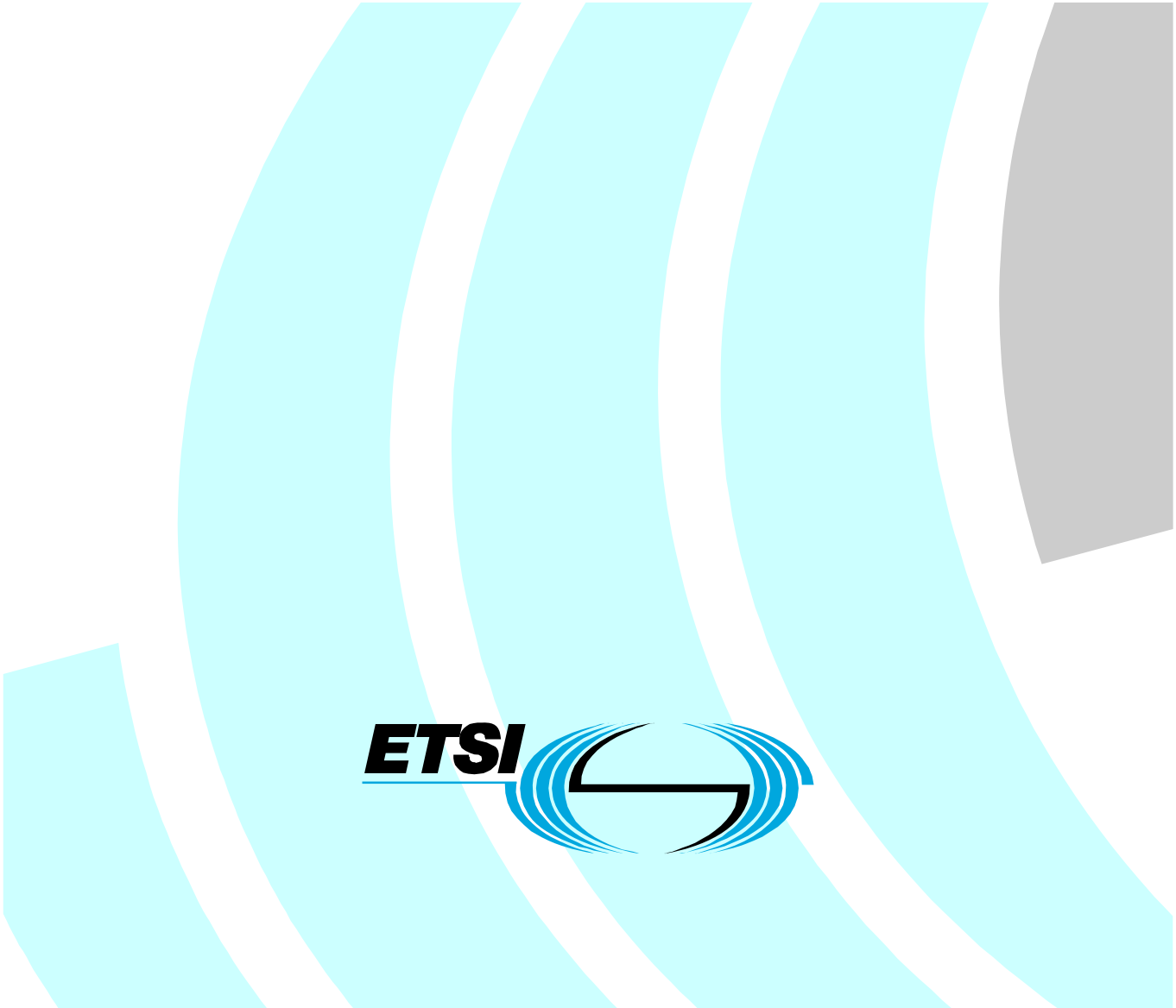
ETSI TR 102 661 V1.1.1 (2008-11)

Technical Report

Lawful Interception (LI); Security framework in Lawful Interception and Retained Data environment



Reference
DTR/LI-00044

Keywords
security, lawful interception

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

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 Lawful Interception (LI).

Introduction

Communication privacy is considered as a valuable asset by the Internet, fixed and mobile telephony providers of electronic communication networks. Indeed, incidents of privacy violations against their subscribers may cause severe impact with commercial and legal consequences. Above considerations are more important when these networks operate critical services in terms of communication privacy, such as, Lawful Interception (LI) and Data Retention (DR) services. Hence, special state-of-the art technologies and mechanisms together with a range of well-defined technical and procedural measures are recommended to be applied in order to verify and maintain an acceptable security level.

1 Scope

The scope of the present document is to recommend a framework for the secure provision of Lawful Interception (LI) and Data Retention (DR) services of a Communication Service Provider (CSP) towards the Law Enforcement Agencies. This framework aims to guarantee security in terms of confidentiality, integrity, forward secrecy, forward integrity and non-repudiation within CSP's LI and DR systems, operations and CSP internal and external interfaces for the delivery of IRI, CC and DR data towards any LEAs.

The present document initially describes the assets to be protected and then analyses the related security threats. Finally it recommends a range of security measures and controls necessary for achieving the desired level of security. The security measures content contains an unbreakable set of security categories where most of the measures, for each category, are indispensable controls while some others can be optionally chosen for creating a tighter security framework. Annexes are also defined. Annex A lists all recommended measures and controls, associates these measures with the respective systems, services and interfaces and also with the respective threats that aims to overcome. Annex B provides a secure logging infrastructure. Annex C provides a solution for protecting the retained data during the operation of the DR service while annex D provides a guide for cryptographic algorithms.

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.

For online referenced documents, information sufficient to identify and locate the source shall be provided. Preferably, the primary source of the referenced document should be cited, in order to ensure traceability. Furthermore, the reference should, as far as possible, remain valid for the expected life of the document. The reference shall include the method of access to the referenced document and the full network address, with the same punctuation and use of upper case and lower case letters.

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 indispensable for the application of the present document. For dated references, only the edition cited applies. For non-specific references, the latest edition 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 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.

[i.1] ETSI TS 101 671: "Lawful Interception (LI); Handover interface for the lawful interception of telecommunications traffic".

NOTE: Periodically TS 101 671 is published as ES 201 671. A reference to the latest version of the TS as above reflects the latest stable content from ETSI/TC LI.

[i.2] ETSI TS 102 232-1: "Lawful Interception (LI); Handover Interface and Service-Specific Details (SSD) for IP delivery; Part 1: Handover specification for IP delivery".

[i.3] IETF RFC 2246: "The TLS Protocol Version 1.0".

[i.4] ETSI TR 101 943: "Lawful Interception (LI); Concepts of Interception in a Generic Network Architecture".

[i.5] ETSI TR 102 528: "Lawful Interception (LI) Interception domain Architecture for IP networks".

[i.6] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995.

[i.7] ETSI TS 102 657: "Lawful Interception (LI); Retained Data".

[i.8] Council decision 2001/264/EC of 19 March 2001 adopting the Council's security regulations.

3 Definitions and abbreviations

3.1 Definitions

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

advanced electronic signature: electronic signature that is able to identify the signatory and able to detect any subsequent change in the data signed, that is related uniquely to the signatory and the data signed and that has been created by means that the signatory has under his sole control

authentication: verification of the claimed identity

authorization: action of granting access with a specific set of capabilities to certain resources based on the identity of the applicant

availability: property of being accessible and usable upon demand by an authorized entity and according to performance specifications

channel: means of communication used to carry information

NOTE: The channels corresponding to the interfaces HI1, HI2 and HI3 will be called channel HI1, channel HI2 and channel HI3 respectively.

confidentiality: property that information is not made available or disclosed to unauthorized individuals, entities or processes

electronic signature: set of data in electronic format, related to another set of data, that can be used as a mean to identify the signatory

forward integrity: property that past integrity protected data will not be affected, if all certificates, concerning a specific time period, are revealed to an atacker

forward secrecy: property that past confidentiality protected data will not be affected, if all certificates, concerning a specific time period, are revealed to an attacker

integrity: property that data has not been changed or destroyed without the requisite authorization

least privilege: security principle that demands that it should be granted the minimum set of capabilities to access and use information and resources that allows to carry out those duties to which someone is expressly authorized

LI/DR assets: involved hardware, software modules and services that produce and manage sensitive information

LI/DR infrastructure: comprises the LI/DR systems and the Network or IT systems that incorporate LI/DR functionality

LI/DR systems: CSP systems that are designed to explicitly operate LI/DR functionality such as Mediator, Administrator and Management functions

LI/DR session: LI or DR session describes the execution of an LI warrant or DR request, and contains all the activities, parameters and actions that are executed within LI/DR systems and services

log infrastructure: physical and functional architecture that will be used for implementation of the defined logging procedures

need to know: security principle that demands that anyone should just know, have access to or posses the information and resources strictly needed to carry out those duties to which she/he is expressly authorized

network or IT systems that incorporate LI/DR functionality: any network or IT CSP entity that is involved in the execution of an LI or DR procedure and incorporates either a software module or manage information assets, related to the LI and DR procedure (e.g. database servers, AAA servers, E-mail servers, Routers, Switches, etc.)

non-repudiation: property of being able to prove that an action or event took place, so that that action or event would not be denied later

qualified electronic signature: advanced electronic signature based on a recognized certificate and created by means of a secure signature creation device

NOTE 1: Even though they could use the same technology, the acts of signing and encrypting are different.

NOTE 2: The qualified electronic signature is also able to ensure the integrity of the signed data.

regulatory authority: represents a government agency responsible to regulate a specific area of interest

NOTE: In our case it regulates communication privacy matters.

secure authentication device: secure signature creation device that contains a recognized electronic certificate, plus an additional authentication mechanism (like a password or biometric authentication)

secure channel: channel that assures state-of-the-art confidentiality, integrity, availability and non-repudiation of the information carried by it, as well as the unequivocal authentication of the parties involved in the communication, providing the highest legal guaranty in accordance with national legislation currently in force

NOTE: A secure channel is not necessarily electronic.

segregation of duties: security principle that demands that processes should be divided in phases assigned to different persons so that it would be impossible that a single person could subvert a process

3.2 Abbreviations

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

AAA	Authentication, Authorization and Accounting
AES	Advanced Encryption Standard
CC	Call Content
CC-IIF	CC Internal Interception Function
CID	Communication IDentifier
CIN	Communication Identity Number
CLI	Command Line Interface
CSP	Communication Service Provider
DB	Data Base

D-H	Diffie-Hellman key exchange algorithm
DR	Data Retention
DSA	Digital Signature Algorithm
ECC	Elliptic Curve Cryptography
ECDSA	Elliptic Curve Digital Signature Algorithm
FFC	Finite Field Cryptography
HI	Handover Interface
HMAC	Hash Message Authentication Code
IFC	Integer Factorization Cryptography
IIF	Internal Interception Function
INI	Internal Network Interface
IRI	Intercept Related Information
IRI-IIF	IRI Internal Interception Function
IT	Information Technology
LEA	Law Enforcement Agency
LEMF	Law Enforcement Monitoring Facility
LI	Lawful Interception
LI/DR	Lawful Interception/Data Retention
LIID	Lawful Interception IDentifier
NID	Network IDentifier
OSI	Open System Interconnect
RA	Regulatory Authority
RSA	Rivest Shamir Adleman algorithm
SHA	Secure Hash Algorithm
SQL	Structured Query Language

4 The architecture

Based on architecture that is defined in TS 101 671 [i.1], figure 1 shows a CSP functional architecture for the secure LI operation. The main functional entities are the LI systems, the Log systems and Network and IT systems enhanced with LI functionality. "Log administration function" aims to have a central log management and mediation role among the LI/DR nodes, all log nodes and the possible CSP external authorities. From the operational point of view, it is identified with the "Mediation Log Device" (for these definitions see clause B.3). "Log event Collection function" aims to collect the log information from all involved nodes. From the operational point of view, it can be functioning either within the "Secure Log Server" or within the "Mediation Log Device" or within both parts (for these definitions see clause B.3). "Log store management function" aims to have a central storing management role. From the operational point of view, it is identified with the main storing part of the "Secure Log Server" (see clause B.3). The rest of the functional entities are later analysed within the present document while the entities within the "LI systems" functional block have already been analysed in TS 101 671 [i.1].

