ETSI GR ETI 001 V1.1.1 (2021-06)

GROUP REPORT

Encrypted Traffic Integration (ETI); Problem Statement

Disclaimer

The present document has been produced and approved by the Encrypted Traffic Inspection 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-001

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

Important notice

The present document can be downloaded from:
http://www.etsi.org/standards-search

The present document may be made available in electronic versions and/or in print. The content of any electronic and/or print versions of the present document shall not be modified without the prior written authorization of ETSI. In case of any existing or perceived difference in contents between such versions and/or in print, the prevailing version of an ETSI deliverable is the one made publicly available in PDF format at www.etsi.org/deliver.

Users of the present document should be aware that the document may be subject to revision or change of status. Information on the current status of this and other ETSI documents is available at https://portal.etsi.org/TB/ETSIDeliverableStatus.aspx

If you find errors in the present document, please send your comment to one of the following services:
https://portal.etsi.org/People/CommiteeSupportStaff.aspx

Notice of disclaimer & limitation of liability

The information provided in the present deliverable is directed solely to professionals who have the appropriate degree of experience to understand and interpret its content in accordance with generally accepted engineering or other professional standard and applicable regulations.
No recommendation as to products and services or vendors is made or should be implied.
No representation or warranty is made that this deliverable is technically accurate or sufficient or conforms to any law and/or governmental rule and/or regulation and further, no representation or warranty is made of merchantability or fitness for any particular purpose or against infringement of intellectual property rights.
In no event shall ETSI be held liable for loss of profits or any other incidental or consequential damages.

Any software contained in this deliverable is provided "AS IS" with no warranties, express or implied, including but not limited to, the warranties of merchantability, fitness for a particular purpose and non-infringement of intellectual property rights and ETSI shall not be held liable in any event for any damages whatsoever (including, without limitation, damages for loss of profits, business interruption, loss of information, or any other pecuniary loss) arising out of or related to the use of or inability to use the software.

Copyright Notification

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 Inspection (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.

1 Scope

The present document describes the problem arising from pervasive encrypted traffic in electronic/digital communications networks. 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 considers the role of compliance obligations on the development and deployment of encrypted traffic and how it impacts different stakeholders.

The purpose of the present document is to consider the impact of pervasive encryption on stakeholders, and 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 the problem from a primarily technical perspective.
- Clause 6 reviews some aspects of the integration of pervasive encryption to protocols in networks.
- Annex A provides a summary of the impact of pervasive encryption on various formal compliance obligations.
- Annex B gives an overview of the various common approaches to provide encryption in networks.
- Annex C offers a number of examples on the impact of pervasive encryption.

The present document is a report into the scope and scale of pervasive encryption in electronic/digital communications networks and the intended readership is all stakeholders. The document structure is intended to guide different readers to appropriate content.

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] 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.2] 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.3] 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.4] 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.5] 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.6] European Standardisation Regulation (EU) 1025/2012: "Regulation (EU) No 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".

[i.7] ETSI TR 103 456: "CYBER; Implementation of the Network and Information Security (NIS) Directive".

[i.8] ENISA: "Gaps in NIS standardisation Recommendations for improving NIS in EU standardisation policy" V.1.0, November 2016.

[i.9] ETSI TS 102 656: "Lawful Interception (LI); Retained Data; Requirements of Law Enforcement Agencies for handling Retained Data".

[i.10] ETSI TS 101 331: "Lawful Interception (LI); Requirements of Law Enforcement Agencies".

[i.11] ETSI TR 103 618: "CYBER; Quantum-Safe Identity-Based Encryption".

[i.12] ETSI TR 103 719: "CYBER; Guide to Identity Based Cryptography".

[i.13] ETSI TS 103 532: "CYBER; Attribute Based Encryption for Attribute Based Access Control".

[i.14] 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.15] ETSI TR 103 369: "CYBER; Design requirements ecosystem".

[i.16] ETSI TR 103 421: "CYBER; Network Gateway Cyber Defence".

[i.17] IETF RFC 8404: "Effects of Pervasive Encryption on Operators".

[i.18] U.S. Office of the Director of National Intelligence (ODNI): "Going Dark: Impact to intelligence and law enforcement and threat mitigation" (2017).

NOTE: Available at https://www.odni.gov/files/PE/Documents/10---2017-AEP_Going-Dark.pdf.

