ETSI TR 187 012 V2.1.1 (2009-11)

Technical Report

Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); NGN Security; Report and recommendations on compliance to the data retention directive for NGN-R2

iTeh STANDARD PREVIEW
(standards.iteh.ai)
Full standard:
https://standards.iteh.ai/catalog/standards/sist/126e3f66-b118-418c-b432-1c1c4027099b/etsi-tr-187-012-v2.1.1-2009-11

Reference
DTR/TISPAN-07032-NGN-R2

Keywords
data, retention

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

iTeh STANDARD PREVIEW
(standards.iteh.ai)
Full standard:
https://standards.iteh.ai/catalog/standards/sist/12fe3f66-b148-41c6-a432-f41c4027099b/etsi-tr-187-012-v2.1.1-2009-11

Important notice

Individual copies of the present document can be downloaded from:
http://www.etsi.org

The present document may be made available in more than one electronic version or in print. In any case of existing or perceived difference in contents between such versions, the reference version is the Portable Document Format (PDF). In case of dispute, the reference shall be the printing on ETSI printers of the 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
http://portal.etsi.org/tb/status/status.asp

If you find errors in the present document, please send your comment to one of the following services:
http://portal.etsi.org/chaircor/ETSI_support.asp

Copyright Notification

No part may be reproduced except as authorized by written permission.
The copyright and the foregoing restriction extend to reproduction in all media.

© European Telecommunications Standards Institute 2009.
All rights reserved.

DECT™, **PLUGTESTS**™, **UMTS**™, **TIPHON**™, the TIPHON logo and the ETSI logo are Trade Marks of ETSI registered for the benefit of its Members.
3GPP™ is a Trade Mark of ETSI registered for the benefit of its Members and of the 3GPP Organizational Partners.
LTE™ is a Trade Mark of ETSI currently being registered
for the benefit of its Members and of the 3GPP Organizational Partners.
GSM® and the GSM logo are Trade Marks registered and owned by the GSM Association.

Contents

iTeh STANDARD PREVIEW
(standards.iteh.ai)
Full standard:
https://standards.iteh.ai/catalog/standards/sist/126e3f66-b118-418c-b432-1cf0c2270ffb/etsi-tr-187-012-v2.1.1-2009-11

iTeh STANDARD PREVIEW
(standards.iteh.ai)
Full standard:
https://standards.iteh.ai/catalog/standards/sist/126e3f66-b118-418c-b432-1c1c4027099b/etsi-tr-187-012-v2.1.1-2009-11

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 (http://webapp.etsi.org/IPR/home.asp).

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 Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN).

iTeh STANDARD PREVIEW
(standards.iteh.ai)
Full standard:
https://standards.iteh.ai/catalog/standards/sist/126e3f66-b118-418c-b432-1c1c4027099b/etsi-tr-187-012-v2.1.1-2009-11

1 Scope

The present document identifies the impact on the NGN in achieving compliance to the data retention directive [i.1]. The present document makes a number of recommendations to operators and manufacturers that may be sufficient to ensure compliance, and identifies where future standardisation may be required.

The present document applies to TISPAN NGN services as specified by TR 180 001 [i.12] (for release 1 specific capabilities) and TR 180 002 [i.13] (for release 2 specific capabilities), and where the NGN user is identified as specified in TS 184 002 [i.11].The present document is structured in the following way:

- NGN analysis with respect to Data Retention:
  - annex containing an analysis of the existing Directive and the available provisions in the NGN;
  - annex providing a comparison of terms between Directive and NGN.
- Identification of the data that is expected to be retained in the NGN under the DR Directive and a mapping to determine if the data is available in the NGN.

The present document does not define the handover domain which is specified in TS 102 657 [i.2] nor does the document cover any conformance aspects relating to IMS. However where other standards bodies are directly impacted by the DR Directive in the NGN the present document identifies in outline form the affected publications from such SDOs.

The present document does not address the application of Data Retention in Customer Premises Networks (CPN) or Next Generation Corporate Networks (NGCN).

iTeh STANDARD PREVIEW
(standards.iteh.ai)
Full standard:
https://standards.iteh.ai/catalog/standards/sist/126e3f60-b118-448c-ba32-1c1c4227099b/etsi-tr-187-012-v2.1.1-2009-11

2 References

References are either specific (identified by date of publication and/or edition number or version number) or non-specific.

- For a specific reference, subsequent revisions do not apply.
- Non-specific reference may be made only to a complete document or a part thereof and only in the following cases:
  - if it is accepted that it will be possible to use all future changes of the referenced document for the purposes of the referring document;
  - for informative references.

Referenced documents which are not found to be publicly available in the expected location might be found at http://docbox.etsi.org/Reference.

NOTE: While any hyperlinks included in this clause were valid at the time of publication ETSI cannot guarantee their long term validity.