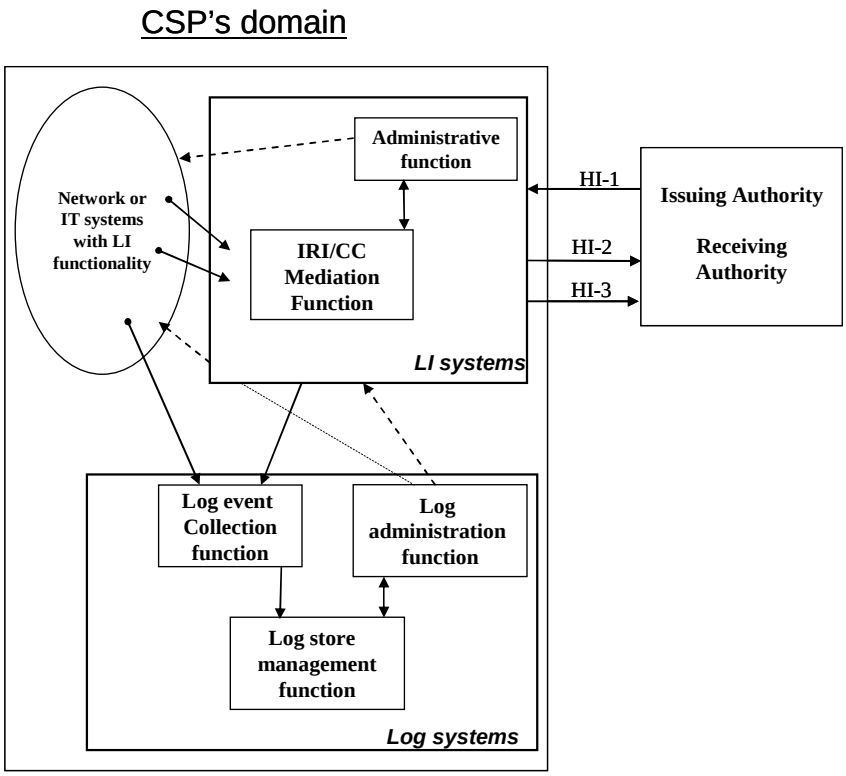


Figure 1: CSP functional architecture for the LI operation

Figure 2 shows a CSP functional architecture for the secure DR operation. Similarly, to the LI case, DR systems, Log systems and Network and IT systems enhanced with DR functionality are the main functional entities. The "Log system" functional block is the same with this of figure 1. The "DR system" functional block is analysed in TS 102 657 [i.7] whereas the rest of the functional entities are the same with these of figure 1.

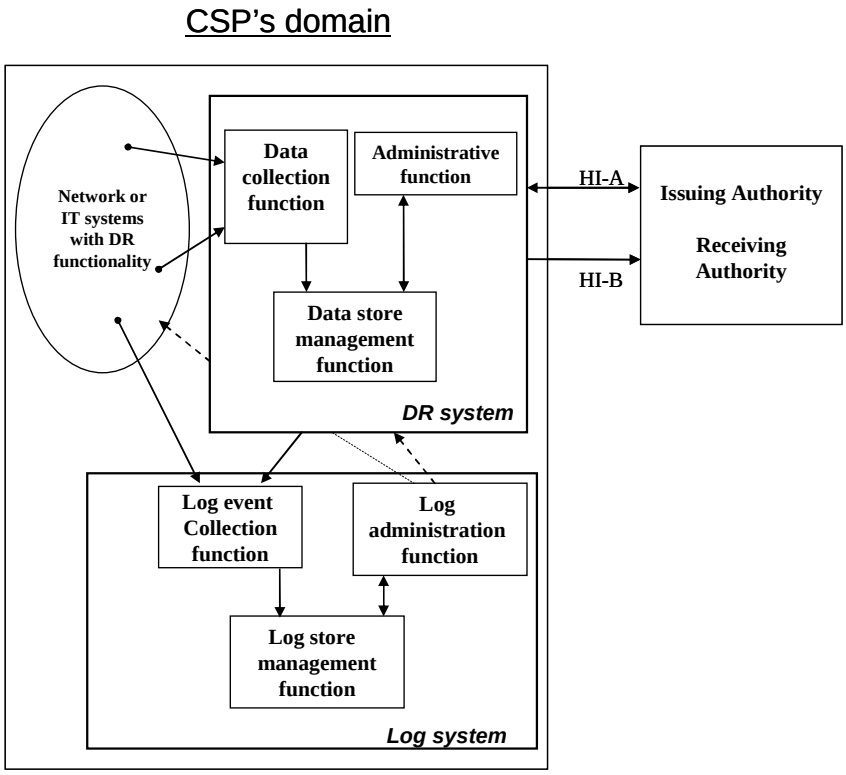


Figure 2: CSP functional architecture for the DR operation

5 Inventory of assets

The LI/DR assets that should be protected are described within the following categories:

1) Information assets.

   Information assets can be separated into the following categories:

   - The *DR retained telecommunication data* which is CSP customers' private communication information. This information is retrieved by the CSP systems and it is stored within the storage devices of DR systems for specific periods of time.

   - *The LI intercepted telecommunication data*, known as IRI and CC data which are retrieved at real time from the CSP systems, and are directly forwarded to the LEA side.

   - The *LI session execution data*. The execution of an LI warrant within the CSP network is reported by the LI session. During the LI session execution, further to the transmission of IRI and CC data, sensitive logged information is created, such as, the related warrant details, the duration and the number of the incidents that the intercepted target was involved. These session data are logged within special storing devices.

   - The *DR session execution data*. The execution of an DR request within the CSP network is reported by the DR session. During the DR session execution, sensitive information *is* generated that contains administrative data that concerns the request/response messages between the Requesting Authority and the CSP and the transmission of the retained telecommunication data and further useful system or session data. These session data are logged within special storing devices. General requirements for log information, log files and their encryption needs, is given in clause 7.10 while annex B proposes a solution for maintaining secure log files and events.

   - *The LI/DR-related log data*. This data is produced from logging mechanisms that are applied to any system and service of the LI/DR infrastructure.

   - *The* LI and DR unintentionally retained data. *This category is referred to unintentionally DR retained telecommunication data (described in the first bullet) or unintentionally retained LI/DR session execution data (described in the third and fourth bullet). These data can be previously deleted data but retained in the system (not destroyed) or historical information about operations performed on the system. In effect these data can be:*

     - *Record storage in databases contains data that has been logically deleted, but not destroyed.*

     - *Indexes also contain such delete values, and in addition may reveal, through their structure, clues about the history of operations that led to their current state.*

     - *The transaction logs that often includes useful information since it often includes before- and after-images of each database update.*

2) Software/Physical assets.

   - *LI/DR systems.*

   - *Network and IT systems that incorporate LI/DR functionalities.*

   - *LI/DR databases.*

3) Services.

   LI/DR services operating within both the LI/DR systems and the network or IT systems that incorporate LI/DR functionalities.

6 Security threats and vulnerabilities

6.1 Security threats

The purpose of this clause is to list possible security threats to the LI/DR environment, detailing what the threats achieve, how they are carried out and where in the system they could occur.

The security threats that should be considered, concerning the LI/DR environment, include the following:

1) (T1) Disclosure of information assets (sensitive data).

The disclosure of any information asset category may be realised against the network or IT systems that incorporate LI/DR functionality (such as AAA servers, routers, switches / DB servers) or directly against the LI/DR systems (e.g. mediation device) or against the Log infrastructure. The disclosure of the retained or intercepted data or any information asset category to unauthorized users, may lead to direct or indirect violation of privacy.

2) (T2) Modification of information assets.

An *accidental* modification may render the intercepted or the retained data useless, while a *deliberate* modification may lead to data misuse. The modification of data threat may affect all information asset categories that exist either in network or IT systems that incorporate LI/DR functionality or in LI/DR systems or in logging systems.

3) (T3) Unauthorized access to the LI/DR data.

Unauthorized access to the information assets that are related to LI may lead to disclosure or modification of data that belong to already intercepted CSP subscribers. This leads to violation of privacy of these intercepted subscribers.

Unauthorized access to the information assets that are related to DR may lead to disclosure or modification of retained data. These data may belong to any CSP subscriber and may lead to the violation of their privacy.

Moreover, modification or deletion of intercepted and DR proofs violates the non-repudiation and integrity policy of the provider too.

4) (T4) Unauthorized access to the LI/DR or Log infrastructure.

Unauthorized access to specific systems of the LI/DR infrastructure may lead to unauthorized use of the LI/DR service and by so being able to eavesdrop current or future LI traffic or DR data that belong to any CSP subscriber. This leads to violation of privacy of any CSP subscriber.

Unauthorized access to the Log infrastructure may lead to abuse of the Log service by so being able to abuse current or future logged LI/DR data.

5) (T5) LI/DR infrastructure (or service) abuse.

Under this threat, malicious code may be installed into the LI/DR infrastructure. Malicious code may lead to identity or password theft of other legitimate users, system abuse, illegal monitoring, disclose or modification of private data.

6) (T6) Illegal use of the retained data.

This involves processing the retained data for purposes other than the intended legal purposes. For example, accessing the communication data of Internet users in order to categorize users for commercial purposes or spy on a user's actions.

7) (T7) Repudiation.

Fake warrants, either deliberately or not, may be issued towards the CSP for their execution without being possible to confirm their existence. Similarly, fake LI or DR data may be sent towards the receiving authority without being possible to confirm their dispatch.

8) (T8) Prolonged interception or retention of data.

This involves the interception or the retention of the data for time periods longer than the lawful interception and retention periods respectively. Concerning the LI case this action composes a direct violation of user communication privacy. Although for the DR case is not a direct violation of privacy, it expands the exposure time of the data to possible attacks and vulnerabilities.

9) (T9) Recovery of unintended data.

When data is deleted, it is not destroyed and often persists on disk. Data owners currently have little control over these operations. They cannot say certainly where sensitive data may end up, whether it is destroyed after deletion or how long it will persist. This may lead to disclosure of LI/DR related data.

10) (T10) Denial of Service.

This involves any attempt that makes any resource (system, service, application, etc.) of the LI/DR infrastructure unavailable to its intended users.

Other sources of candidate threats can be found in TR 101 943 [i.4].

6.2 Security vulnerabilities

The LI/DR environment should also be assessed for common security vulnerabilities, which may include:

1) Lack of accountability.

If the users with legitimate access rights to the LI/DR infrastructure are not accountable for their actions, then malicious actions may be executed to these systems, resulting to disclosure, modification or illegal use of communication data of target users.

2) Lack of availability.

If any part of the LI or DR infrastructure is not available for a time period this may render the retained or logged data useless.

3) Vulnerabilities on the network and system design and implementation.

The design and implementation of the related networks and systems should be assessed for weak points including the transmission medium and equipment and network faults.

6.3 Attack scenarios

Based on the threats and vulnerabilities described in clauses 6.1 and 6.2, a number of possible attack scenarios are mentioned. This list is not exhaustive. The malicious user that executes the attack may be a local or a remote user.

