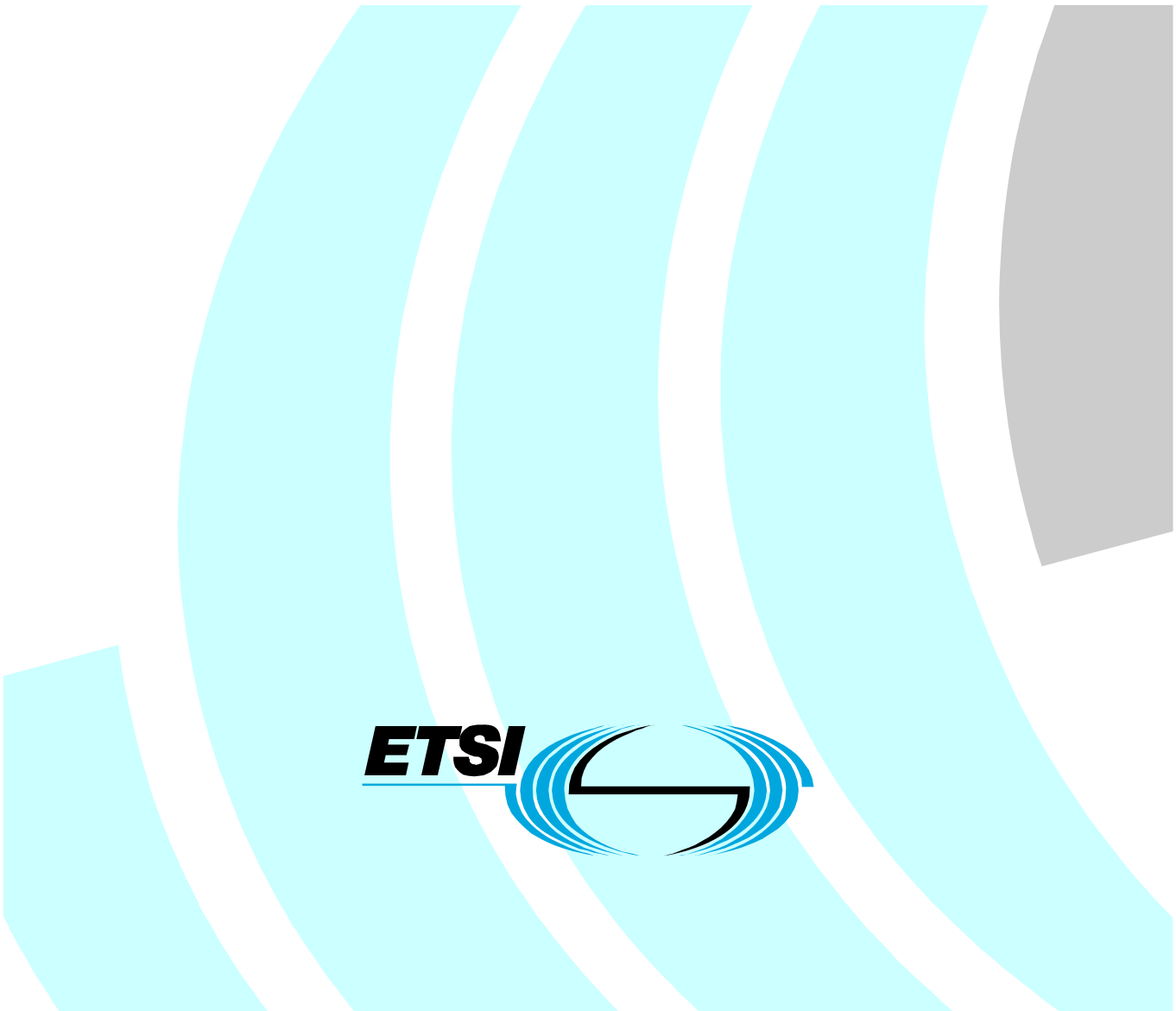
ETSI TR 187 012 V2.1.1 (2009-11)