2.1 Normative references

The following referenced documents are not essential to the use of the present document but they assist the user with regard to a particular subject area. For non-specific references, the latest version of the referenced document (including any amendments) applies.

Not applicable.

2.2 Informative references

The following referenced documents are not essential to the use of the ETSI deliverable but they assist the user with regard to a particular subject area. For non-specific references, the latest version of the referenced document (including any amendments) applies.

[i.1] Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC.

[i.2] ETSI TS 102 657: "Lawful Interception (LI); Retained data handling; Handover interface for the request and delivery of retained data".

[i.3] ETSI TS 102 656: "Lawful Interception (LI); Retained Data; Requirements of Law Enforcement Agencies for handling Retained Data".

[i.4] 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).

[i.5] Recommendation of the OECD Council in 1980 concerning guidelines governing the protection of privacy and transborder flows of personal data (the OECD guidelines for personal data protection.

[i.6] Directive 95/46/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.7] ETSI ES 282 001: "Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); NGN Functional Architecture".

[i.8] ETSI SR 002 211 (V1.1.1): "List of standards and/or specifications for electronic communications networks, services and associated facilities and services; in accordance with Article 17 of Directive 2002/21/EC".

[i.9] ETSI TR 102 661: "Lawful Interception (LI); Security framework in Lawful Interception and Retained Data environment".

[i.10] ETSI TS 187 005: "Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); NGN Release 2 Lawful Interception; Stage 1 and Stage 2 definition".

[i.11] ETSI TS 184 002: "Telecommunications and Internet Converged Services and Protocols for Advanced Networking (TISPAN); Identifiers (IDs) for NGN".

[i.12] ETSI TR 180 001: "Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); NGN Release 1; Release definition".

[i.13] ETSI TR 180 002: "Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); Release 2 definition".

[i.14] 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.15] ETSI TS 187 001: "Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); NGN SECurity (SEC); Requirements".

iTeh STANDARD PREVIEW
(standards.iteh.ai)
https://standards.iteh.ai/catalog/standards/sist/115e3f6f-b11f-418c-b432-1c1c402109ab/etsi-tr-187-012-2.1.1-2009-11

3 Definitions and abbreviations

3.1 Definitions

For the purposes of the present document, the terms and definitions given in Directive 2006/24/EC [i.1], TS 102 657 [i.2] and the following apply:

Point of Retention (PoR): NGN Functional Entity that is assigned to retain a particular data item

NOTE: In any implementation a data element may appear at multiple NGN FEs per retention event and in practice should only be retained once per retention event. Satisfying this recommendation may require that particular NGN FEs may be assigned as the primary or master point of retention for a particular data item.

retention event: event triggered by an NGN user giving rise to the retention of data as defined by the data retention directive [i.1] or by national law

3.2 Abbreviations

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

AN	Access Network
CPN	Customer Premises Networks
CSCF	Call Session Control Function
CSP	Communications Service Provider
DNS	Domain Name System
DR	Data Retention
ECN	Electronic Communications Network
ECN&S	Electronic Communications Network and Services
ECS	Electronic Communications Service
FE	Functional Entity
HI	Handover Interface
HLR	Home Location Record
HSS	Home Subscriber Server
IMS	IP Multimedia Subsystem
IP	Internet Protocol
LEA	Law Enforcement Authority
LI	Lawful Interception
NASS	Network Access Sub-System
NGCN	Next Generation Corporate Networks
NGN	Next Generation Network
PES	PSTN Emulation System
PoR	Point of Retention
RDHI	Retained Data Handover Interface
SGW	Signalling GateWay
SPDF	Service Policy Decision Function

iTeh STANDARD PREVIEW
(standards.iteh.ai)
Full standard:
https://standards.iteh.ai/catalog/standards/sist/126e3f66-7118-418c-b432-1c1c4027909b/etsi-tr-187-012-v2.1.1-2009-11

4 Introduction

The NGN is required to operate within a regulated environment. In Europe the privacy directive EC/2002/58 [i.4] applies and article 5 states:

1) Member States shall ensure the confidentiality of communications and the related traffic data by means of a public communications network and publicly available electronic communications services, through national legislation. In particular, they shall prohibit listening, tapping, storage or other kinds of interception or surveillance of communications and the related traffic data by persons other than users, without the consent of the users concerned, except when legally authorised to do so in accordance with Article 15(1). This paragraph shall not prevent technical storage which is necessary for the conveyance of a communication without prejudice to the principle of confidentiality.

2) Paragraph 1 shall not affect any legally authorised recording of communications and the related traffic data when carried out in the course of lawful business practice for the purpose of providing evidence of a commercial transaction or of any other business communication.