1) A malicious user may eavesdrop customers' communication data or LI/DR session data by using the usual operations and commands offered by the LI/DR or Log services, respectively. He should have legitimate administrator rights or operator access rights for specific CSP services (e.g. LI, DR or Log services) and systems or he should be able to disclose the administrator's password. Additionally, in case of disclosing the log events the user should probably need to disclose some existing encryption keys. In order for the malicious user not to be detected by any audit procedures, he should be able to modify the content of some log files and cancel any related alerts that may be activated.

2) The malicious user may eavesdrop customers' communication data or LI/DR session data by not using the usual operations and commands offered by the LI/DR or Log services, respectively. This action presupposes the installation of a malicious software module within the LI/DR infrastructure either installed as autonomous module or incorporated within any appropriate legal software module. The malicious user should have legitimate administrator rights or he should be able to disclose the administrator's password. The malicious software should be intelligent to pass over any security policies (e.g. software key verification during installation) and avoid logging procedure during operation. In order for the malicious user not to be detected by any audit procedures, he should be able to modify the content of the log files during installation and cancel any related alerts that may be activated.

3) Hackers, privileged persons of the issuing authority or anyone malicious user who has gained access to the system of the issuing authority may issue fake DR requests towards the CSP. Moreover, privileged persons of the issuing authority may also issue legal DR requests that may later deny their existence. From the CSP side, malicious users may sent legal LI or DR answers towards the receiving authority that may later deny this dispatch.

4) Hackers, privileged insiders, or anyone who has gained physical access to hardware through theft or loss, may perform forensics analysis in a storing device (e.g. database system) and can reproduce partial histories from the unintended traces stored by the system. For example, a record deleted by a user and no longer accessible through the SQL interface can still be recovered from the file system. Anyone with access to these lower-layer interfaces can read data that was unintentionally retained.

7 Security measures

7.1 Personnel security

Personnel security policy is recommended to be applied to LI/DR systems, network or IT systems that incorporate LI/DR functionality and services.

1) People that are able to have access to CSP's LI/DR mechanisms and functions as well as to any information related to LI/DR, should be the minimum needed to assure the provision of LI/DR in the established conditions. Their access to information or any other resources related to LI/DR should be based on the following principles: *need to know*, *least privilege*, *segregation of duties and authorization*.

2) The CSP should appoint a team of people (*LI/DR team*) that will carry out any activity (technical, legal, procedural, or any other) related to LI/DR. These people can be partly occupied with LI/DR duties, but no other people can partly participate in LI/DR duties.

3) The LI/DR team consists of a number of different people, each one having an explicit, distinct and well defined role. Each role of the LI/DR team can be supported by more than one person, but one person can have only one role in the LI/DR team.

4) At least the following roles will be defined:

   a) *The LI/DR team leader*, who is responsible for the overall operation of the LI/DR system, as well as for guaranteeing that the system is appropriately operated and used.

   b) The LI/DR auditor: this person is responsible to assess the legitimate operation of LI/DR sessions as well as the proper and correct operation of LI/DR systems and all related services, such as LI/DR sessions that operate within the CSP-involved LI/DR infrastructure.

   c) *The LI/DR system user* (or *operator*): the person responsible for the operation of the basic functionality regarding the LI/DR services, like initiating, modifying or terminating an interception or a data retention retrieval.

   d) *The LI/DR system administrator*: the person responsible for the configuration, maintenance, and support of the CSP-involved LI/DR infrastructure, as well as the security of this infrastructure.

   e) The Log system administrator: the person responsible for the configuration, maintenance, and support of the Log infrastructure (see clause 7.10 and annex B).

5) Anybody who belongs to the LI/DR team should:

   a) Be expressly authorized to keep secret any information related to lawful interception.

   b) Have a clearly defined job-description and role. It is the responsibility of the CSP to define the role of the *personnel of the LI/DR team.*

   c) Be properly trained for her/his role, in both the operational and security-related issues. It is the responsibility of the CSP to properly train the personnel, according to the role.

d) Be well-informed about the liabilities and responsibilities entailed by her/his work. It is the responsibility of the CSP to define these issues.

6) All persons belonging to the LI/DR team are recommended to sign a specific Responsibility Statement and Confidential Agreement, before undertaking their duties. The minimum contents of the Responsibility Statement and Confidential Agreement are related to the aforementioned issues (clause 6).

7) The identities of the personnel consisting the LI/DR team should be classified and treated by the CSP as "highly confidential". To protect their anonymity, whenever there is a need to refer them pseudonyms would be used to avoid the disclosure of their personal identities.

7.2 Incident handling

1) The LI/DR team leader of the CSP should be in charge of drawing and keeping up to date an incident (contingency) plan that will ensure compliance with the security measures according to national regulation. The plan procedures should be well defined and concise. The team leader has to update them periodically and whenever the system is updated or changed.

2) Any member of the LI/DR team that suspects that there is any security breach or that any malicious activity is happening should inform the LI/DR team leader immediately.

3) The team leader should charge one person (i.e. the LI/DR system administrator) with the responsibility to detect any malicious action in the system.

4) As soon as a malicious action in the system is detected, the team leader should:

   a) Put the incident plan into action immediately.

   b) Inform the appropriate persons, as these are referred in the policy plan, immediately.

   c) Inform the LEAs immediately.

   d) Initiate an investigation immediately.

   e) Solve the problem as soon as possible, with the help of the LI/DR system administrator when necessary.

   f) As soon as the incident is solved, inform the LEA about the restoration of the security status and if possible report to investigation to a Regulatory Authority.

7.3 Physical and environmental security

Physical and environmental security policy is recommended to be applied to the LI/DR infrastructure. The main objective is recommended to be the prevention of unauthorized physical access to the LI and DR installation/room that contains the LI/DR system and the prevention of loss of critical information or equipment. The following measures is recommended to be implemented:

1) The LI/DR system, but the Internal Interception Functions (IIF), that are spread across the CSP telecommunications infrastructure, and the DR database servers, which would need special facilities, are recommended to be located inside rooms (the minimum number of them, preferably only one) that satisfies the following security requirements:

   a) Its location should be discreet and any information about it secret.

   b) The LI/DR installation/room should be protected by using all the necessary control mechanisms, such as barriers and locks, to all external doors and windows.

   c) Strong and up to date intrusion detection systems should be installed in order to cover all external doors and windows.

   d) Access to LI/DR installation/room should be restricted to authorized personnel. The access will only be possible after successful identification, authentication and authorization verification using strong and up to date controls.

e) An audit trail of all access should be securely maintained. The LI/DR team leader should be responsible for the integrity and safe storage of these data.

f) Access rights to LI/DR installation/room should be frequently reviewed by the LI/DR team leader. There should be a record with all the authorizations that have been given since the kick-off of the LI/DR system operation.

g) The presence of people that do not belong to the LI/DR team in this room should be limited to the minimum needed. Its presence should be authorized by the LI/DR team leader. In this authorization it should be stated the personal identity of every people, the period of presence authorized and the reason for her/his presence in the room. Her/his presence will be always accompanied by members of the LI/DR team. Any measure needed to assure that the presence of these people does not compromise the security will be adopted.

h) There should be an updated inventory of any equipment present inside the LI/DR installation/room.

i) Every removal or replacement of relevant equipment, either entrance or exit, should be recorded, accordingly.

j) It is strictly forbidden to bring into this room mobile phones or any other electronic devices, except with the express authorization of the security administrator.

k) Physical connections of the interception systems should be physically locked in a way that prevents placing malicious devices. Only the LI/DR team leader should be able to unlock these connections.

2) The Internal Interception Functions (IIF), the DR data base servers and more generally all network or IT systems and services that incorporate LI/DR functionalities are recommended to be protected at least by the following measures:

a) Physical access to the CSP internal systems that incorporate LI/DR functionalities should be protected by state-of-the-art telecommunication infrastructure security measures.

b) The location of the IIFs and DR DB servers should be discreet and any information about them should be secret.

c) Any action (installation, repair) on network or IT internal systems that incorporate LI/DR functionalities and services should be done discreetly by people expressly authorized by the LI/DR team leader, in her/his presence and under her/his responsibility and supervision.

7.4 Media handling

1) Clear criteria should be established to classify electronic as well as paper information according to the applicable security measures.

2) A secure storage necessary to keep documents (i.e. interception warrants, backup copies, interception system documentation,) either in hard copy or in electronic storage media which are critical for the security of the lawful interception and data retention is required. This secure storage will be opened only when it is strictly necessary and only the LI/DR team leader or the Log system administrator will be able to open it.

3) Documents defined in this clause should not leave the secure storage nor the LI/DR premises unless it is strictly needed. In this case, any measure needed to assure confidentiality, integrity and availability of these documents will be adopted and they will be transported by persons expressly authorize to it.

4) A log should exist to record the entrance and the leaving of any hard copy or electronic storage media from the LI/DR premises as well as a second log to record the entrance and the leaving of any hard copy or electronic storage media from the secure storage of these premises. Also, the person who brings the document should be recorded into these logs.

5) When the preservation period of these documents expires, the LI/DR auditor should destroy them in a secure manner. The destruction of each document should be also recorded.

7.5 Access control

Access control policy is recommended to be applied to the entire LI/DR infrastructure.

1) The LI/DR systems should have a well-known (logical) access point for every kind of operation (use, administration, security control, or other). The LI/DR team leader is recommended to define and write down all the aforementioned (logical) access points. It is the liability of the LI/DR team leader to ensure that there is no other (logical) access point to the LI/DR system, apart from the well known ones.

2) The LI/DR team personnel should be able to access the LI/DR infrastructure, according to stated (see note) authorization criteria, only by means of an *identity* defined in the system, after successful identification, authentication and authorization. It is strictly forbidden to access the system by using the identity of someone else. Therefore, the system should have state-of-the-art measures to prevent the use of the account of someone else (e.g. with secure authentication devices). People who are allowed to access the system should take all the necessary precautions to prevent someone else being able to use her/his identity.

NOTE: The activation (or execution) of every LI/DR command that is required to be executed can be done in conjunction to password verifications.

3) A strong cryptographic authentication mechanism is recommended to be supported by the LI/DR systems for either local or remote users (LEAs). It is recommended a combination of a password by cryptographic keys with secure devices or biometrics.

4) The information of the identities of the people authorized to access the system and their respective accounts is securely stored and classified. This information is recommended to be kept as stored for the entire life of the LI/DR infrastructure existence. The use of this information is restricted to the investigation of malicious actions in the LI/DR system by the appropriate authorities.

5) Authorization to access to information and other resources of the LI/DR system should be granted to people as well as to processes according to the LI/DR team's defined roles and it should be based on the principles of "need to know", and "least privilege". The system should assure that the privileges to access to information and other resources of the LI/DR system match strictly with the role of the person who owns the user. It is the responsibility of the LI/DR team leader and the LI/DR system administrator to define the authorization levels for each role.

6) The number of failed login attempts is recommended to be limited to a specified number (e.g. three attempts). Exceeding that number of failed login attempts will set out the pertinent procedure for handling security events (see clause 7.2).

7) Successful or unsuccessful access attempts to the LI/DR infrastructure should be securely logged (see clause 7.10).

8) Any user of the LI/DR system should exit or lock the LI/DR system before leaving his/her workplace.

9) Before accessing the LI/DR system, a warning message is recommended to appear on screen warning the user about the contents of the Responsibility Statement and Confidential Agreement he/she has signed, and that his/her activity should be recorded and supervised. This message will need to be accepted before actually accessing the system.

10) The LI/DR system should be locked whenever a user remains inactive for more than a defined period of time (suggestion: 5 minutes).

