design powerful malicious software.

The first cryptovirology attack, "cryptoviral extortion" [i.15], was presented at the 1996 IEEE Security & Privacy conference. This attack featured either a cryptovirus, crypto worm, or cryptotrojan, containing the public key of the attacker, which would then hybrid encrypt the victims' files, the term for this type of attack was later coined to be ransomware.

C.3 Melissa virus and malicious software distribution

Many computer viruses and other forms of malware have to a greater or lesser extent, relied upon encryption to bypass protection and infect computer end points. Examples include the Melissa virus dating from 1999, the Morris worm, which was the precursor to Melissa dating from 1988, and attacks such as those performed by ransomware.

The Melissa virus was a fairly simple macro-virus, used to distribute content by inveigling itself to commercial email programs and accessing contact data, then distributing itself through the email program to a subset of the infected account's contacts. Whilst not of itself particularly malicious, Melissa spawned the development of much more malicious code by proving the value of a delivery mechanism, and gave impetus to the study of cryptovirology, the application of cryptography for implementation of malicious software.

If payloads can be encrypted, for example using a Melissa-like virus accessing contact lists where the public key of the contact is visible, then a malicious payload can be distributed and protected from observation by the network through end-to-end encryption. Given that the recipient is receiving mail from a known and trusted contact the likelihood of successful transmission of the viral and malicious content is more assured.

Whilst whole disk encryption is commonly applied by computer users at end points (minimizes risk in event of loss or theft of the computer or its disk), variations of it may be applied with malicious intent. This is somewhat exacerbated with most modern computers having crypto-acceleration built in, having Hardware Security Modules (HSMs), and having direct access to crypto-libraries from the OS. The generic fields of Ransomware and of Kleptography use attacker-controlled encryption to variously encrypt critical files on a computer with the effect of making the computer unusable. In some instances the attack is reversible (e.g. using an asymmetric key pair with one key used to encrypt the target and the matching paired key to release/decrypt the target), but the attacker is not required to be able to return an attacked system to its previous state (e.g. encrypting a target and not retaining the key to allow decryption).

The increasing reliance and acceptance of the end-to-end encryption together with the wider availability of the cryptographic primitives at the end points, increases the risk of malware distribution and attack. This risk may be mitigated by opening and inspecting the nature of the encrypted content.

C.4 Coercive control

ETSI TR 103 936 [i.17] identifies a large number of concerns regarding the misuse of devices and applications in the context of coercive control within intimate relationships often known as Consumer IoT Enabled abuses or Technology Facilitated Abuse (TFA). TFA behaviours include but are not limited to stalking and omnipresence, surveillance (wiretapping, bugging, videotaping, geolocation tracking, data mining, social media mapping, and the monitoring of data and traffic on the internet), intimidation, impersonation, humiliation, threats, consistent harassment/unwanted contact, sexting, and image-based sexual abuse.

Where the attacker is able to use encryption tools this may make it more difficult to identify the source and content of traffic that enables coercive control. It is recognized, and shown in ETSI TR 103 936 [i.17], that many capabilities offered by devices and applications are also legitimate and that not all invocations of them are malicious, rather it may be reasonably suggested that the majority of invocations are benign. The reasonable protection offered by such devices being accessible only over an encrypted connection is, as suggested reasonable. The countermeasure model identified in clause 7.4 of the present document of "{pervasive encryption, integrity, transparency and explicability}" should give assurance that the affected party has knowledge of the affecting party.

Annex D (informative): Application of Security and Privacy Controls

D.1 NIST

NIST 800-53 [i.23] provides *"... a catalog of security and privacy controls for information systems and organizations to protect organizational operations and assets, individuals, other organizations …*" from threats and possible attacks. The "*consolidated control catalog addresses security and privacy*" from two perspectives:

a) functionality, which includes control mechanisms; and

b) assurance, which includes confidence levels of security and privacy capabilities provided by the control mechanisms.

Annex E (informative): Bibliography

- Mbanaso and Cooper: "Conceptual Design of Obligation of Trust Protocol".

History

Version	Date	Status
V1.1.1	September 2025	Publication