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



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

Contents

Intellectual Property Rights 5
Foreword 5
1 Scope 6
2 References 6
2.1 Normative references 6
2.2 Informative references 7
3 Definitions and abbreviations 8
3.1 Definitions 8
3.2 Abbreviations 8
4 Introduction 9
5 NGN overview with respect to data retention 10
5.1 Data categorisation 10
5.2 Retention obligation 10
6 Abstract architecture for data retention in the NGN 11
6.1 Overview 11
6.2 Mapping of NGN architecture to DR abstract architecture 12
6.3 Security considerations for DR in generic CSP 14
6.3.1 Privacy considerations in the NGN with respect to DR 14
Annex A: Analysis of Directive with respect to the NGN 15
Annex B: Comparison of terms between Directive and NGN 18
Annex C: National declarations regarding application of the directive 19
C.1 Austria 19
C.2 Belgium 19
C.3 Republic of Cyprus 19
C.4 Czech Republic 19
C.5 Estonia 19
C.6 Finland 19
C.7 Germany 20
C.8 The Hellenic Republic 20
C.9 Republic of Latvia 20
C.10 Republic of Lithuania 20
C.11 The Grand Duchy of Luxembourg 20
C.12 The Netherlands 20
C.13 Republic of Poland 21
C.14 Slovenia 21
C.15 Sweden 21
C.16 United Kingdom 21
Annex D: Mapping to LEA requirements (TS 102 656) 22
D.1 User (LEA) requirements 22

D.1.1 Introduction 22
D.1.2 General requirements 22
D.1.3 Requests 22
D.1.4 Request for retained data 22
D.1.5 Delivery 22
D.1.6 Content of delivery 23
D.1.7 Location information 23
D.1.8 Availability constraints 23
D.1.9 Information transmission and information protection requirements 23
D.1.10 Internal security 23
D.1.11 Technical handover interfaces and format requirements 23
D.1.12 Temporary obstacles to transmission 24
D.1.13 Identification of the request criteria 24
D.1.14 Multiple requests 24

Annex E: Bibliography 25

History 26

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).

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).

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".

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

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).

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.

Some of the terms used in the Directive are not in common use in the NGN (see annexes A and B). Whilst the detail of the directive identifies the following classes of network either in isolation or in groups the NGN as specified in ETSI does not fall cleanly into any of the classes:

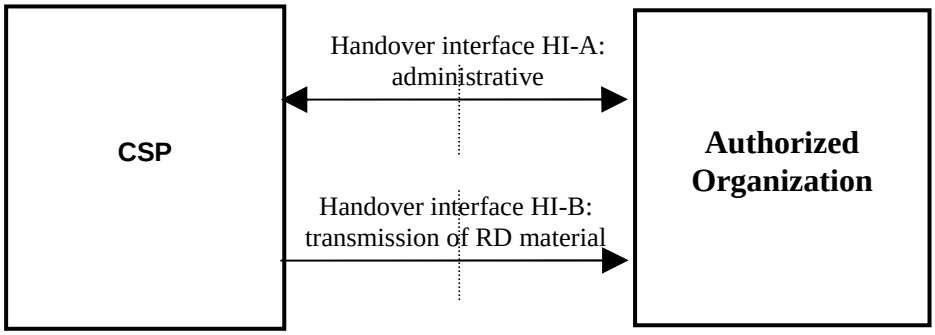
- Fixed network telephony.
- Fixed network telephony and mobile telephony.
- Internet access, Internet e-mail and Internet telephony.
- Internet e-mail and Internet telephony.
- Mobile telephony.

The obligation to ensure retention of data however is understood to apply irrespective of the network class but to CSPs in general.

6 Abstract architecture for data retention in the NGN

6.1 Overview

Figure 6.1 is the reference model for the request and transmission of retained telecommunications data taken from TS 102 657 [i.2].



NOTE 1: The term Authorized Organization covers any agency legally authorized to make Retained Data Handover Interface requests.
NOTE 2: Handover Interface-B delivers data from CSP to the Authorized Organization. There may be related supporting lower level messages from the Authorized Organization to CSP on HI-B.

Figure 6.1: Functional diagram showing handover interface HI

Within the CSP block three internal CSP functions have been identified in TS 102 657 [i.2] and are shown in figure 6.2:

- an *administrative function to* manage the Retained Data handover requests and responses;
- a *data collection function* to collect data from the various internal network elements and prepare the data for retention.

NOTE: The data collection function will gather data from Points of Retention (PoR) in the NGN.

- a *data store management function* to index and store the data, execute queries, and manage the maximum retention period for Retained Data.

The internal functions, and the interfaces between them, are examined with respect to the NGN in the present document.