7.6 Confidentiality

The privacy of sensitive information for each different LI/DR session should be protected during the transmission or storage, by using appropriate cryptographic mechanisms.

Only standardized and well known encryption algorithms are recommended to be used, such as the Advanced Encryption Standard (AES). The key length of the related encryption keys should provide adequate protection from exhaustive attacks. The related cryptographic keys should be securely managed during their generation, use, storage and destruction.

7.6.1 Confidentiality of stored data

LI case:

The *LI session execution data* and the *LI-related log data* are recommended to be encrypted during their storage, either in isolated log servers or within other CSP devices (e.g. the mediation device, the AAA server, the network or data link layer elements, etc.). Secure logging clause (clause 7.10) analyses the measures for fulfilling this security requirement. In effect, only authorized users should be able to see this information decrypted. It is recommended to not be possible to get decrypted information through the ports of the system but by authorized users. Moreover, the system should assure that the deletion of information is done in a secure way, without prejudice to the auditing activity established in clause 7.10 and according to the deletion requirements that are set in clause 7.11.

DR case:

DR data that are stored within storing devices, require high protection in terms of confidentiality. Hence, the *DR retained telecommunication data*, the *DR session execution data* and the *DR-related log data* (for definition analysis see clause 5) that the CSP network produces and stores, is recommended to be kept encrypted during their entire retention period within storage devices. Key management procedures, necessary for succeeding any encryption procedures, is recommended to be also taken into consideration. Each encryption key should have retention period equal to the retention period of the stored data that encrypts and then it should be removed together with the data that normally encrypts. Secure removal and deletion of information should follow the requirements described in clause 7.11. General requirements for the *LI/DR-related log data*, log files and their encryption needs, are given in clause 7.10 while annex B proposes a solution for secure management of the log events.

7.6.2 Confidentiality of transmitted (INI and HI interfaces) data

For achieving confidentiality criteria for the LI intercepted telecommunication information the following requirements should be applied:

1) In the internal LI interfaces:

   a) Non disclosure of generated LI intercepted telecommunication information for each target user (target information): Target information, as this is transmitted by the internal CSP nodes (IRI-IIF and CC-IIF nodes), should not be accessible to unauthorized personnel from any operational management station, via management protocols, Command Line Interfaces (CLI) and traces and dumps, and should not be stored in Non Volatile Memory. If the IRI-IIF or CC-IIF device fails or re-boots, all intercepted related information and states should disappear and should not be accessible by any means (TR 102 528 [i.5]).

   b) Non disclosure of IRI and CC: Transmission of data and target information through INI2 and INI3 interfaces should be done in a secure manner. The option for the IRI and CC data to be routed through the network independently of other traffic should be available and should be preferred, so that it is possible to forward traffic over secured network links (TR 102 528 [i.5]).

Alternatively, the LI intercepted telecommunication information should be protected by encrypting the internal communication links.

2) In the handover LI interfaces:

   - The privacy of the transmitted data through the external communication interfaces (HI1, HI2 and HI3 for LI) shall be protected through strong encryption (at least 128 bits). The recommended technology is to use TLS (RFC 2246 [i.3]) for these interfaces. TS 102 232-1 [i.2].

For achieving confidentiality criteria for collecting the DR retained telecommunication data the following requirements should be applied:

1) In the internal DR interfaces:

   - DR user data are generated within network nodes and stored as DR retained telecommunication data, within internal CSP network elements. These data should be collected by the DR data collection function in a secure manner. Hence, all DR user data should be routed through the CSP internal network independently of other traffic so that it is possible to forward these data over secured network links.

Alternatively, the DR telecommunication data is recommended to be protected by encrypting data through their passing to the internal communication links.

2) In the handover DR interfaces:

   - The privacy of the transmitted data through the external communication interfaces (HIA and HIB for DR) is recommended to be protected through strong encryption (at least 128 bits). More specifically, for the DR interfaces, security methods such as IPSec or TLS are suggested. These security methods can be defined as connection level security methods.

7.7 Data and system integrity

7.7.1 Integrity of the LI/DR system software

The integrity of the LI, DR and Log system software, their updates and patches and any other piece of software installed in the LI or the DR system is recommended to be signed by means of a recognized electronic signature by its manufacturer. The LI/DR system administrator should previously successfully verify their integrity by means of the recognized electronic signature.

All recognized electronic signatures related to the integrity, after their verification, is recommended to be logged in an updated log file that will also identify the software installed date and time of installation and the identity of the installers. The produced log information should be securely kept according to the requirements mentioned in clause 7.10.

In case that any system action is executed within the LI or DR system without taking into consideration the aforementioned measures an alarm system should notify the LI/DR system administrator and the operation of the LI or the DR system (with all the planned and in progress LI or DR sessions) should be automatically stopped.

7.7.2 Integrity of stored data

LI/DR session execution data and LI/DR-related log data should be integrity protected by means described in clause 7.10).

Moreover, data retention involves the retained telecommunication data that should be integrity protected too. Any system that is used for the storage of the DR data should protect the integrity of the data, by using hashing algorithms (see annex D).

7.7.3 Integrity of transmitted data

Internal LI/DR interfaces:

INI1 interface that is used by the administration function to provision the IRI-IIF and indirectly the CC-IIF with intercept orders, should perform some short of cryptographic message integrity checking. INI2 and INI3 interfaces, should be also integrity protected. Hashing the transmitted packets and adding the hash checksums to the transmitted information wherever this is possible is a recommended method. This same method can be applied to the interfaces used for transmitting the collected DR telecommunication data from the point of their origin towards the storing machines.

External LI/DR interfaces:

The integrity of the transmitted LI data through the external communication interfaces (HI1, HI2 and HI3) should be protected through hashing or HMAC algorithms. Clause 7.2.3 of TS 102 232-1 [i.2] analytically describes a method that guaranties the integrity of these data sent by actually inserting hashes created over the data PDUs, into the data stream.

Regarding the request for DR data and the transmission of them through the external interfaces (HI-A, HI-B), their integrity can be guaranteed by applying security measures to application level. The process involves:

a) The LEA entity (an authorized person sending requests for requesting DR data) by computing a hash over the entire set of fields in the request (including the timestamp) applies data integrity protection. Then the hash is digitally signed with the entity's private key. The signed hash and the entity's certificate (validating its public key) are sent in the request to the CSP. The CSP may choose to validate the request by computing the request's hash and verifying that it matches the one signed by the LEA. The CSP may choose to validate the certificate as well.

b) The CSP entity where similarly computes a hash of each required response and following signs the hash value of the entire set of fields (including the timestamp) and sending towards LEA the signed hash and its certificate (validating this public key) with the set of fields.

7.8 Non-repudiation

In the LI case, in case that the warrant is submitted electronically, non-repudiation of origin, concerning the HI1 interface, is required, so that a fake warrant which was not issued by the appropriate authority not to be executed. This can be achieved by using digital signatures (RSA or DSA). Additionally, digital signatures are recommended to be used for non repudiation of the CSP that sends IRI and CC data towards the LEA. This requires that a digital signature to be inserted periodically into the data stream for HI2 and HI3. The detailed analysis is given in TS 102 232-1 [i.2] in the security requirements clause.

In the DR case, non-repudiation of origin (e.g. an authorized LEA officer) and of the respective CSP entity can be guaranteed by applying the application level security measure described in clause 7.7.3 where the origin makes the request and following the CSP entity response. In both parts the same methodology is used, that is, by using the private key digitally sign the hashed data of the entire request or response message. Following the entire block of information (the data of the request or response, the signed hash and the entity's certificate) is sent towards the correct destination.

7.9 Availability

The operating system should be up to date and there should be installed all the state-of-the-art applications needed to detect and protect the system against malicious programs, intrusions and any other threats. All users, services, applications, ports and addresses of the system not strictly needed for the lawful interception activity should be removed or locked in an irreversible way. Physical connections of the interception systems should be physically locked in a way that prevents placing malicious devices. Only the security administrator should be able to unlock these connections.

Security measures should be updated constantly to state-of-the-art level. The security administrator is in charge of this updating.

7.9.1 Protection against denial of service attacks

The security of Li systems will be partially embedded in general network security provisions. It is no less necessary to protect the critical parts of the telecommunications systems from intrusion than it is requires to do so for the LI systems. There are however some aspects of the LI systems that can make them special targets of criminal organizations, potentially interested in blocking the function of LI systems or even taking control of them to use for their own purposes. Criminals could be expected to approach cyber mafias to launch denials of service attacks in order to prevent successful lawful interception. A Lawful Interception solution should be deployed with a correspondent carrier-class security solution. Otherwise their ability to comply with the requirements of the warrant could be compromised and also the risk of attack on the core infrastructure could be increased.

LI solutions should be deployed with built-in security capabilities and be complemented with network security solutions in order to prevent, mitigate and investigate denial of service attacks Techniques such as access control list, black holing or null routing can be used to drop the attack traffic at the edge routers. Mitigation solutions such as sink holing can help to look for evidences than can implicate a target for interfering with the investigation.

7.9.2 Fault tolerance

Fault tolerance assures continuous interception operations regardless of equipment, network, or system fault. Equipment fault tolerance is assured through duplicated platform components. Network fault can be mitigated through buffering.

7.9.3 Disaster recovery

A comprehensive solution for disaster recovery should be deployed to ensure continuous interception operations in the event that a complete interception facility becomes incapacitated due to a catastrophic event (war, terrorism, natural disaster) or more mundane causes (electric and/or communications line breaks, local fire). The solution calls for a rapid transition to a fully functioning interception facility with replicated interception capabilities. In local disaster recovery, downed mediation systems can be restored or rebuilt through a step-by-step process that implements a recovery media.

7.10 Secure, verifiable and intelligible logging

Secure log files and their effective management are important requirements. Indeed, during security audits the examined log files should be correlated, in order to assure that the intended technical measures are in place and that the security policies and procedures are implemented. During non-scheduled security audits, e.g. as a response to a security incident, log files may also be analyzed in order to discover the cause of the incident, such as lack of security measures, non conformance with security procedures or system miss-configurations.

Hence a framework is recommended. This framework will describe logging procedures and will set the requirements for achieving secure log files, secure log management as well as pointing the corresponding log network infrastructure and its implementation design. All these details should be collected within a logging policy that the CSP should maintain.

7.10.1 Requirements

All systems in a LI/DR infrastructure are recommended to be supported by secure logging mechanisms. Secure logging mechanisms are responsible to collect, store, control, manage all adequate logged information and maintain it into highly secured log files, by assuring their authenticity, confidentiality, integrity, and availability during the life time of the system. This clause concentrates on security requirements regarding these functions:

a) Logging mechanisms should be able to collect logged information from critical LI/DR functions and procedures that apply to the entire LI/DR infrastructure (i.e. Mediator and Administrator device, Databases, AAA servers, Routers, Switches). The following bullet list aims to group these functions and provide some minimum requirements concerning the related log file structure.

- **LI/DR session functions:** This category may include all commands that are involved in initiating, monitoring, terminating and operating LI/DR sessions. The log files concerning this category may contain the following fields, TS 101 671 [i.1]:

    1) Lawful Interception Identifier (LIID).

    2) Communication Identifier (CID):

        - Network Identifier (NID).

        - Communication Identity Number (CIN).

    3) Warrant reference number.

    4) The date and time of the start of the session.

    5) The date and time of the end of the session.

    6) The address of the LEMF to which IRI/CC/DR information should be sent.

    7) Identification of the intercepted subject.

- **Security functions:** This category may include: user access control functions, user authentication and authorization functions, user account management functions, etc. The log files concerning this category may contain the following fields:

    1) User identifier.

    2) Date and time of user attempt.

    3) User attempt identifier.

    4) Status of attempt (successful/unsuccessful).

