ETSI TR 103 304 V1.1.1 (2016-07)

CYBER;
Personally Identifiable Information (PII) Protection in mobile and cloud services

Reference

DTR/CYBER-0002

Keywords

access control, 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 only prevailing document is the print of the Portable Document Format (PDF) version kept on a specific network drive within ETSI Secretariat.

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

IPRs essential or potentially essential to the present document 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.

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

ICT is moving towards a genuinely distributed and virtualized environment characterized by a rich set of mobile and cloud services available to users. In this context, it may be difficult to have a priori knowledge of who may need access to data, when and where this may happen and whether that data could be or contain Personally Identifiable Information (PII). The present document proposes a number of scenarios focusing on today's ICT and develops an analysis of possible threats related to PII in mobile and cloud based services. It also presents technical challenges and needs derived from regulatory aspects (lawful interceptions). The aim is to consolidate a general framework, in line with regulation and international standards, on top of which technical solutions for PII protection can be developed.

1 Scope

The present document proposes a number of scenarios focusing on today's ICT and develops an analysis of possible threats to Personally Identifiable Information (PII) in mobile and cloud based services. It also presents technical challenges and needs derived from regulatory aspects (lawful interceptions). It consolidates a general framework, in line with regulation and international standards, where technical solutions for PII protection can be plugged into.

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] ISO/IEC 29100:2011: "Information technology - Security techniques - Privacy framework".

[i.2] National Institute of Standards and Technology NIST SP 800-122: "Guide to Protecting the Confidentiality of Personally Identifiable Information (PII)".

[i.3] Regulation 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC.

[i.4] Regulation 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.5] Directive 2002/21/EC of the European Parliament and of the council of 7 March 2002 on a common regulatory framework for electronic communications networks and services (Framework Directive).

[i.6] Directive 2002/22/EC of the European Parliament and of the Council of 7 March 2002 on Universal service and users' rights relating to electronic communications networks and services (Universal Service Directive - OJ L 108, 24.04.2002).

[i.7] Directive 1999/5/EC of the European Parliament and of the Council of 9 March 1999 on radio equipment and telecommunications terminal equipment and the mutual recognition of their conformity.

[i.8] Directive 1995/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data.

[i.9] US President's Council of Advisors on Science and Technology: "Report to the president. Big data and privacy: a technological perspective".

[i.10] ETSI TR 101 567: "Lawful Interception (LI); Cloud/Virtual Services for Lawful Interception (LI) and Retained Data (RD)".

[i.11] ETSI Cloud Standards Coordination: Final Report.

[i.12] ISO/IEC 11889:2009: "Information technology - Trusted Platform Module" (Parts 1-4).

[i.13] ISO/IEC 29191:2012: "Requirements for partially anonymous, partially unlinkable authentication".

[i.14] ISO/IEC 29115:2011: "Entity authentication assurance framework".

[i.15] ETSI TS 119 612: "Electronic Signatures and Infrastructures (ESI); Trusted Lists".

[i.16] ETSI TR 103 308: "CYBER; Security baseline regarding LI and RD for NFV and related platforms".

[i.17] 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.18] ISO/IEC 27040:2015: "Information technology - Security techniques - Storage security".

[i.19] ISO/IEC 17789:2014: "Information technology - Cloud computing - Reference architecture".

[i.20] ISO/IEC 9594-8:2014: "Information technology - Open Systems Interconnection - The Directory - Part 8: Public-key and attribute certificate frameworks".

[i.21] ETSI TS 101 331: "Lawful Interception (LI); Requirements of Law Enforcement Agencies".

[i.22] ETSI TS 101 671: "Lawful Interception (LI); Handover interface for the lawful interception of telecommunications traffic".

[i.23] ISO/IEC JTC 1/SC 38 CD 19944: "Information technology - Cloud computing - Data and their flow across devices and cloud services".

NOTE: Standard under development.

[i.24] ISO/IEC JTC 1/SC 37 AWI 20889: "Information technology - Security techniques - Privacy enhancing data de-identification techniques".

NOTE: Standard under development.