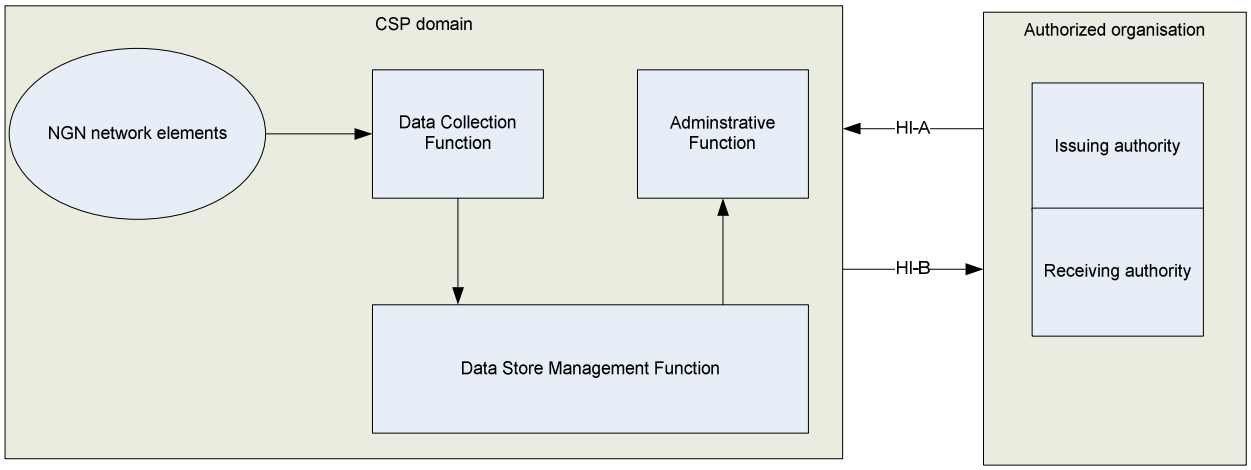


Figure 6.2: Functional model

For the NGN only those elements in the existing NGN definition that lie on the CSP side of the model are in the scope of the present document.

6.2 Mapping of NGN architecture to DR abstract architecture

The functional architecture of the NGN is defined in ES 282 001 [i.7] and shown for convenience in figures 6.3 (NGN overall architecture) and 6.4 (Distributed subsystems supporting the NGN).

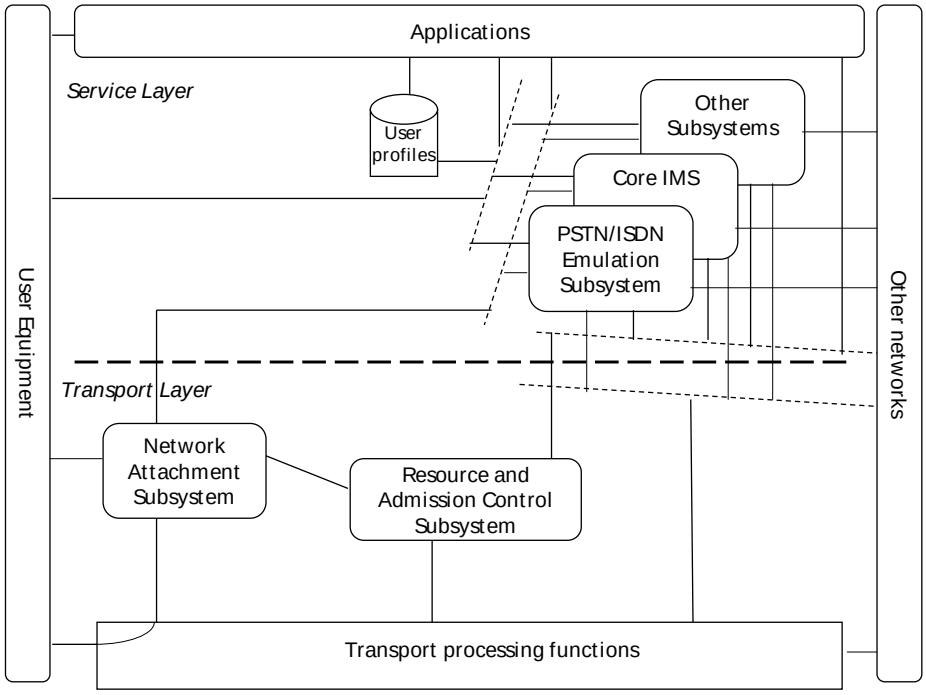


Figure 6.3: TISPAN NGN overall architecture

The NGN architecture and its decomposed subsystems may be distributed over multiple CSP domains and this is illustrated in figure 6.4 (from ES 282 001 [i.7]).