    5) Active users indication.

    6) User access rights.

    7) Result of the security verifications carried out by the LI team leader.

    8) Records of the document destruction.

9) User access attempts over log files.

- **System services and OS management functions:** This category may include:

  1) Configuration functions used regarding the system services and the OS.

  2) Troubleshooting management functions.

  3) Procedures for installing/uninstalling software modules.

  4) Patching/upgrading procedures.

  5) Authorization rights to install hardware and software elements to all entities of the CSP-involved LI/DR infrastructure.

  6) Installation and configuration incidents and changes related to LI/DR services that operate within all entities of the CSP-involved LI/DR infrastructure.

  7) Any other LI/DR system activity and related incidents.

  8) Commands of administrators and operators related to LI/DR sessions that regard all entities of the CSP-involved LI/DR infrastructure.

  9) LI/DR modules activation and deactivation events within all involved LI/DR systems.

  Data produced by above functions and procedures should be logged accordingly.

- **Network management functions:** This category may include:

  1) Network configuration/maintenance procedures.

  2) Network connectivity procedures.

  3) Commands of administrators and operators related to LI/DR sessions.

  4) Authorization rights to configure hardware/software elements to the network entities involved in LI/DR infrastructure.

b) Logging mechanisms should operate continuously without any interruptions. If logging mechanism fails for a period of time, LI/DR procedures should stop being executed for this specific period.

c) Logging, concerning the collection of log events, should be almost real time and guarantying there will be not any excessive delays.

d) Log files structure should be well defined following an agreed format. This structure may be standardized according to national requirements. In general, it should avoid any syntactical complexities, provide clear and generic log information categories and maintain a common formalization for all provider's networks. Log file fields and identifiers format should be chosen in a way as for achieving a useful audit analysis that may be used either by the Provider or a Regulatory Authority (RA).

e) The frequency of secure logging the generated log events should be decided beforehand and based upon national requirements.

f) The storage capabilities should be also decided (i.e. the form, duration and location of storage).

g) The log system administrator should be in charge of the design, operation, and maintenance of the entire Logging Infrastructure.

h) Produced log files should be almost at real time transferred and collected into a secure Log Server dedicated solely for this purpose. Each communication should be done by means of a secure channel.

i) The secure Log Server should be solely managed by the log system administrator.

j) Access to the log files should be controlled and only authorized entities should have access rights to particular entities.

k) Log entries of the log files should be encrypted in a way as for assuring their confidentiality and integrity.

l) Log events is recommended to be categorized according to their vulnerability level against the security threats and the importance of information that may offer if a security incident take place. The most important categories should be named as "critical log events". Examples of critical events may include: system restart, service mode modification (i.e. starting a service or halting a running service), modifications of users and user privileges, modifications of the log file and modification of the criticality level of a command.

m) Critical log events is recommended to be secured as close to their point of origin (e.g. routers) as possible and before they are stored into their log files. By these means the possibility of modification of these log events is reduced.

n) The LI/DR team leader is recommended to identify and define all required implementation scenarios for guarantying the maximum security level of all log events. For example identify the best implementation scenario for securing either critical or random log events or their combination.

o) To assure the authenticity and integrity of the logged information the encrypted log files should be signed by means of recognized electronic signature at least once a day and record the result of this verification into a WORM (Write Once Read Many) media. These media, once full, should be kept in a secure box in the LI/DR premises. Backup copy of them should be optionally kept in a different distant place that enjoys a similar level of security to assure its availability in case of destruction or loss.

p) Audit records and its verification results are at the inspectorate authority disposal.

q) In case of failure of the verification process, the LI/DR team leader should apply immediately the measures established in clause 7.2, paragraph "Incident Handling". Furthermore, she/he should warn the person in charge of the LI/DR team to order the immediate suspension of the activity of the interception system.

r) In case of failure in audit records generation, transmission or storage process, the LI/DR team leader should apply immediately the measures established in clause 7.2, paragraph "Incident Handling".

s) Encryption and signature keys is recommended to be protected in a secure and isolated signature device. These keys are recommended to be also created, managed and destroyed according to a well defined plan.

t) Log devices and signature devices is recommended to be managed by separate administrators.

7.11 Secure information destruction

LI or DR data that are scheduled to be deleted, after the deletion procedure may exist within their storage environments (database or file systems) as unintentionally retained data. Unintentionally retained data may be not resistant to unwanted forensic analysis and for this reason their privacy and confidentiality may be violated.

In order to avoid the unintended retention of data threat, specific techniques is recommended to be applied. A fundamental requirement that is recommended to be taken into consideration is "increasing forensics transparency". Forensic transparency is achieved by applying the following generic measures:

a) Retain only records and files that can be retrieved by the database services or the file systems respectively.

*b) Records and files that **cannot** be retrieved by database services (deleted records) or file systems respectively should be also removed by the system within a short, fixed time from when they become as unable to be retrieved. Hence, a small upper bound on the time that the non-retrieved records or files will be able to remain in the database or in the file systems, should be determined.*

Indeed, deletion of records is accomplished by setting a deletion bit. By this way data are not removed and is fully recoverable. The result is the inadvertent disclosure of sensitive information. A range of technical measures for counter above threats is recommended, such as:

1) Overwriting the logically deleted (but not destroyed) records that remain within the database (DB) page is recommended. This measure may require to change the code of the DB engine in order to overwrite tuples when these are put on the free list. This method, with attentive design, does not cause any performance degradation.

2) Most DB systems store their tables in a B+Tree data structure. Operations (i.e. insert, delete, update) that cause B+Tree modifications usually result in leaving copies of DB records in unused parts of the B+Tree. For achieving a security goal, code parts that cause B+Tree modifications is recommended to be additionally function as to overwrite obsolete data. Again this code modification, with attentive design, does not cause any performance degradation. By this means no data records are left destroyed and also the possibility that left data will be released to the file system through a vacuum function is also minimized.

3) Transaction log data is recommended to be efficiently expected too. Transaction logs contain logs that are used to provide recovery from transaction and system failure. They include before- and after- images of modified data pages. Usually, transaction logs contain quite old records that will never need to be used for recovery. A strategy for expunction of these old log records is to encrypt the log data and following removing the encryption keys.

4) Overwriting the storage medium with new data is also recommended. Overwriting is generally an acceptable method of clearing, as long as the media is writable and not damaged. To counter more advanced data recovery techniques, specific overwrite patterns are often prescribed. These may be generic patterns intended to eradicate any trace signatures. For example, writing repeated, alternating patterns of ones and zeros may be more effective than zeros alone. Combinations of patterns are frequently specified.

7.12 Development, maintenance and repair

1) Development, maintenance and repair of the LI/DR systems should be carried out on-site by the LI/DR system administrator(s) or persons of the manufacturer authorized by the LI/DR team Leader under the supervision of the LI/DR team Leader.

2) Any action (development, maintenance and repair) of the CSP network or IT systems that incorporate LI/DR functionalities and services should be done discreetly by people expressly authorized by the LI/DR team Leader, under his supervision.

3) In cases the provisions in paragraph 1 and 2 above cannot be applied, remote maintenance of the systems is permitted provided that is carried out by personnel authorized by the LI/DR team Leader, at times permitted by the provider and under demonstrate adequate security measures for maintaining the security level of the data.

4) All hardware, software or procedural changes should be properly logged (see clause 7.10) to enable the LI/DR auditor to assess the legitimate operation of LI/DR systems.

5) All hardware, software (e.g. updates, patches) changes to the LI/DR systems should take place only after the authorization of the LI/DR team Leader. The LI/DR system administrator(s) is responsible to verify the software authenticity and integrity by means of the recognized electronic signature.

6) To assure the authenticity and the integrity of the system software, this software, as well as its updates and patches and any other piece of software installed in the system should be signed by means of a recognized electronic signature by its manufacturer.

7) Key splitting may also be used for software changes together with electronic signatures. More than one authorized persons (e.g. LI/DR team Leader and LI/DR system administrator) may cooperate in order to activate the operation of new installed module.

8) The operating system of the LI/DR systems and the network or IT systems that incorporate LI/DR functionalities should be up to date with all the required state-of-the-art applications needed to detect and protect the system against malicious programs, intrusions and any other threats.

9) The LI/DR systems should be appropriately hardened so as to permit only services strictly required for executing interception/retaining data activities.

Annex A:
List of security measures

A.1 Introduction

Annex A lists all recommended measures and controls. It associates these measures with the respective functional blocks and interfaces and also with the respective threats that aims to overcome. Threats are mentioned with the letter "T" in a parenthesis after the measure description.

Table A.1: Recommended security measures and controls

Security Measures	Functional Blocks [n/a: not applicable] [√: the measure applies to the specific functional block]							Clause
	(DR / LI) Admin. Function	*(DR)* Data Collection / *(LI)* Mediation function	*(DR / LI)* Data store	*(DR / LI)* Network elements	*(DR / LI)* Log elements	*(DR / LI)* Internal Inter-faces	*(DR)* HI-A HI-B / *(LI)* HI-1; HI-2 HI-3	
Personnel Security (related to all threats: T1 - T10)								**7.1**
Minimum number of people that have access	√	√	√		√			
need to know, least privilege, segregation of duties and authorization principles	n/a	n/a	n/a	n/a	n/a	n/a	n/a	
LI/DR team	n/a	n/a	n/a	n/a	n/a	n/a	n/a	
explicit, distinct and well defined roles	n/a	n/a	n/a	n/a	n/a	n/a	n/a	
LI/DR team Leader	√	√	√		√			
LI/DR auditor	√	√	√					
LI/DR system user	√							
LI/DR System administrator	√	√	√					
Log System administrator					√			
Responsibility Statement & Confidential Agreement	n/a	n/a	n/a	n/a	n/a	n/a	n/a	
Anonymity of LI/DR team	n/a	n/a	n/a	n/a	n/a	n/a	n/a	
Incident Handling								7.2
Physical and Environmental Security (T4, T5)								7.3
Physical Security	√	√	√		√	√		
Discreet location	√	√	√		√			
protection control mechanisms	√	√	√		√			
intrusion detection systems	√	√	√		√			
access restricted to authorized personnel	√	√	√		√			
audit trail of access	√	√	√		√			
frequent review of access rights	√	√	√		√			
minimum people presence	√	√	√		√			
updated inventory	√	√	√		√			
recording of removal or replacement of equipment	√	√	√		√			
strictly forbidden mobile phones or other electronic devices	√	√	√		√			

Security Measures	Functional Blocks [n/a: not applicable] [√: the measure applies to the specific functional block]							Clause
	(DR / LI) Admin. Function	*(DR)* Data Collection / *(LI)* Mediation function	*(DR / LI)* Data store	*(DR / LI)* Network elements	*(DR / LI)* Log elements	*(DR / LI)* Internal Inter-faces	*(DR)* HI-A HI-B / *(LI)* HI-1; HI-2 HI-3	
physical connections locked	√	√	√		√			
physical access based on SoA security measures						√		
discreet location						√		
any action done only by authorized people						√		
Media Handling*								
Access Control (T1, T2, T3, T4, T5, T10)								7.5
Well-defined (logical) access points	√	√	√		√			
Identity-based Access	√	√	√		√			
Securely stored and classified people identities	√	√	√		√			
Authorization levels	√	√	√		√			
Restricted number of login attempts	√	√	√		√			
Successful or unsuccessful access attempts securely logged	√	√	√		√			
Exit or lock the LI/DR system before leaving his/her workplace	√	√	√		√			
Warning message about the Responsibility Statement and Confidential Agreement	√	√	√		√			
Automatic system lock after an inactivation time	√	√	√		√			
Confidentiality of stored data (T1, T3)								7.6.1
AES encryption is recommended to be applied for DR retained telecommunication data			√					7.6.1
Encryption of DR session execution data and DR-related log data	√				√ (see 7.10)			7.6.1