[i.25] J.A. Akinyele, C. U. Lehmanny et Al. Self-Protecting Electronic Medical Records: Using Attribute-Based Encryption. Cryptology ePrint Archive, Report 2010/565. 2010.

3 Definitions and abbreviations

3.1 Definitions

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

app: "software application", typically running on a user's device platform

anonymization: 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

Cloud Service Customer: individual or organization consuming one or more cloud services provided by a Cloud Service Provider

Cloud Service Partner: individual or organization providing support to the provisioning of cloud services by the Cloud Service Provider, or to the consumption of cloud service by the Cloud Service Customer

Cloud Service Provider: individual or organization providing cloud services to one or more Cloud Service Customers

Cloud Service user: individual consuming one or more cloud services using a particular device

consent: freely given specific and informed indication of his wishes by which the data subject signifies his agreement to personal data relating to him being processed

data breach: compromise of security that leads to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to protected data transmitted, stored or otherwise processed [i.18]

data consumer: entity accessing data for a given purpose

data fusion: process of combining multiple data sets into one improved data set in order to discover any information which cannot be derived from the original data sources

data subject: identifiable person, i.e. a person who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity

de-anonymization: any process in which anonymous data is cross-referenced with other sources of data to re-identify the anonymous data source

Device Platform Provider: Cloud Service Provider providing services necessary to support the device platform

generalization: process that reduces the degree of granularity (known as precision) of a set of attributes

identity theft: inappropriate use of someone else's credentials to commit fraud or crimes

lock-in: process which makes a customer dependent on a given service provider and unable to use another provider without substantial switching costs

metadata: data about the data, which can be structural or descriptive

mis-contextualization: process in which data from different personas is mixed and used inappropriately

over-collection: practice of collecting information unrelated to a stated purpose

persona: role played by an individual user in the context of a service

Personally Identifiable Information (PII): any information that (a) can be used to identify the PII principal to whom such information relates, or (b) is or might be directly or indirectly linked to a PII principal

NOTE 1: To determine whether a PII principal is identifiable, account can be taken of all the means which can reasonably be used by the privacy stakeholder holding the data, or by any other party, to identify that natural person [i.1].

NOTE 2: In the US, according to [i.2]: any information about an individual maintained by an agency, including any information that can be used to distinguish or trace an individual's identity, such as name, social security number, date and place of birth, mother's maiden name, or biometric records; and any other information that is linked or linkable to an individual, such as medical, educational, financial, and employment information.

PII controller: privacy stakeholder that determines the purposes and means for processing personally identifiable information (PII) other than natural persons who use data for personal purposes [i.1]

PII principal: natural person to whom the personally identifiable information (PII) relates [i.1]

PII processor: privacy stakeholder that processes personally identifiable information (PII) on behalf of and in accordance with the instructions of a PII controller [i.1]

portability: usability of the same software, data or metadata in different environments

processing of PII: operation or set of operations performed upon personally identifiable information (PII) [i.1]

NOTE: Examples of processing operations of PII include, but are not limited to, the collection, storage, alteration, retrieval, consultation, disclosure, anonymization, pseudonymization, dissemination or otherwise making available, deletion or destruction of PII) [i.1].

pseudonymization: process that replaces an actual identifier with an alias ensuring that it cannot be reverted by reasonable effort of anyone (other than the party providing them)

randomization: process that reduces the degree to which data reflects the true value of a set of attributes (known as accuracy)

ransomware: type of malware that restricts access to the infected device, demanding that the user pay a ransom to the malware operators to remove the restriction

re-identification: action performed on de-identified data with the purpose of re-linking the information to a person or group of persons

secure data deletion: irreversible destruction of electronic data so that no party is capable of recovering

spyware: type of malware that collects/intercepts/retrieves data from a (mobile) device and sends it to a remote (Command&Control) server

Terminal Equipment: product enabling communication or relevant component thereof which is intended to be connected directly or indirectly by any means whatsoever to interfaces of public telecommunications networks

traceability: ability to interrelate individuals in a way that is verifiable

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

unlinkability: act of ensuring that a user may make multiple uses of resources or services without others being able to link these uses together

3.2 Abbreviations

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

5G-PPP	5G Infrastructure Public Private Partnership
ABE	Attribute-Based Encryption
API	Application Programming Interface
AWI	Approved Work Item

NOTE: http://www.iso.org/iso/home/faqs/faqs_abbreviations.htm.