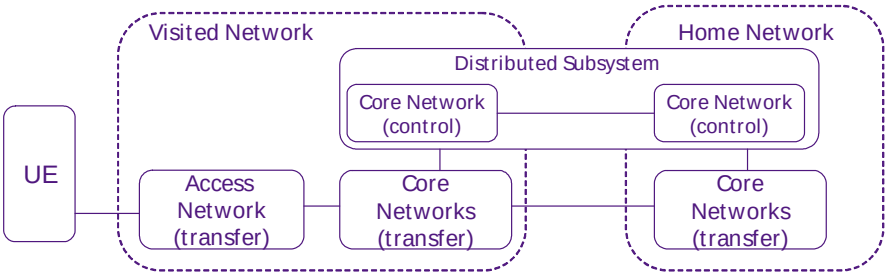


Figure 6.4: Distributed subsystems supporting the NGN

When the NGN is modelled as an instance of an ECN&S network as defined by the Framework Directive the structure shown in figure 6.5 applies.

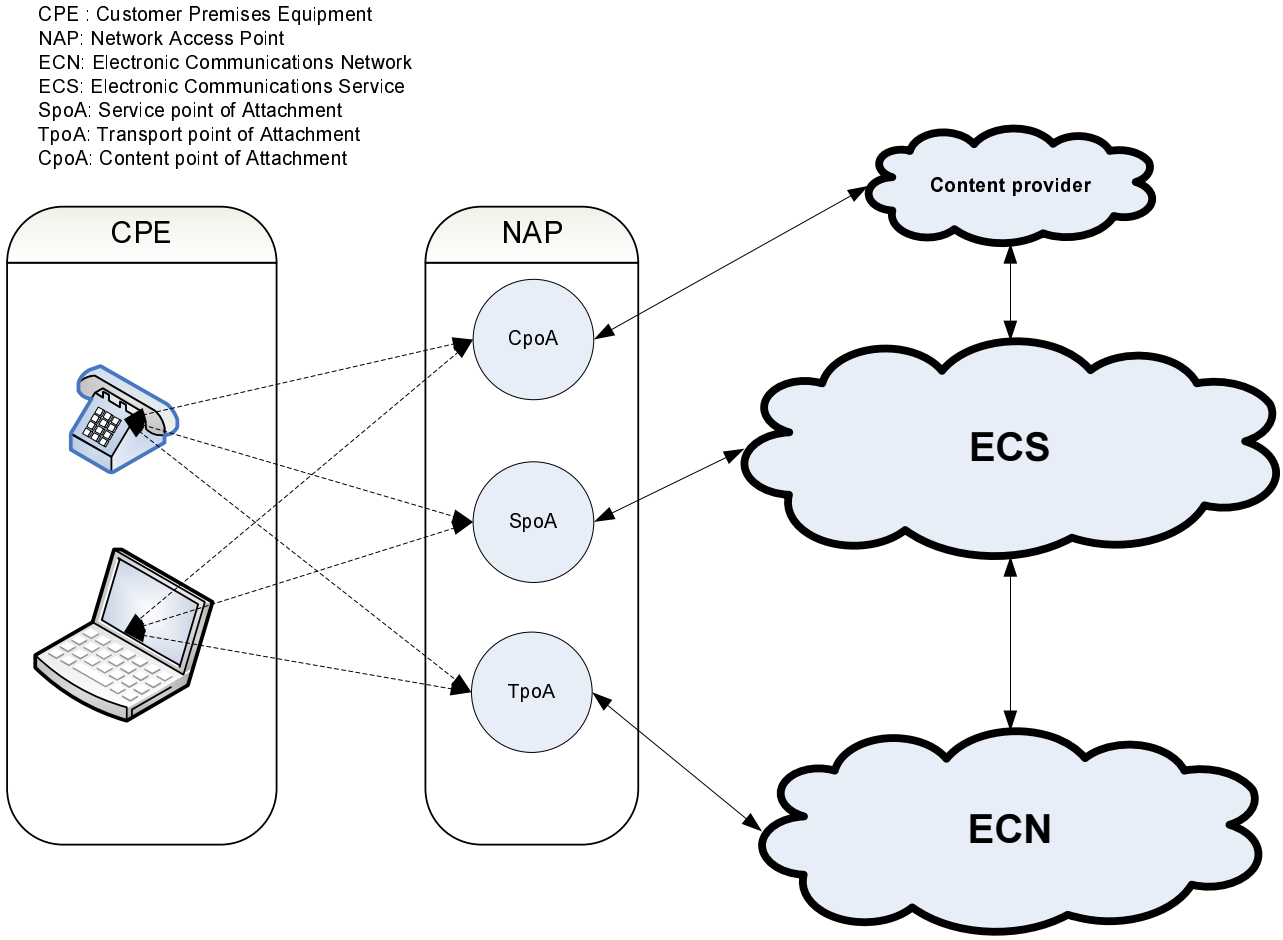


Figure 6.5: The ECN&S model

In the NGN the following subsystems may be seen to contain points of retention.