[i.19] Council of the European Union: "Resolution on Encryption - Security through encryption and security despite encryption" No. 13084/1/20, Brussels, 24 Nov 2020.

[i.21] Recommendation ITU-T X.800: "Security architecture for Open Systems Interconnection for CCITT applications".

[i.22] Tor project.

NOTE: Available at https://www.torproject.org/about/history/.

[i.23] EU Cyber Security Act (CSA): "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.24] 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.25] ETSI TR 102 661: "Lawful Interception (LI); Security framework in Lawful Interception and Retained Data environment".

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.15].

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.

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.25] 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

3.2 Symbols

Void.

3.3 Abbreviations

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

CEP	Communication End Point
CSP	Communications Service Provider
EDF	Ephemeral Diffie Helman
ENISA	European Network Information Security Agency
ETI	Encrypted Traffic Integration
EU	European Union
GDPR	General Data Protection Regulation
ICT	Information and Communications Technologies
IP	Internet Protocol

NIS	Network and Information Security
OS	Operating System
OSI	Open Systems Interconnection
PII	Person Identifying Information
QSC	Quantum Safe Cryptography
RED	Radio Equipment Directive
TE	Terminal Equipment
UE	User Equipment
VPN	Virtual Private Network
WPA	WiFi Protected Access

4 Roles of encryption in networks

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

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

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 is 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 are they 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. 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 itis 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 mapping is used:

- **Encryption** - as defined in ETSI TS 103 532 [i.13], transformation of data by a cryptographic algorithm to produce a ciphertext, i.e. to hide the information content of the data. If data is encrypted it can only be seen by the entity with the key.
- **Trust** - as defined in ETSI TS 103 532 [i.13] is the level of confidence in the reliability and integrity of an entity to fulfil specific responsibilities. If a network cannot fulfil its obligations because it cannot access data in encrypted content, it will become less trusted. The concern in this case is that as trust in the network is lowered more encryption from outside the control of the network is then applied, thus further degrading the trust.
- **Integrity** - as defined in Recommendation ITU-T X.800 [i.21], when referring to data, is a property that data has not been altered or destroyed in an unauthorized manner. In wider discourse integrity is often placed in an ethical context to refer to honesty and, to an extent, trustworthiness. In the telecommunications domain the term systems integrity is often used to mean the property that data and the methods of handling the data cannot be altered or destroyed in an unauthorized manner. The role of pervasive encryption can lead to operations which are sanctioned or authorized to enable maintenance of systems integrity by the operator are no longer available to the operator.

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.

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 exposes users to threats from malicious traffic which, 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 end user. 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 firewalls in combination with other network management systems to remove malicious traffic.

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.16], [i.17] and [i.19]). Additionally, pervasive encryption poses significant difficulties for government authorities and imposition of requirements on communication service providers as documented in references [i.18] and [i.10].

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.

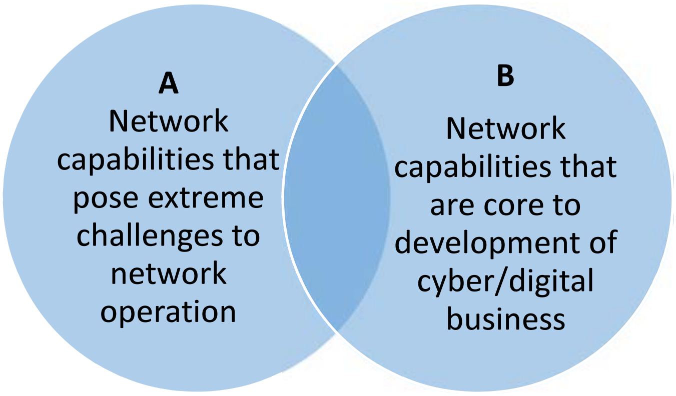

A
Network capabilities that pose extreme challenges to network operation
B
Network capabilities that are core to development of cyber/digital business

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.