BYOD	Bring Your Own Device
CA	Certification Authority
CD	Committee Draft
CEO	Chief Executive Officer
CP-ABE	Ciphertext Policy Attribute-Based Encryption
CPU	Central Processing Unit
CSC	Cloud Service Customer
CSP	Cloud Service Provider
CSPa	Cloud Service Partner
Csu	Cloud Service user
DPP	Device Platform Provider
EC	European Community
EU	European Union
GPS	Global Positioning System
GSM	Global System for Mobile
ICT	Information and Communication Technology
IMEI	International Mobile Station Equipment Identity
IMSI	International Mobile Subscriber Identity
ISO	International Organization for Standardization
JTC	Joint Technical Committee
LEA	Law Enforcement Authority
LI	Lawful Interception
PC	Personal Computer
PII	Personally Identifiable Information
PIN	Personal Identification Number
PKI	Public Key Infrastructure
PLMN	Public Land Mobile Network
PNR	Passenger Name Record

PUA	Potentially Unwanted Application
RAM	Random Access Memory
SAREF	Smart Appliances REFerence ontology
SC	Subcommittee
SMS	Short Message Service
TE	Terminal Equipment
TEE	Trusted Execution Environment
TPM	Trusted Platform Module
TS	Technical Specifications
UMTS	Universal Mobile Telecommunications System
US	United States

4 Overview

An even growing number of human activities are today performed using Internet-based (and particularly, cloud-based) services. Information that can be used to identify a natural person or might be directly or indirectly linked to her, known in literature as Personally Identifiable Information (PII) may be potentially present in almost all these activities. While technology is apparently "disappearing" to naive eyes, as people are focusing on services regardless of the devices, terminals or platforms they actually use, awareness of data transaction and transparency about its use is decreasing. This may cause social and legal concerns when data transactions may involve PII.

Code of practices and regulatory aspects protecting PII were present since the advent of mobile communications in middle 1990s. Directive 95/46/EC (data protection) [i.8], directive 2002/58/EC (privacy) [i.7], and Directive 99/5/EC (radio equipments) [i.5], [i.6], for instance, state the legal obligations to preserve a user's control of their identity in electronic communication, as well as obligations intended to avoid frauds. Properly using identifiers and identity management as suggested in previous ETSI TR 187 010 [i.17] massively reduces the risk to exploit of PII in traditional communication signalling.

However, today the ICT is moving towards a genuinely distributed and virtualized environment characterized by a rich set of mobile and cloud services available to users. The eIDAS Regulation [i.3] first and the EU General Data Protection Regulation [i.4] then have provided a legal framework to address challenges raising from the digital age and its "app economy", in order to booster citizen's trust in the emerging Digital Single Market.

In fact, differently from previous telecom scenario where user data was mostly accessible from network functional elements, several kinds of information are today easily accessible from terminal equipments or end user devices, through open and specialized Application Programming Interface (API). Thus, it may be difficult to have a priori knowledge of who may need access to users' data, when and where this may happen and whether that data could be or contain PII.

PII in long term data records (e.g. in health, public administration, education, financial and legal domains) are dynamic and grow over the life of an individual. The set of actors/individuals/roles that need to access and amend it over a lifetime is potentially unlimited. It is also not reasonable to expect the record to be "a single document" rather to likely appear as a large set of data, retained in data centres located in many different national Countries and managed by various stakeholders with different levels of trust. In such records there may be a need to enable security controls of some complexity.

The present document proposes a number of scenarios focusing on today's ICT and develops an analysis of possible threats related to PII in mobile and cloud based services.

5 Threats to PII

5.1 Overview

This clause presents threats derived from the analysis of the scenarios reported in Annex A. The scenarios are not exhaustive rather they are representative of most common and relevant situations.

Threats sources may include accidents, natural disasters, humans authorized or unauthorized to access data and systems. A synopsis relating threats with risks and vulnerabilities is provided in table 5.1.