- ECS (Service Domain):
  - IMS.
    - This is the primary system of the NGN in the form of an ECS where user specific service signalling is terminated.
  - PES.

- NASS:
  - This is the primary system of the NGN in the form of an ECN where user specific transport domain signalling is terminated. Where the NASS manages signalling for the provision of service specific transport resources the relevant functional entities in the NASS may be required to act as a PoR.
- Transport domain general:
  - Where the transport domain manages signalling for the provision of IP addresses for example it is noted the relevant entity may be required to act as a PoR.

Annex A provides further mapping of the NGN FEs to the data retention requirements identified in the Directive [i.1]. In general there will be no provision of a point of retention in the Customer Premises Equipment but the PoR is only to be found within the NGN, and in most cases will be an extension of the core NGN Functional Entities.

Where a subscriber is accessing the NGN services through a roaming or migration agreement the Points of Retention in each of the home, visited, or transit networks are only required to be active for those elements of the service managed in each network and where there is a direct association between the activity and the target identity.

6.3 Security considerations for DR in generic CSP

Retained data needs to be of evidential quality (as it is used in enforcement) and an audit trail for all movements of retained data in the CSP environment should be recorded. In addition there is a need to ensure that data has not been manipulated during its storage and a further requirement to ensure that data when transferred is not at risk from exploit through eavesdropping.

The security guidelines for assurance of the CSP environment in gathering Retained Data and its handover given in TR 102 661 [i.9] should be followed.

6.3.1 Privacy considerations in the NGN with respect to DR

In addition to the strict security provisions and guidelines given in TR 102 661 [i.9], and the underlying security requirements for the NGN identified in TS 187 001 [i.15] the obligations for data protection given in the EU Data Protection Directive [i.4] and in the OECD guidelines for the collection of data [i.5] also apply. In the NGN these obligations are extended to cover protection of identity in TR 187 010 [i.14] and further provisions for protection of both identity and privacy of users of the NGN being addressed in the TISPAN NGN work programme need to consider the exemptions required by Data Retention and advertise these accordingly. The impact of this may affect the wording of contracts with subscribers in order to advise them that the CSP complies with the data retention directive and may hold records of activity for periods defined by law.

Annex A:
Analysis of Directive with respect to the NGN

The purpose of the Directive [i.1], as stated in article 1 of the directive, is to harmonise EU Member States' provisions concerning the obligations of the providers of publicly available electronic communications services (ECNs) or of public communications networks (ECNs) with respect to the retention of certain data which are generated or processed by them, in order to ensure that the data are available for the purpose of the investigation, detection and prosecution of serious crime, as defined by each Member State in its national law.

NOTE 1: Whilst there are common definitions of serious crime across the EU Member States not all member states agree on the explicit set of serious crimes that on investigation require access to retained data.

The Directive applies to traffic and location data on both legal entities and natural persons and to the related data necessary to identify the subscriber or registered user. It does not apply to the content of electronic communications, including information consulted using an electronic communications network.

EU member states have an obligation to retain data in the forms specified in Article 5 where those data are generated or processed, and stored or logged by providers of both ECNs and ECSs within the jurisdiction of the Member State concerned in the process of supplying the communication services concerned. The Directive does not require data relating to unconnected calls to be retained.

NOTE 2: This last requirement suggests a distinction between unconnected calls and unsuccessful calls that does not appear to exist in the NGN. If the perception of the user is taken into account there may be no difference between an unconnected call and an unsuccessful call attempt.

EU member States have to adopt measures to ensure that the retained data are provided only to the competent national authorities in specific cases and in accordance with national law. The procedures to be followed and the conditions to be fulfilled in order to gain access to retained data in accordance with necessity and proportionality requirements have to be defined by each Member State in its national law, subject to the relevant provisions of European Union law or public international law, and in particular with respect to any provisions on protection of citizens as interpreted by the European Court of Human Rights.

