ETSI TR 103 370 V1.1.1 (2019-01)

Practical introductory guide to Technical Standards for Privacy

Reference
DTR/CYBER-0010

Keywords
confidentiality, privacy

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 - NAF 742 C
Association à but non lucratif enregistrée à la
Sous-Préfecture de Grasse (06) N° 7803/88

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

Contents

Intellectual Property Rights

Essential patents

IPRs essential or potentially essential to normative deliverables may have been declared to ETSI. The information pertaining to these essential IPRs, if any, is 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 IPR Policy, no investigation, 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.

Foreword

This Technical Report (TR) has been produced by ETSI Technical Committee Cyber Security (CYBER).

Modal verbs terminology

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

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

Executive summary

The present document has been prepared in response to Mandate M/530 [i.9] and presents a guide to the application of standards in the implementation of privacy management. The present document has been structured in four parts to achieve the goals of the Mandate:

Part 1: Privacy terms and definitions based on existing documents.

Part 2: Status of standardization work considering existing or future work in ISO, CEN/CENELEC, ETSI and other bodies - identification of the basic building blocks.

Part 3: General principles how to introduce privacy management in equipment, services and solutions.

Part 4: Application of the principles for privacy by design to some examples:

- Least to know/collect.
- Data/privacy protection and data brokering (especially considering aggregated data, here in many legal systems it is the case that applying advanced algorithms on open data may result in private data).
- The right to be forgotten.

In addition, the present document identifies gaps in standardization and makes a number of recommendations for addressing those gaps.

1 Scope

The present document gives a guide to the use of standards to assist in the management of privacy. The present document contains the following key elements:

- Table 1 contains a collation of terms related to data protection and privacy from selected SDOs and comparison to the GDPR [i.1].
- Privacy terms and definitions based on existing documents (ISO, ENISA, and others).
- Status of standardization work including consideration of existing or future work in ISO, CEN/CENELEC, ETSI and other bodies.
- Identification of the basic building blocks and main principles for privacy protection and their mapping to available standards.
- Fundamental privacy by design principles that are commonly recognized.
- Examples of application of the privacy by design principles.

In addition, the present document identifies gaps in standardization and makes several recommendations for addressing those gaps.

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] European Convention of Human Rights.

NOTE: Available at www.echr.coe.int.

[i.3] Universal Declaration of Human Rights.

NOTE: Available at http://www.un.org/en/universal-declaration-human-rights/.

[i.4] ETSI TS 103 486: "CYBER; Identity management and naming schema protection mechanisms".

[i.5] ETSI TS 103 485: "CYBER; Mechanisms for privacy assurance and verification".

[i.6] ETSI TR 187 010: "Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); NGN Security; Report on issues related to security in identity imanagement and their resolution in the NGN".

[i.7] ISO/IEC 29100:2011 amended by ISO/IEC 29100:2011/Amd 1:2018: "Information technology -- Security techniques -- Privacy framework".

[i.8] ISO/IEC 29191:2012: "Information technology -- Security techniques -- Requirements for partially anonymous, partially unlinkable authentication".

[i.9] M/530 Commission Implementing Decision C(2015) 102 final of 20.1.2015 on a standardisation request to the European standardisation organisations as regards European standards and European standardisation deliverables for privacy and personal data protection management pursuant to Article 10(1) of Regulation (EU) No 1025/2012 of the European Parliament and of the Council in support of Directive 95/46/EC of the European Parliament and of the Council and in support of Union's security industrial policy.

[i.10] Article 29 Data Protection Working Party, Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in a high risk" for the purposes of Regulation 2016/679.

[i.11] ETSI TS 103 532: "CYBER; Attribute Based Encryption for Attribute Based Access Control".

[i.12] Charter of Fundamental Rights of the European Union.

[i.13] ISO/IEC 29134:2017: "Information technology -- Security techniques -- Guidelines for privacy impact assessment".

[i.14] ISO/IEC 27001:2013: "Information technology -- Security techniques --Information security management systems - Requirements".