Security Measures	Functional Blocks [n/a: not applicable] [√: the measure applies to the specific functional block]							Clause
	(DR / LI) Admin. Function	*(DR)* Data Collection / *(LI)* Mediation function	*(DR / LI)* Data store	*(DR / LI)* Network elements	*(DR / LI)* Log elements	*(DR / LI)* Internal Inter-faces	*(DR)* HI-A HI-B / *(LI)* HI-1; HI-2 HI-3	
Confidentiality of transmitted DR data (T1, T3)								
Routing DR data through internal interfaces independently of other traffic (T1)						√		7.6.2
Strong encryption should be used for passing data through HI-A and HI-B interfaces (TLS is recommended) (T1)							√	7.6.2
Data/System Integrity (next three measures should be implemented together)								
All DR and Log software modules (for integrity protection) should be accompanied with electronic signatures **(T4, T5)**	√	√	√	√ (DR part)	√			7.7.1
Operate log procedures by logging at least the following content: signatures of the installed software, the date/time of installation and the person's id that executes software changes **(T4, T5)**	√	√	√	√	√			7.7.1
Operate an alarm system for above logging procedures **(T4, T5)**					√			7.7.1
Integrity protection for DR session execution data and DR-related log data is recommended (see Logging clause 7.13) **(T2, T3, T4)**				√	√			7.7.2
Integrity protection of retained telecommunication data is recommended (hashing as SHA-1 or HMAC) **(T2, T3, T4)**			√					7.7.2

Security Measures	Functional Blocks [n/a: not applicable] [√: the measure applies to the specific functional block]							Clause
	(DR / LI) Admin. Function	*(DR)* Data Collection / *(LI)* Mediation function	*(DR / LI)* Data store	*(DR / LI)* Network elements	*(DR / LI)* Log elements	*(DR / LI)* Internal Inter-faces	*(DR)* HI-A HI-B / *(LI)* HI-1; HI-2 HI-3	
Integrity protection of transmitted DR data within internal interfaces **(T2, T3)**						√		7.7.3
Application level integrity protection of transmitted DR data within external interfaces (HI-A, HI-B) by using hashes and digital signatures **(T2, T3)**							√	7.7.3
Non-repudiation of origin								
Digital signatures are recommended for non-repudiation of both sides (LEA, CSP side) **(T7)**	√						√	7.8
Availability								7.9
Up-to-date operating system	√	√	√	√	√			
Removed or locked services/ applications/ports/ addresses	√	√	√	√	√			
Physically locked connections	√	√	√	√	√			
Up-to-date security measures	√	√	√	√	√			
Protection against Denial of Service attacks*	√	√	√	√	√			
Fault Tolerance*	√	√	√	√	√			
Disaster Recovery*	√	√	√	√	√			
Secure, Verifiable and Intelligible Logging (T1 - T5)								7.10
Maintain a Log policy	√	√	√	√	√			7.10
Filter the appropriate information for successful logging	√	√	√	√	√			
Continuous operation	√	√	√	√				
real time log events collection	√	√	√	√				
well-defined log file structure	√	√	√	√				
log event generation frequency*	√	√	√	√				
Create a log infrastructure					√			
real-time transfer of log files to Log Server	√	√	√	√				

Security Measures	Functional Blocks [n/a: not applicable] [√: the measure applies to the specific functional block]							Clause
	(DR / LI) Admin. Function	*(DR)* Data Collection / *(LI)* Mediation function	*(DR / LI)* Data store	*(DR / LI)* Network elements	*(DR / LI)* Log elements	*(DR / LI)* Internal Inter-faces	*(DR)* HI-A HI-B / *(LI)* HI-1; HI-2 HI-3	
log entries of log files are recommended to be encrypted for assuring confidentiality and integrity	√	√	√	√				
Only the log system administrator has access privileges for the log server						√		
A list of critical log events should be defined and secured before they are packaged into log files	√	√		√	√			
In case of failure of the verification process "Incident Handling" should be activated	√	√	√	√	√			
Secure information destruction								7.11
Overwrite the logically deleted records that remain within a DB page			√		√			
Data structure (e.g. B+ tree) modification procedures recommended to overwrite obsolete data			√		√			
Encrypt the log data of transaction logs and following removing the encryption keys			√		√			
Overwrite with new data the storage medium (file systems) by using specific overwrite patterns	√	√	√	√	√	√		
Development, Maintenance and repair rules								7.12
On-site Development, maintenance and repair by authorized people (T1, T2, T3, T4, T5)	√	√	√	√	√	√	√	
Remote maintenance by authorized people (T1, T2, T3, T4)	√	√	√	√	√	√	√	

Security Measures	Functional Blocks [n/a: not applicable] [√: the measure applies to the specific functional block]							Clause
	(DR / LI) Admin. Function	*(DR)* Data Collection / *(LI)* Mediation function	*(DR / LI)* Data store	*(DR / LI)* Network elements	*(DR / LI)* Log elements	*(DR / LI)* Internal Inter-faces	*(DR)* HI-A HI-B / *(LI)* HI-1; HI-2 HI-3	
Logging of hardware/software/ procedural changes (T2, T5)	√	√	√		√	√	√	
Hardware/software changes after authorization of DR team leader (T1, T2, T3, T4)	√	√	√		√	√	√	
Recognized electronic signature by manufacturer (T1, T2, T3, T5)	√	√	√		√	√	√	
Key splitting for software changes (T1, T2, T3, T5)	√	√	√		√	√	√	
Up-to-date operating system (T5, T10)	√	√	√	√	√	√	√	
Hardening (T10)	√	√	√					

Annex B:
Building secure logging

B.1 A generic methodology for defining and organizing log information in an LI/DR environment

Before any security measures are taken for the LI/DR infrastructure, it is required to explicitly define what is important to be logged. This decision involves both the Provider and the Regulatory Authority (if the authority is prescribed by national law).

A ***Log Reference Model [B2]*** *is proposed*, as shown in figure B1 that can be used as a guide for each Provider to identify and organize the events that could be logged. This model is an abstract representation linking *Functions i.e.* general categories related to LI/DR network and operational events or jobs, to the corresponding *Log Files* that monitor these Functions, through the *Services* which implement the Functions (i.e. Log files are created by monitoring the Service commands). This model analyzes the logging needs from three different views, called *Planes*. These planes are:

(1) **Functional Plane:** It models the network and operational events or jobs within a provider's network that belong to the LI/DR infrastructure, without taking into consideration implementation details, architectural or topology constraints and design requirements. Suggestively and not limitedly in a provider's environment the following categories of Functions should be defined and logged:

   (a) LI/DR session functions.

   (b) Security Functions.

   (c) System services and OS management functions.

   (d) Network Management Functions.

(2) **Service Plane:** It describes all specific services i.e. password management service or AAA service, etc. which are executed within the network or IT nodes that belong to the LI/DR infrastructure. It aims to discriminate system from application services to identify the OS platform, communication protocols, interconnections, interfaces and hardware used.

(3) **Logging Plane:** It describes specific commands and events of each used service, which can be grouped into separated log files. For example, the command "show user" (captured for displaying user names) will be logged in a log file named "password management". This log file will correspond to the password management service, which implements part of the "Security functions" category.

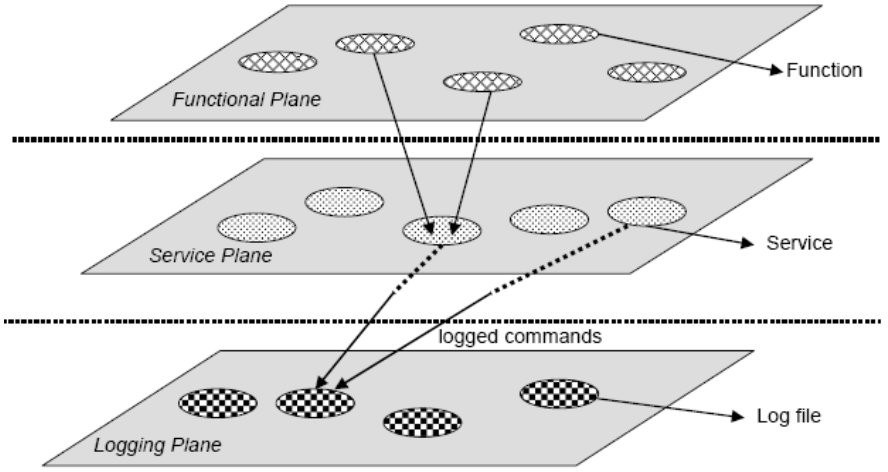


Figure B.1: An abstract representation of a Log Reference Model

B.2 Providing secure log files

In order to secure the log files from external and common internal attacks all the functions which have been identified in the previous phases should be securely logged. Secure logging can be based on standardized secure log systems such as the LogCrypt or the Schneier-Kesley system. Attack scenarios 1 and 2 of clause 6.3 proves that further care should be considered for achieving a secure logging procedure. In order to enable traceability of such an attack, a simple solution is the Provider to make use of digital signatures under the supervision of a trusted Regulatory Authority *RA* (this can be optional too) and to implement various scenarios according to his needs.

In addition with the need of a secure Log Server, each provider should be assigned with independent public/secret key pairs (e.g. *PK*1*/SK*1, *PK*2*/SK*2) and use them according to the implemented scenarios. For example, keys *PK*1*/SK*1, *PK*2*/SK*2 may be used to sign log files and log events, respectively. Following, the signatures should be sent to the RA. The signature keys should be certified through the corresponding digital certificates (e.g. *Cert*1, *Cert*2). The digital certificates are issued by a mutually trusted, external certification authority, so that all the parties can verify the validity of the signatures (e.g. generated with the keys *SK*1, *SK*2). The key management functions such as generation, certification, revocation and updating of the signature keys may be supported by one or more independent certification authorities, which are trusted by the *RA* and the providers. The various scenarios that can be implemented mainly regard what information should be signed (log files or leg events) and the signing frequency of the logged information. Hence, scenarios such as, a) signing log files in predefined time periods, b) real time signing of critical log events (this is feasible because critical log events create a small number of events in comparison to the total number of log events), c) real time signing of the random log events (the provider collects real time log events in time intervals of his decision). Moreover the Provider should identify the architecture that he will decide to use either for collecting the logging information or for storing the produced signatures and the signed logged information.

B.3 Providing the skeleton for implementing a secure log environment

The implementation of the log signing scenarios mentioned above requires a distributed architecture with dedicated services, which will implement the above mentioned scenarios. Figure B.2 illustrates the main entities with their interfaces that are required for creating a secure log environment, involving both the provider and the *RA*.

These entities are analyzed:

(1) The *Mediation Log Device*. It aims to have a central management and mediation role among the LI/DR nodes and the external authorities (external authorities are required if possible generated signatures need to be sent to them), necessary for the execution of all possible log scenarios. It hosts the required business logic and communicates with the *RA* through a well-defined secure interface. Many sessions that implement above mentioned scenarios should be allowed to be served in parallel by this node. Finally, this device should hold a secret key (e.g. *SK*2) that could be used to sign *random log events* and being able to send signatures to the *RA*.

(2) The *Secure Log Server*. This is a cryptographically enhanced Log Server that is required for collecting the log events from all the nodes of the LI/DR infrastructure and also communicating with the *Mediation Log Device* for receiving management commands during the execution of the implemented scenarios.