Table A.1: Retained data identified in Directive 2006/24/EC [i.1] and provision in NGN

Class of data	Class of network	Retained data	Provision in NGN (Candidate PoR)
Data necessary to trace and identify the source of a communication	Fixed network telephony and mobile telephony	the calling telephone number	CSCF
		the name and address of the subscriber or registered user	Subscriber management entity
	Internet access, Internet e-mail and Internet telephony	the user ID(s) allocated	CSCF
		the user ID and telephone number allocated to any communication entering the public telephone network	CSCF
		the name and address of the subscriber or registered user to whom an Internet Protocol (IP) address, user ID or telephone number was allocated at the time of the communication	Subscriber management entity
Data necessary to identify the destination of a communication	Fixed network telephony and mobile telephony	the number(s) dialled (the telephone number(s) called), and, in cases involving supplementary services such as call forwarding or call transfer, the number or numbers to which the call is routed	CSCF SGW
		the name(s) and address(es) of the subscriber(s) or registered user(s)	Subscriber management entity
	Internet e-mail and Internet telephony	the user ID or telephone number of the intended recipient(s) of an Internet telephony call	CSCF
		the name(s) and address(es) of the subscriber(s) or registered user(s) and user ID of the intended recipient of the communication	Subscriber management entity
Data necessary to identify the date, time and duration of a communication	Fixed network telephony and mobile telephony	the date and time of the start and end of the communication	CSCF
	Internet access, Internet e-mail and Internet telephony	the date and time of the log-in and log-off of the Internet access service, based on a certain time zone, together with the IP address, whether dynamic or static, allocated by the Internet access service provider to a communication, and the user ID of the subscriber or registered user	SPDF HSS NASS
		the date and time of the log-in and log-off of the Internet e-mail service or Internet telephony service, based on a certain time zone	SPDF HSS NASS
Data necessary to identify the type of communication	Fixed network telephony and mobile telephony	the telephone service used	CSCF
	Internet e-mail and Internet telephony	The Internet service used	CSCF

Class of data	Class of network	Retained data	Provision in NGN (Candidate PoR)
Data necessary to identify users' communication equipment or what purports to be their equipment	Fixed network telephony	the calling and called telephone numbers	CSCF
	Mobile telephony	the calling and called telephone numbers	CSCF
		the International Mobile Subscriber Identity (IMSI) of the calling party	3GPP AN, HLR
		the International Mobile Equipment Identity (IMEI) of the calling party	3GPP AN, HLR
		the IMSI of the called party	3GPP AN
		the IMEI of the called party	3GPP AN, VLR
		in the case of pre-paid anonymous services, the date and time of the initial activation of the service and the location label (Cell ID) from which the service was activated	Subscriber management entity. 3GPP HLR/HSS
	Internet access, Internet e-mail and Internet telephony	the calling telephone number for dial-up access	
		the digital subscriber line (DSL) or other end point of the originator of the communication	NASS admin
Data necessary to identify the location of mobile communication equipment		the location label (Cell ID) at the start of the communication	
		data identifying the geographic location of cells by reference to their location labels (Cell ID) during the period for which communications data are retained	

Annex B:
Comparison of terms between Directive and NGN

Table B.1: Comparison of terms used in Directive and equivalent term in NGN

	Term	Definition in Directive 2006/24/EC [i.1]	Definition in NGN
(a)	"data"	traffic data and location data and the related data necessary to identify the subscriber or user	No equivalent all encompassing definition
(b)	"user"	any legal entity or natural person using a publicly available electronic communications service, for private or business purposes, without necessarily having subscribed to that service	A user as defined by the possession of an NGN identity (as defined in TS 184 002 [i.11])
(c)	"telephone service"	calls (including voice, voicemail and conference and data calls), supplementary services (including call forwarding and call transfer) and messaging and multi-media services (including short message services, enhanced media services and multi-media services)	Any NGN (IMS/PES) service
(d)	"user ID"	a unique identifier allocated to persons when they subscribe to or register with an Internet access service or Internet communications service	an NGN identity as defined in TS 184 002 [i.11]
(e)	"cell ID"	the identity of the cell from which a mobile telephony call originated or in which it terminated	As per the directive
(f)	"unsuccessful call attempt"	a communication where a telephone call has been successfully connected but not answered or there has been a network management intervention	Any NGN (IMS/PES) service where the signalling is completed but the call does not transfer to a media active state

Annex C:
National declarations regarding application of the directive

NOTE: Not all EU Member States have recorded a declaration regarding the application of the directive.

C.1 Austria

Austria declares that it will be postponing application of this Directive to the retention of communications data relating to Internet access, Internet telephony and Internet e-mail, for a period of 18 months following the date specified in Article 15(1).

C.2 Belgium

Belgium declares that, taking up the option available under Article 15(3), it will postpone application of this Directive, for a period of 36 months after its adoption, to the retention of communications data relating to Internet access, Internet telephony and Internet e-mail.

C.3 Republic of Cyprus

The Republic of Cyprus declares that it is postponing application of the Directive in respect of the retention of communications data relating to Internet access, Internet telephony and Internet e-mail until the date fixed in Article 15(3).