3) Member States shall ensure that the use of electronic communications networks to store information or to gain access to information stored in the terminal equipment of a subscriber or user is only allowed on condition that the subscriber or user concerned is provided with clear and comprehensive information in accordance with Directive 95/ 46/EC, inter alia about the purposes of the processing, and is offered the right to refuse such processing by the data controller. This shall not prevent any technical storage or access for the sole purpose of carrying out or facilitating the transmission of a communication over an electronic communications network, or as strictly necessary in order to provide an information society service explicitly requested by the subscriber or user.

SR 002 211 [i.8] identifies those aspects of standardisation that are required to ensure compliance with the European Framework Directive. In some instances the right to privacy can be withheld as suggested in paragraph 2 of article 5 of the privacy directive [i.4] (see clause 5.1). Provisions for the lawful interception of traffic, and for retention of signalling data are allowed exceptions as defined in Article 15(1) of the privacy directive:

1) Member States may adopt legislative measures to restrict the scope of the rights and obligations provided for in Article 5, Article 6, Article 8(1), (2), (3) and (4), and Article 9 of this Directive when such restriction constitutes a necessary, appropriate and proportionate measure within a democratic society to safeguard national security (i.e. State security), defence, public security, and the prevention, investigation, detection and prosecution of criminal offences or of unauthorised use of the electronic communication system, as referred to in Article 13(1) of Directive 95/46/EC. To this end, Member States may, inter alia, adopt legislative measures providing for the retention of data for a limited period justified on the grounds laid down in this paragraph. All the measures referred to in this paragraph shall be in accordance with the general principles of Community law, including those referred to in Article 6(1) and (2) of the Treaty on European Union.

The obligations from the directive are placed on member states but may be met by the provision of specific capabilities in the NGN and for DR these are as follows:

- An NGN operator should provide mechanisms to ensure the interception and handover of signalling of specific NGN users if required to by a lawful authority (defined in TS 187 005 [i.10]).
- An NGN operator should provide mechanisms to ensure the interception and handover of the content of communication of specific NGN users if required to by a lawful authority (defined in TS 187 005 [i.10]).
- An NGN operator should provide mechanisms to ensure the retention and handover of signalling of specific NGN users if required to by a lawful authority (the feasibility of achieving this is examined in the present document).

iTeh STANDARD PREVIEW
(standards.iteh.ai)

5 NGN overview with respect to data retention

5.1 Data categorisation

Retained Data has been broken down into the following categories in TS 102 657 [i.2] which has rationalised the categorisations given in the EU Retained Data Directive [i.1] to take into account the requirements of law enforcement specified in TS 102 656 [i.3]:

- Subscriber data: information relating to a subscription to a particular service (e.g. Name, Address).
- Usage data Information relating to usage of a particular service (e.g. Call Records).
- Equipment data: information relating to an end-user device or handset.
- Network element data: information relating to a component in the underlying network infrastructure.
- Additional service usage: information relating to additional services used (e.g. DNS).

Within the NGN the CSP is required to break down its information into the categories listed above and is not allowed or expected to provide information outside of the above categories within the context of using TS 102 657 [i.2] as the interface from the NGN to the LEA. For certain NGN services particular data categories may not apply.

5.2 Retention obligation

The obligation to retain data and the periods for which to retain data are outlined in the Directive [i.1] and by relevant national law. Data in the categories outlined in clause 5.1 have to be retained by the CSP if that data are generated or processed by providers of publicly available electronic communications services or of a public communications network within their jurisdiction in the process of supplying the communications services concerned. It is noted that within the context of the Framework directive and the ECN&S model it defines there may be many CSPs working in concert to offer NGN services to users. Each CSP is responsible for ensuring the retention of data in the context of their specific service provision and for ensuring that the retained data is an accurate record of the activity of the user as received in the CSP. The responsibility for assurance of correctness of data is further illustrated in the following:

a) Distinction is to be made between:

   a1) parameters required for the purpose of charging, which are available anyway;

   a2) additional parameters for the specific purpose of law enforcement, which require dedicated functions.

NOTE: Depending on the country's legal requirements difference functions have to be implemented in the systems for the fulfilment of law enforcement: a1) above requires some processing in order to deliver the information according to handover requirements; a2) above refers to functions to be implemented solely for law enforcement.

b) Parameters may be:

   b1) created in the domain of the CSP delivering the information;

   b2) created outside the domain.

The obliged CSP can take responsibility for the parameters b1), while for the parameters b2), the correctness is not guaranteed, unless c1) (below) applies.

c) Parameters may be:

   c1) mandatory for successful communication completion, i.e. self-verifying;

   c2) not relevant for successful communication completion and not verifiable, i.e. they may be wrong.

The obliged CSP can take responsibility for the parameters c1), while for the parameters c2), the correctness is not guaranteed, unless b1) applies.

iTeh STANDARD PREVIEW
(standards.iteh.ai)
https://standards.iteh.ai/catalog/standards/sist/126e3f6f-b118-d18c-b432-c1c0b7099e/etsi-tr-187-012-v2.1.1-2009-11