[i.15] ISO/IEC 27552: 2019: "Extension to ISO/IEC 27001 and ISO/IEC 27002 for privacy information management - Requirements and guidelines (PIMS)".

NOTE: At the time of publication of the present document ISO/IEC 27552 is not yet published.

[i.16] ETSI TR 103 305-5: "CYBER; Critical Security Controls for Effective Cyber Defence; Part 5: Privacy enhancement".

[i.17] ETSI TS 102 165-1: "CYBER; Methods and protocols; Part 1: Method and pro forma for Threat, Vulnerability, Risk Analysis (TVRA)".

[i.18] ETSI TR 103 305-1: "CYBER; Critical Security Controls for Effective Cyber Defence; Part 1: The Critical Security Controls".

[i.19] ETSI GS NFV-SEC 006: "Network Functions Virtualisation (NFV); Security Guide; Report on Security Aspects and Regulatory Concerns".

[i.20] ISO/IEC 15408 series: "Information technology -- Security techniques -- Evaluation criteria for IT security".

[i.21] ISO/IEC 20889:2018: "Privacy enhancing data de-identification terminology and classification of techniques".

[i.22] ISO/IEC 29151:2017: "Information technology -- Security techniques -- Code of practice for personally identifiable information protection".

[i.23] ISO/IEC 27018:2014: "Information technology -- Security techniques -- Code of practice for protection of personally identifiable information (PII) in public clouds acting as PII processors".

[i.24] ISO/IEC CD 29184: "Information technology -- Online privacy notices and consent" (under develpment).

[i.25] ISO/IEC PDTR 27550: "Information technology -- Security techniques -- Privacy engineering" (under develpment).

[i.26] ISO/IEC 29146:2016: "Information technology -- Security techniques -- A framework for access management".

[i.27] ISO/IEC 29190:2015: "Information technology -- Security techniques -- Privacy capability assessment model".

[i.28] ISO/IEC 27002:2013: "Information technology -- Security techniques -- Code of practice for information security controls".

[i.29] Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications).

3 Definition of terms, symbols and abbreviations

3.1 Terms

For the purposes of the present document, the terms given in clause 4 apply.

3.2 Symbols

Void.

3.3 Abbreviations

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

ABE	Attribute Based Encryption
DPIA	Data Protection Impact Assesment
EC	European Commission
ECHR	European Court of Human Rights
ENISA	European Union Agency for Network and Information Security
GDPR	General Data Protection Regulation
ICT	Information and Communication Technology
IOT	Internet Of Things
ISMS	Information Security Management System
ISO	International Standard Organization
IV	Initial Value
NGP	Next Generation Protocol
PET	Privacy Enhancing Technology
PIA	Privacy Impact Assessment
PII	Personally Identifiable Information
PIMS	Privacy Impact Management System
TE	Terminal Equipment
TEDDI	Terms and Definitions Database Interactive
TS	Technical Specification
UDHR	Universal Declaration of Human Rights

4 Glossary of terms

4.1 Collation of terms

Table 1 presents a general collation of the terms from a small set of primary sources of the terms used in addressing privacy in standards. The primary sources that have been used to build this collation are:

- Regulation (EU) 2016/679 (GDPR) [i.1];
- ISO/IEC 29000 series [i.8], [i.7] and [i.13];

- ISO/IEC 15408 series [i.20];
- ISO/IEC 20889 [i.21]; and
- ETSI TEDDI repository https://webapp.etsi.org/Teddi/.