C.4 Czech Republic

Pursuant to Article 15(3), the Czech Republic hereby declares that it is postponing application of this Directive to the retention of communications data relating to Internet access, Internet telephony and Internet e-mail until 36 months after the date of adoption thereof.

C.5 Estonia

In accordance with Article 15(3) of the Directive of the European Parliament and of the Council 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.4], Estonia hereby states its intention to make use of use that paragraph and to postpone application of the Directive to retention of communications data relating to Internet access, Internet telephony and Internet e-mail until 36 months after the date of adoption of the Directive.

C.6 Finland

Finland declares in accordance with Article 15(3) of the Directive 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.4] that it will postpone application of that Directive to the retention of communications data relating to Internet access, Internet telephony and Internet e-mail.

C.7 Germany

Germany reserves the right to postpone application of this Directive to the retention of communications data relating to Internet access, Internet telephony and Internet e-mail for a period of 18 months following the date specified in the first sentence of Article 15(1).

C.8 The Hellenic Republic

Greece declares that, pursuant to Article 15(3), it will postpone application of this Directive in respect of the retention of communications data relating to Internet access, Internet telephony and Internet e-mail until 18 months after expiry of the period provided for in Article 15(1).

C.9 Republic of Latvia

Latvia states in accordance with Article 15(3) of Directive 2006/24/EC [i.1] 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.4] that it is postponing application of the Directive to the retention of communications data relating to Internet access, Internet telephony and Internet e-mail until 15 March 2009.

C.10 Republic of Lithuania

Pursuant to Article 15(3) of the draft Directive of the European Parliament and of the Council on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or public communications networks and amending Directive 2002/58/EC [i.4] (hereafter the "Directive"), the Republic of Lithuania declares that once the Directive has been adopted it will postpone the application thereof to the retention of communications data relating to Internet access, Internet telephony and Internet e-mail for the period provided for in Article 15(3).

C.11 The Grand Duchy of Luxembourg

Pursuant to Article 15(3) of the Directive of the European Parliament and of the Council 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.4], the Government of the Grand Duchy of Luxembourg declares that it intends to make use of Article 15(3) of the Directive in order to have the option of postponing application of the Directive to the retention of communications data relating to Internet access, Internet telephony and Internet e-mail.

C.12 The Netherlands

Regarding the Directive of the European Parliament and of the Council on the retention of data processed in connection with the provision of publicly available electronic communications services and amending Directive 2002/58/EC [i.4], the Netherlands will be making use of the option of postponing application of the Directive to the retention of communications data relating to Internet access, Internet telephony and Internet e-mail, for a period not exceeding 18 months following the date of entry into force of the Directive.

C.13 Republic of Poland

Poland hereby declares that it intends to make use of the option provided for under Article 15(3) of the Directive of the European Parliament and of the Council on the retention of data processed in connection with the provision of publicly available electronic communications services and amending Directive 2002/58/EC [i.4] and postpone application of the Directive to the retention of communications data relating to Internet access, Internet telephony and Internet e-mail for a period of 18 months following the date specified in Article 15(1).

C.14 Slovenia

Slovenia is joining the group of Member States which have made a declaration under Article 15(3) of the Directive of the European Parliament and the Council on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks, for the 18 months postponement of the application of the Directive to the retention of communication data relating to Internet, Internet telephony and Internet e-mail.

C.15 Sweden

Pursuant to Article 15(3), Sweden wishes to have the option of postponing application of this Directive to the retention of communications data relating to Internet access, Internet telephony and Internet e-mail.

C.16 United Kingdom

The United Kingdom declares in accordance with Article 15(3) of the Directive 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.4] that it will postpone application of that Directive to the retention of communications data relating to Internet access, Internet telephony and Internet e-mail.

Annex D:
Mapping to LEA requirements (TS 102 656)

In like manner to the translation of the International User Requirement for Lawful interception to an ETSI deliverables there has been an extended translation of the base data retention directive requirements into an ETSI deliverable in the form of TS 102 656 [i.3]. The present annex identifies the implications on the NGN CSP of the requirements stated in the latter document. The annex is structured as an analysis of clause 4 of TS 102 656 [i.3].

D.1 User (LEA) requirements

D.1.1 Introduction

In TS 102 656 [i.3] this clause presents the user requirements related to the retained data of telecommunications with the LEA being the user with the note that these user requirements are subject to national law and international treaties and should be interpreted in accordance with applicable national policies. As such there is a good chance that some of the requirements might not correspond to national laws and regulations meaning that implementation takes place if required by national law.