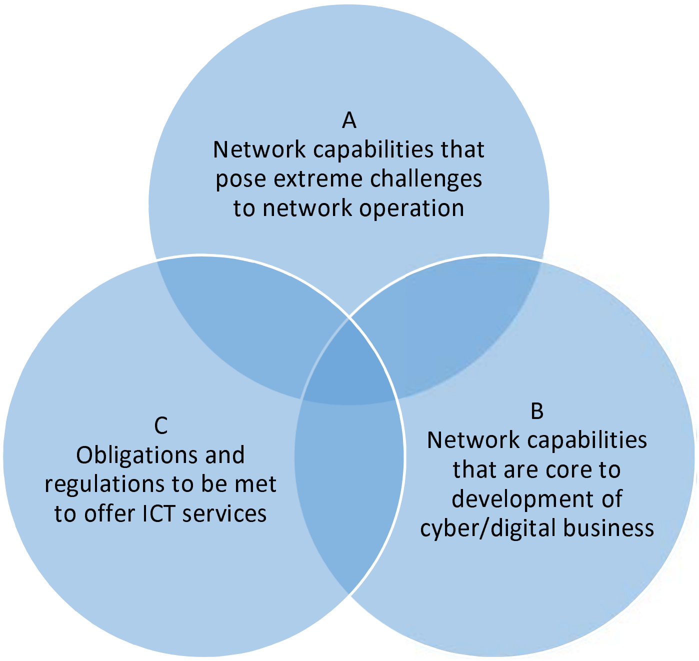

A
Network capabilities that pose extreme challenges to network operation
C
Obligations and regulations to be met to offer ICT services
B
Network capabilities that are core to development of cyber/digital business

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 [i.9], ETSI TS 101 331 [i.10], the GDPR [i.1], obligations under the NIS [i.2] directive and the Cyber Security Act [i.23], 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 "C", can be found in Annex A of the present document.

6 Technical view of the problem of ETI

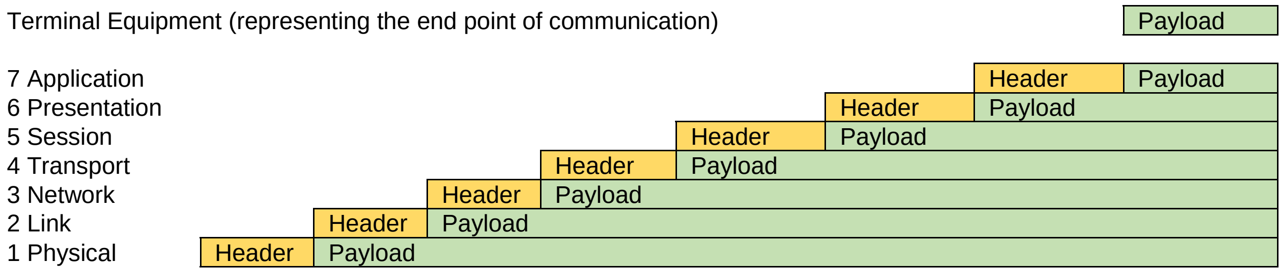
6.1 Simplified network model

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.3]) 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.3]) 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.22]. 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.