Table 1: Collation of terms related to data protection and privacy from selected SDOs and comparison to the GDPR

Term	Definition	Source of definition	Remarks
anonymity	characteristic of information that does not permit a personally identifiable information principal to be identified directly or indirectly	ISO/IEC 29100	To determine whether an individual is identifiable, account should be taken of all the means likely reasonably to be used by the entity holding the data or by any other party, to identify that individual
	principle whereby ones identity is withheld from other parties (see note 1)	ETSI TEDDI, group NA	Identical text
	'Anonymity' is the principle whereby ones identity is withheld from other parties (see note 1)	ETSI TEDDI, group SMG	
	ability of a user to use a resource or service without disclosing the user's identity (see note 2)	ETSI TEDDI, group ITS	Derived from ISO/IEC 15408-2
	act of ensuring that a user may use a resource or service without disclosing the user's identity (see note 2)	ETSI TEDDI, group SMG	
anonymization	process by which personally identifiable information (PII) is irreversibly altered in such a way that a PII principal can no longer be identified directly or indirectly, either by the PII controller alone or in collaboration with any other party	ISO/IEC 29100	
	process that replaces an actual identifier with an attribute obtained by randomization or generalization in such a way that there is a reasonable level of confidence that no individual can be identified	ETSI TEDDI, group CYBER	
de-anonymization	Any process in which anonymous data is cross-referenced with other sources of data to re-identify the anonymous data source	ETSI TEDDI, group CYBER ISO/IEC 20889	
anonymized data	data that has been produced as the output of a personally identifiable information anonymization process		
de-identification	process of removing the association between a set of identifying data and the data principal	ISO/IEC 20889	

Term	Definition	Source of definition	Remarks
enterprise	natural or legal person engaged in an economic activity, irrespective of its legal form, including partnerships or associations regularly engaged in an economic activity	GDPR	See also 'undertakings' in GDPR
	unit of economic organization or activity, especially a business organization	ETSI TEDDI groups 3GPP&TISPAN	
identifiability	condition which results in a personally identifiable information (PII) principal being identified, directly or indirectly, on the basis of a given set of PII		
identifier	set of attribute values that unambiguously distinguish one entity from another one in a given context		
	total list of attribute values of an entity that allows this entity to be unambiguously distinguished from all other entities within a context and to be recognized as a single identity in that specific context		Appears to overlap with definition of identity below
	means of indicating a point of contact, intended for public use such as on a business card. Telephone numbers, email addresses, and typical home page URLs are all examples of identifier in other systems	ETSI TEDDI, group 3GPP	
	series of digits, characters and symbols used to identify uniquely subscriber(s), user(s), network element(s), function(s) or network entity(ies) providing services/applications	ETSI TEDDI, group TISPAN	
	user's name and optionally a password		
	attribute or a set of attributes of an entity which uniquely identifies the entity within a certain context	ETSI TEDDI, group ITS	
	series of digits, characters and symbols or any other form of data used to identify subscriber(s), user(s), network element(s), function(s), network entity(ies) providing services/applications, or other entities (e.g. physical or logical objects)	ETSI TEDDI, group NGP	
	user identification (name and, where appropriate, password) which can be supplied during the call in order to indicate entitlements with regard to operations on files	ETSI TEDDI, group TE	

Term	Definition	Source of definition	Remarks
identity	set of attributes which make it possible to identify the personally identifiable information principal		
	technical label which may represent the origin or destination of any telecommunications traffic, as a rule clearly identified by a physical telecommunications identity number (such as a telephone number) or the logical or virtual telecommunications identity number (such as a personal number) which the subscriber can assign to a physical access on a case-by-case basis	ETSI TETRA	
	attributes by which an entity or person is described, recognized or known	ETSI TEDDI, group OCG	
	data or information (identifier) that are used to distinguish one object or person from others. These data can take many forms, and also a single object or person may have different identities associated. Authentication can be used to verify purported identities. An identity, which has been so verified, is called an authenticated identity	ETSI TEDDI, group HF	
	essence of an entity and often described by its characteristics	ETSI TEDDI, group BROADCAST	
	identifier allocated to a particular entity, e.g. a particular end-user, provides an Identity for that entity	ETSI TEDDI, group TISPAN	
	a system unique tag applied to an entity	ETSI TEDDI, group SMG	
	information about an entity that is sufficient to identify that entity in a particular context	ETSI TEDDI, group NGP	
opt-in	process or type of policy whereby the personally identifiable information (PII) principal is required to take an action to express explicit, prior consent for their PII to be processed for a particular purpose (see note 7)	ISO/IEC 29100	