(3) The *Signature Server*. This is an isolated server that hosts the secret key *SK*1 or all the secrets keys (if the *Signature Server* holds all the secret keys then the *Mediation Log Server* does not need to hold any secret key). It should implement only one interface to receive signature requests normally from the *Mediation Log Device*. The secure Log Server and the Signature Server will have separate administrators. In this way, the Log Server administrator will not be privileged to access the keys.

(4) The *Network Nodes*. This entity is used to model any network or IT elements (routers, database servers, etc) that are involved in the execution of LI/DR scenarios and generate log events, which are following stored to the *Secure Log Server* or even in the *Mediation Log Device*. This means that *Network Nodes* are the log generators and are partially trusted nodes. Each *Network Node* should be enhanced or configured to receive commands (e.g. snmp trap requests) from the *Mediation Log Device* and responds back to him or sent log events directly to the S*ecure Log Server*.

(5) The *Terminal Equipment*. This entity is optional and is hosted within the RA side. It may initiate any session of the implemented scenarios, mainly those that require external initialization, by invoking requests towards the *Mediation Log Device* and at the end of the session execution to receive signatures from the *Mediation Log Device*. It should be able to store the signatures within a signature repository in a secure place either within or outside this entity.

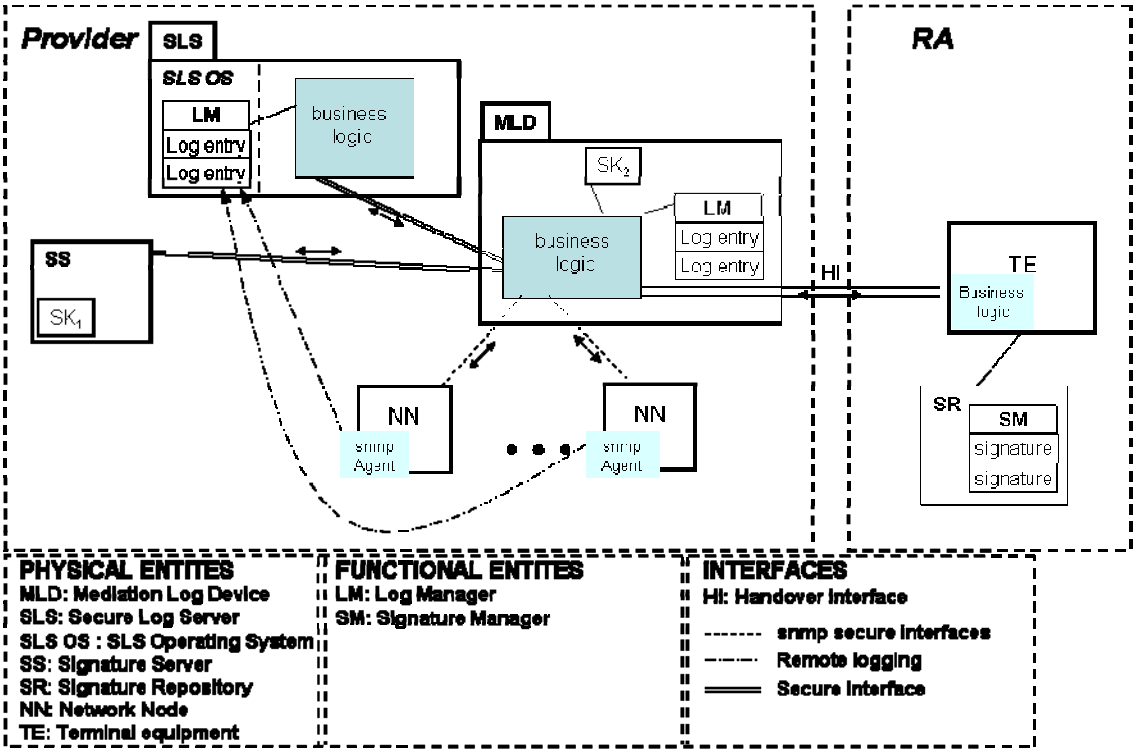


Figure B.2: Main entities that are required for creating a secure log environment

B.4 References annex B

[B1] V. Stathopoulos, P. Kotzanikolaou, E. Magkos, "Secure Log management for privacy assurance in electronic communications", accepted for publication in Computers and Security, Elsevier journal, 2008.

[B2] V. Stathopoulos, P. Kotzanikolaou, E. Magkos, "A Framework for Secure and Verifiable Logging in Public Communication Networks", J. Lopez (ed.): CRITIS 2006, LNCS4347, pp. 273-284, 2006, Springer Verlag Berlin Heidelberg, 2006.

Annex C:
Protection of retained data

C.1 Introduction

There are some basic requirements regarding storage of retained data related to personal integrity and security:

1) There should not be any leakage of information from the data repository.

2) It should be secured that retained data remain authentic, i.e. non-reputable.

3) Information about investigated cases should be protected.

The basic assumption for a security regime is that information is protected through regular procedures of the operators' and secured transmission links between operator and LEA. This is likely to be true for large operators, who can include O&M for retained data in their regular operations without excessive overhead. Smaller operators may however have a problem with this and would be interested in engaging a 3rd party service for administration of retained data. This would however bring security out of the operator's control and increase risks for leakage of various kinds. In order to eliminate such risks, a regime with encryption and hashing of critical data may be applied. A suggestion for such a scheme is presented here.

C.2 Overview of the proposed system

Figure C.1 shows key elements and mechanisms. It is suggested to use symmetrical, random generated, keys for the stored data and encrypt these with asymmetrical RSA-keys (public/private) for retrieval by LEAs. Index values would be processed through a hashing algorithm before storage. Queries for retained data would be performed with lookup of related index values. Key values provided by a LEA would be passed through the same hashing algorithm to produce lookup values for the related indices. By this, the requirements would be met in the following ways:

1) Leakage of information is prevented through encryption of stored data.

2) Data cannot be altered after storage, since key values are unknown (except to LEAs when data has been retrieved through due process).

3) Information about investigated cases, like phone numbers in a query, is protected through the hashing process.

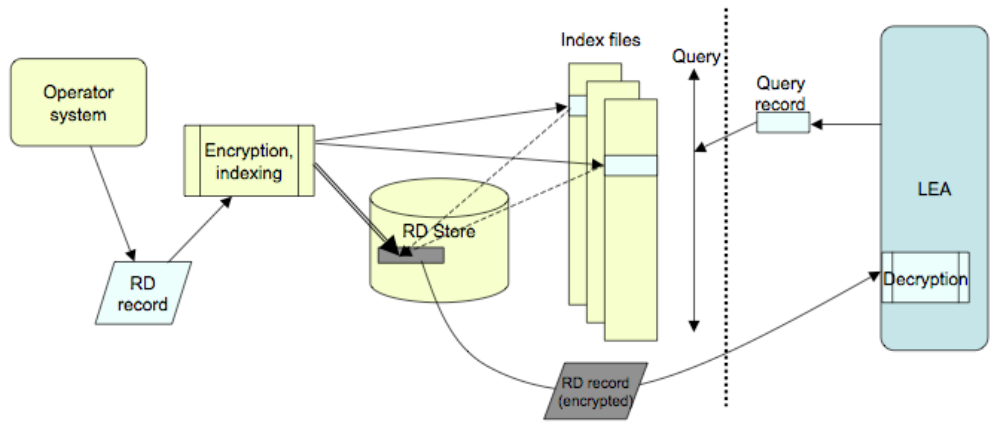


Figure C.1: Diagram of encryption/decryption process for RD Store

C.3 Encryption and storage of retained data record

When an RD record is sent for storage, it will be passed through a process for encryption of critical data and creation of index values.

First a set of key values to be indexed will be identified. These values will be passed through a hashing algorithm and stored in a set of index files along with a pointer to the location where the RD record will be stored.

Then a symmetrical key value will be generated in a random process. This key will be encrypted with the public key of the LEA(s). Possibly multiple encrypted key values will be generated, if there is a requirement that each LEA should have its own. There will however be only one symmetrical key value and one encrypted RD record.

Finally the RD record is encrypted with a symmetrical algorithm, e.g. DES-3, and stored in the repository.

Among the indices there should be a non-encrypted time stamp for the date of storage, such that obsolete RD records can be deleted when the retention period has expired.

C.4 Query and retrieval of retained data

When making a query, the LEA would set up one or more search criteria. Key values of these criteria would be passed through the hashing algorithm to create lookup values. The resulting query record(s) would be compared with the appropriate index file(s). If matching values are found, the corresponding RD record will be fetched from for RD Store and passed on to the LEA.

On arrival of a retrieved record, the LEA can decrypt the key value using the private key of the LEA. The retrieved key value can then be used to decrypt the contents of the RD record.

C.5 Purging of RD Store

There should be daily scans of the index where date of storage is kept. Any records that are older than the stipulated retention period should be purged from the RD Store.

C.6 Discussion of resilience and vulnerability

The data store would be resilient against scan of e.g. subscriber names or phone numbers, which otherwise might compromise data related to personal integrity.

The index files would be resilient against leakage of business critical information for an operator, such as how many subscribers there are, what the calling patterns are or how the base station network is configured; the hashed index values would not reveal any such relationships.

When querying about a specific subscriber name, a phone number, a location etc, the LEA would not reveal identities outside its own premises. Hashed values cannot be reversed to find out input data.

The most apparent vulnerability of this system is that a private key for a LEA might be compromised. This would allow an intruder, who has access to the RD repository, to decrypt keys of the RD records and then decrypt contents. If such an intrusion is detected, the remedy would be to re-encrypt key values in the RD store, using a new set of asymmetric keys. The contents of the store itself would however not have to be re-encrypted to protect contents. It may be observed that access to key values would be of rather limited value, since the intruder would be left with a chunk of data several hundred Terabytes large to decrypt record-by-record before they can be compromised.

Annex D:
Guide for selecting cryptographic algorithms and minimum key sizes in LI/DR systems

D.1 Introduction

To protect information assets in the context of LI/DR systems the selection of the appropriate cryptographic protocols, algorithms, and keys to reach the security objectives is an essential task that needs to be done.

Although it is widely recognized that the openness principle is the right approach, it still does not make the problem of implementing security a minor task since it is still needed to determine which algorithms and keys are appropriate for the required level of security without hindering the functionality and performance of the system.

The purpose of this annex is providing guidance to make this selection easier and more adequate for this specific context.

In order to establish the level of security needed, it is required to consider *the nature the information to be protected, the type of foreseen attackers* and *the period of time* that the information needs to be protected.

In relation to the first matter, a *classification* of the information managed by the LI/DR systems is needed. Since information classification depends upon national circumstances and regulations, general approaches setting the proper framework will be given.

Concerning the second issue, the traditional attackers categories ("hackers", small, medium or large organization and intelligence agencies), each with different motivations and resources, may provide a first approach to the security level required. Since the special sensitiveness of the information managed by LI/DR systems and the key sizes recommended should be those that would make the attack unfeasible for intelligence agencies as far as it can be guarantee with the known state-of-the-art.

On the other hand, when security is to be maintained for longer periods than a few months, it should be taken into consideration that attackers may upgrade their resources according to state-of-the-art developments. A generally accepted way to deal with this point is to assume Moore's law.

This annex gives guidance for selecting cryptographic algorithms and key lengths in order to acquire the desired level of security. The main categories studied are the following:

- Symmetric key algorithms.
- Asymmetric key algorithms.
- Hash functions.

Although only standardized, prevalent, mature, and algorithms that have received and intensive security analysis are included, the fact that a specific algorithm is not mentioned in this annex cannot be taken as indication that the particular algorithm is not recommended. Reasons for exclusion may be limited practical use because of the lack of standardization and/or deployment, etc. On the other hand, inclusion does not guarantee that a particular algorithm is secure, only that it is secure as known in current state of the art. Moreover, while different experts agree that it is to be expected that Moore's law will continue to be valid for at least a decade or even more, it may also need to be considered others entirely different types of hardware and computational models and suggest the applicable solutions for those cases (e.g. quantum computing).