D.1.2 General requirements

The general requirements presented reinforce those in the directive itself with 2 notes in particular being drawn out as important.

NOTE 1: The retention of data applies to the use of services. This applies to subscribers, visitors etc. of the service.

NOTE 2: The retention of data applies to all calls or services including those from roaming scenarios, e.g. mobile roaming records (ISO spec).

D.1.3 Requests

The clause covering requests again reinforces the directive but does clarify this as meaning both the data generated or processed in association with communication or communication attempts and subscriber data. It is also drawn out that any LEA request shall not (the mandate is made in the referred document) require the CSP to make any subjective decisions, to use any judgement or discretion. In other words, requests shall be such that it is immediately clear whether a particular record matches the request.

D.1.4 Request for retained data

The content of the "request for retained data" clause gives guidance on the identifying data for the retained data that is to be handed over to the LEA and reinforces and clarifies the content of the Directive itself. The clause itself splits along the lines of data required for retained subscriber data, and the data required to request retained communications data.

D.1.5 Delivery

The intent of the "delivery" clause is to give guidance to the CSP on fulfilling a retained data request. The main points introduced are:

- Correlation identifier:
  - Required to map the data to the lawful authorisation.
- Identification of known omissions and errors.

D.1.6 Content of delivery

The "content of delivery" clause provides clarification of article 5 of the Directive and which is examined in clause 6 of the present document.

NOTE: Multi-party and multi-way particularly applies to conference call and email exploder.

D.1.7 Location information

The clarification given on location information identifies a number of forms and sources of data where information is expected to be made available from normal network operation:

a) the geographic, physical or logical location of the target identity, when telecommunications activity (involving communication or a service) is taking place;

b) the geographic, physical or logical location of the target identity, irrespective of whether telecommunications activity (involving communication or a service) is taking place or not (in accordance with particular national requirements);

c) the geographic, physical or logical location of an identity temporarily associated with a target service because of successful telecommunication or an unsuccessful attempt to establish telecommunication (in accordance with particular national requirements);

d) the geographic, physical or logical location of an identity permanently associated with a target service (in accordance with particular national requirements).

D.1.8 Availability constraints

The text of this clause provide reinforcement that the intention of the regulation applies for all future services offered by CSPs. This is particularly noted in notes in the text where the DR requirement applies to the introduction of modifications to the telecommunication installation or to new operational features for existing telecommunications services to the extent of their impact on existing data retention and delivery capabilities.

There is some recognition that the amount of data which has to be handled and delivered may incur some time to gather and deliver but reasonableness is expected (i.e. it should not be seen to be several generations behind the extant state of the art).

D.1.9 Information transmission and information protection requirements

The obligations incumbent on service providers concerning measures to ensure data quality and their obligations concerning measures to ensure confidentiality and security of processing of data apply in full to data being retained and this acts as a direct reinforcement of the Directive.

D.1.10 Internal security

The requirements on CSPs to configure the technical arrangements in the data retention installation so as to enable the processing of requests for retained data in accordance with applicable national laws (including the selection of staff enabling the process) are noted as being subject to relevant national security regulations. In addition the guidance on security of the CSP installation given in TR 102 661 [i.9] should be taken into account.

D.1.11 Technical handover interfaces and format requirements

This clause in TS 102 656 [i.3] is a direct lead into the RDHI work and specifications from TC LI that are analysed in annex A.

D.1.12 Temporary obstacles to transmission

Simplified the two points raised can be copied for the NGN:

a) When transmission to law enforcement, in exceptional cases, is not possible the results shall be delivered as soon as the connection has been re-established.

b) Prevention of the delivery of requested data is not permitted.

D.1.13 Identification of the request criteria

a) Where the special properties of a given service, and the justified requirements of the LEAs, necessitate the use of various identifying characteristics for determination of the data set, CSP with the LEA shall ensure that the data set can be delivered on the basis of these characteristics.

b) In each case the characteristics shall be identifiable without unreasonable effort and shall be such that they allow clear determination of the data set to be delivered.

D.1.14 Multiple requests

The text of this clause in TS 102 656 [i.3] simply points out that a CSP has to be able to cope with multiple requests for retained data. As the data may be requested from multiple agencies there has to be clear separation of the data to ensure confidentiality of both the identities of the requesting agencies and the investigations they are undertaking.

Annex E: Bibliography

ETSI TS 188 002-2: "Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); Network and Service Management; Subscription Management; Part 2: Information Model".

History

Document history		
V2.1.1	November 2009	Publication