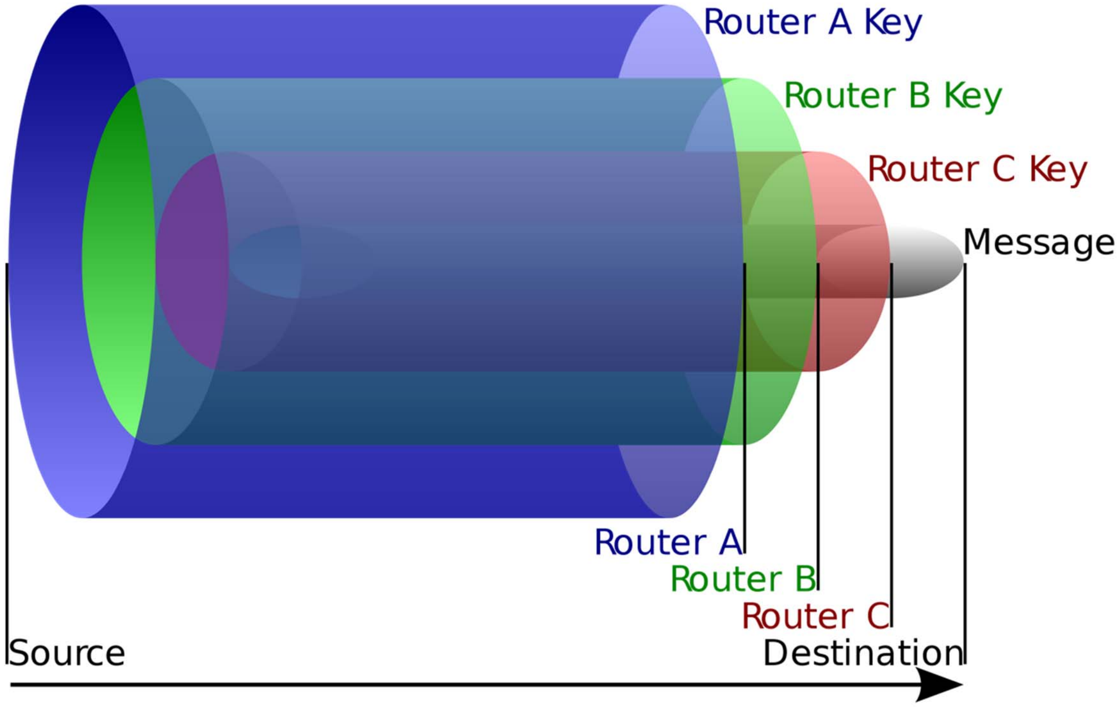


Figure 4: Layer overlaid on layer model as seen in VPNs and onion-routing

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

6.3.1 Adversarial stakeholders

In very simple terms 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, or adversary. 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 key to the success of network management.

Annex A: Compliance Obligation Examples

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.15].

A.2 EU GDPR

The General Data Protection Regulation (GDPR) [i.1] 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 NIS Directive

The Network and Information Security Directive (NIS Directive) [i.2] applies in particular to two forms of commercial entity:

1) Operators of essential services

2) Digital service providers

In ETSI TR 103 456 [i.7] and in the ENISA report on gaps in NIS standardisation [i.8] a wide overview of the impact of the NIS Directive [i.2] 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.2] 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.2] when end-to-end encryption is deployed.

In broad outline the purpose of the NIS Directive [i.2] 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.2] 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 recently adopted the "Council Resolution on Encryption - Security through encryption and security despite encryption" [i.19]. 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.23] 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.5] 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 mention 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 (network security elements may be activated)

The Radio Equipment Directive 2014/53/EU ("RED") [i.4] 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.4] and the European Standardisation Regulation (EU) 1025/2012 [i.6], the Commission is empowered to adopt measures that determine access to markets.

For the bulk of the RED [i.4] only radio aspects are considered and the test conditions are specified in Harmonised ENs. However, there are aspects of the RED [i.4] that address security and privacy that may be impacted by end-to-end encryption.

A.8 Lawful access to communication and communications data

ETSI TS 102 656 [i.9] and ETSI TS 101 331 [i.10] 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*.

Annex B: 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.11], ETSI TR 103 719 [i.12]).
    - Attribute based encryption (see ETSI TS 103 532 [i.13], ETSI TS 103 458 [i.14]).
- 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 methodsidentical 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 WiFi™ networks, and use of Ephemeral Diffie Helman (EDF) in key exchanges.

Annex C: 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.18] as a major concern for law enforcement.

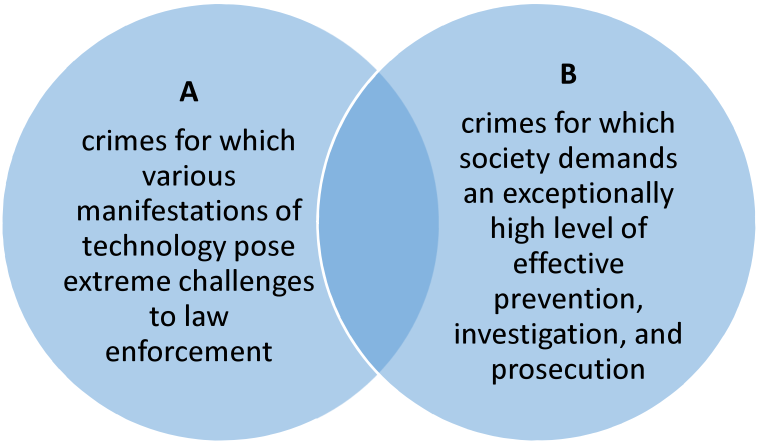

A
crimes for which various manifestations of technology pose extreme challenges to law enforcement
B
crimes for which society demands an exceptionally high level of effective prevention, investigation, and prosecution

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. 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.24], 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 by 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.

History

Document history		
V1.1.1	June 2021	Publication