Finally it is necessary to emphasize the importance of acquiring cryptographic systems with appropriate algorithm and key sizes to provide sufficient protection for the expected life of the system and also for any data protected by the system during the expected lifetime of the data.

The recommendations given in this annex assume that the algorithm is properly implemented, used, and managed and run in a secure environment not subject to side-channel attacks.

D.2 Cryptographic security strength basis and LI/DR systems

Depending of the algorithm and the key size used, cryptographic algorithms provide different level or strengths of security. One basic concept to measure the cryptographic security strength is the number of *bits of security.*

D.2.1 Bits of security

An algorithm's key size is different from its cryptographic security. The security of an algorithm for a specific key size is measured in "*bits of security*", that will not necessary match the number of bits of the key. The security strength is a logarithmic measure of the fastest known computational attack on the algorithm, also measured in bits. Therefore, the security of an algorithm cannot exceed its key length since any algorithm can be cracked by brute force but it can be smaller.

Although most symmetric key algorithms are design in such a way that their security is equal to their key size, in some cases it can be smaller. For example, Triple DES with a key size of 168 bits provides at most 112 bits of security.

On the other hand, asymmetric-key algorithms do not have this property and elliptic curve cryptography usually has an effective security of approximately half its key length.

The following table shows an example of how the number of *bits of security* protects the information against different kinds of attacks providing different security levels.

Table D.1: Security levels

Security level	Bits of security	***Protection***
1	32	*Attacks in real time by individuals*
2	64	*Very short term protection against small organizations*
3	72	*Shirt-term protection against medium organizations, medium protection against small organizations*
4	80	*Very short term protection against agencies, long term protection against small organizations*
5	96	*Legacy standard level*
6	112	*Medium term protection*
7	128	*Long-term protection*
8	*256*	*Foreseeable future*

D.2.2 Bits of security in LI/DR systems

In order to select, in a more accurate manner, the most appropriate number of bits of security for the cryptographic material used in LI/DR systems, it is necessary to study the nature of the information managed by these systems. A classification of the information is needed as it is shown in the following clause.

D.3 LI/DR information classification

Classification of information is a key task prior to define any general security measure and more specifically in relation to the selection of cryptographic algorithms and key sizes.

A study of the nature of the different types of information managed by the f LI/DR systems is essential to perform a classification with the purpose of selecting the most appropriate cryptographic material.

A very first approach to this kind of study, subject to national regulations but with many points in common within larger communities (e.g. EU directives, international agreements etc.), show two main groups that may be observed.

1) Classified information.

2) Personal data.

D.3.1 Classified information

Some of the information managed by LI/DR systems is classified information. The term classified information means any information (or material) an unauthorized information of which could cause varying degrees of prejudice to the countries' affected.

Although the classification systems vary from country to country, most have levels corresponding to the following definitions: Top Secret, Secret, Confidential and Restricted. A comparison of national security classifications can be found in the Council decision of 19 March 2001 adopting the Council's security regulations (2001/264/EC [i.8]).

D.3.2 Personal data

LI/DR systems also manage personal data. Personal data means, according to the Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 [i.6], any information relating to an identifiable natural person.

Although the classification of personal data varies from country to country, most have levels corresponding to the following definitions: basic and high or basic, medium and high.

D.3.3 Classification levels equivalence

Table D.2 is merely orientative and intends to represent the equivalence between the information classification levels, regarding security measures.

Table D.2: Classification levels equivalence

<table>
<tr><th>CLASSIFIED INFORMATION</th><th>PERSONAL DATA</th></tr>
<tr><td>TOP SECRET</td><td></td></tr>
<tr><td>SECRET</td><td></td></tr>
<tr><td rowspan="2">CONFIDENTIAL</td><td></td></tr>
<tr><td rowspan="2">HIGH</td></tr>
<tr><td rowspan="2">RESTRICTED</td></tr>
<tr><td rowspan="2">MEDIUM</td></tr>
<tr><td rowspan="2">UNCLASSIFIED</td></tr>
<tr><td>BASIC</td></tr>
</table>

D.4 Cryptographic algorithms and key sizes for LI/DR systems

D.4.1 Minimum bits of security

Table D.3 shows the recommended minimum number of bits of security depending on the security lifetime and the desired level of protection.

NOTE: In some cases, as it is in the Spanish regulation on personal data protection, retained data is classified as personal data that needs a high level of protection.

Table D.3: Recommended minimum bits of security

Bits of security	Security lifetime	Level of protection for classified information	Level of protection for personal data
80	Through 2010	RESTRICTED	BASIC/MEDIUM
112	Through 2030	CONFIDENTIAL	HIGH
128	Beyond 2030	SECRET	HIGH
192	Beyond 2030	SECRET/TOP SECRET	HIGH
256	Beyond 2030	TOP SECRET	HIGH

D.4.2 Symmetric key algorithms

For symmetric key algorithms, if it is assumed that they are secure for the lifetime of protected data, the only attack way is generally a brute force or exhaustive key search attack. However, as we mention before, the characteristics of some cryptographic algorithms make possible that a certain kind of attack reduces the amount of work necessary to find the correct key by not being necessary to try all of them. In this case the bits of security would be less than the key size.

Table D.4: Symmetric key algorithms security strengths

Bits of security	Symmetric key algorithms
80	2TDEA
112	3TDEA
128	AES-128
192	AES-192
256	AES-256

D.4.3 Asymmetric key algorithms

In the case of asymmetric cryptography there are more efficient attacks than brute force (e.g. factorization). For that reason comparative studies between symmetric key strength and asymmetric key strength are needed to assess the level of security against the common measure of *bits of security*. For frequently used symmetric and asymmetric keys the equivalence is the following (see table D.5).

Table D.5: Asymmetric key algorithms security strengths

Bits of security	FFC (DSA,D-H)	IFC (RSA)	ECC (ECDSA)
80	L=1024 N=160	k=1024	f = 160-223
112	L=2048 N=224	k=2048	f = 224-255
128	L=3072 N=256	k=3072	f = 256-383
192	L=7680 N=384	k=7680	f = 384-511
256	L=15360 N=512	k=15360	f = 512+
FFC: Finite field cryptography L: public key size N: private key size IFC: Integer factorization cryptography k: key size ECC: Elliptic curve cryptography f: key size			

D.4.4 Hash functions

In relation to hash functions the number of bits of security depends not only upon the specific function and the output or hash size, but also by the algorithm or scheme in which the hash function is going to be used.

NOTE: Some applications may require a message digest that is shorter than the full-length message digest provided. In such cases, it may be appropriate to use a subset of the bits produced by the cryptographic hash function as the shortened message digest. Truncating the message digest can impact the security of an application. By truncating a message digest, the estimated collision resistance strength is reduced. For example, even though SHA-256 provides 128 bits of security, the bits of security provided by a 96-bit truncated message digest are half the length of the truncated message digest, which is 48 bits, in this case

Table D.6: Hash functions security strengths

Bits of security	Digital Signatures and hash-only applications	HMAC Key derivation functions Random number generation
80	SHA-224 SHA-256 SHA-384 SHA-512	SHA-1 SHA-224 SHA-256 SHA-384 SHA-512
112	SHA-224 SHA-256 SHA-384 SHA-512	SHA-1 SHA-224 SHA-256 SHA-384 SHA-512
128	SHA-256 SHA-384 SHA-512	SHA-1 SHA-224 SHA-256 SHA-384 SHA-512
192	SHA-384 SHA-512	SHA-224 SHA-256 SHA-384 SHA-512
256	SHA-512	SHA-256 SHA-384 SHA-512

D.4.5 Summary table

Table D.7: Security strengths summary table

Security lifetime	Information classification 1. Classified information 2.Personal data	Symmetric key algorithms	FCC (e.g. DSA, D-H)	IFC (e.g. RSA)	ECC (e.g. ECDSA)	Digital Signatures and hash-only applications	HMAC Key derivation functions Random number generation	Security lifetime
THROUGH 2010 (>= 80 bits of security)	RESTRICTED BASIC/MEDIUM	2TDEA 3TDEA AES-128 AES-192 AES-256	Minimum: L=1024 N=160	Minimum: K=1024	Minimum: f=160	SHA-224 SHA-256 SHA-384 SHA-512	SHA-1 SHA-224 SHA-256 SHA-384 SHA-512	THROUGH 2010 (>= 80 bits of security)
THROUGH 2030 >= 112 bits of security	CONFIDENTIAL HIGH	3TDEA AES-128 AES-192 AES-256	Minimum: L=2048 N=224160	Minimum: K=2048	Minimum: f=224	SHA-224 SHA-256 SHA-384 SHA-512	SHA-1 SHA-224 SHA-256 SHA-384 SHA-512	THROUGH 2030 >= 112 bits of security
BEYOND 2030 >= 128 bits of security	SECRET HIGH	AES-128 AES-192 AES-256	Minimum: L=3072 N=256	Minimum: K=3072	Minimum: f=256	SHA-256 SHA-384 SHA-512	SHA-1 SHA-224 SHA-256 SHA-384 SHA-512	BEYOND 2030 >= 128 bits of security
BEYOND 2030 >= 192 bits of security	SECRET/TOP SECRET HIGH	AES-192	Minimum: L=7680 N=384	Minimum: K=7680	Minimum: f=384	SHA-384 SHA-512	SHA-224 SHA-256 SHA-384 SHA-512	BEYOND 2030 >= 192 bits of security
BEYOND 2030 >= 256 bits of security	TOP SECRET HIGH	AES-256	Minimum: L=15360 N=512	Minimum: K=15360	Minimum: f=512 * (*f=384 is recommended for performance reasons)	SHA-512	SHA-256 SHA-384 SHA-512	BEYOND 2030 >= 256 bits of security

D.4.6 Algorithm suites

Many applications require the use of several different cryptographic algorithms. In general, the weakest algorithm and key size used to provide cryptographic protection determines the strength of the protection. Exceptions to this principle require extensive analysis.

D.5 Bibliography annex D

[D1] ECRYPT Yearly Report on Algorithms and Key sizes, http://www.ecrypt.eu.org/documents/D.SPA.21-1.1.pdf

[D2] NESSIE consortium, NESSIE Security report, available at https://www.cosic.esat.kuleuven.be/nessie/deliverables/D20-v2.pdf

[D3] Recommendation for Key Management, Special Publication 800-57 Part 1, NIST, 03/2007, available at http://csrc.nist.gov/groups/ST/toolkit/documents/SP800-57Part1_3-8-07.pdf

[D4] Fact Sheet NSA Suite B Cryptography http://www.nsa.gov/ia/industry/crypto_Suite_b.cfm?MenuID=10.2.7

[D5] Bekanntmachung zur elektronischen Signatur nach dem Signaturgesetz und der Signaturverordnung (Übersicht über geeignete Algorithmen) http://www.bundesnetzagentur.de/media/archive/12198.pdf

[D6] Algoritmos y parámetros para firma electrónica segura. CCN-STIC-405 https://www.ccn-cert.cni.es/publico/2008/ccn-stic/CCN-STIC-405.htm

Annex E:
Change request history

Status of the present document: TR 102 661 Security framework in Lawful Interception and Retained Data environment		
Date	**Version**	**Remarks**
October 2008	1.1.1	First publication of the TR after approval by ETSI/TC LI#19 (30 September - 2 October 2008, Prague) Version 1.1.1 prepared by Vassilis Stathopoulos (ADAE) (rapporteur TR)

History

Document history		
V1.1.1	November 2008	Publication