Security framework for an LI/DR infrastructure

ETSI TC LI Work Item
DTR/LI-00044

Vassilios Stathopoulos
ADAE - Authority for the Assurance of Communication Security and Privacy
Greece

Work so far

- European ETSI/TC LI meetings over the last 12 months and a lot of group discussions
- Up to 75 people from services providers, governments and equipment vendors
- We have created a final draft; we hope for approval at the ETSI/TC LI Meeting (30 September – 2 October in Prague)

ETSI WI - DTR/LI-00044 ToC

- ***Scope***
- **Inventory of LI/DR assets**
- ***Security threats and attack scenarios***
- ***Security measures***
  - *Personnel security*
  - *Incident Handling*
  - *Physical and Environmental security*
  - *Media Handling*
  - *Access Control policy*
  - *Confidentiality (stored data/ transmitted data)*
  - *Integrity (system software/stored data/ transmitted data)*
  - *Non-repudiation*
  - *Secure Verifiable and Intelligible logging*
  - *Secure Information destruction*
  - *Development Maintenance and Repair*

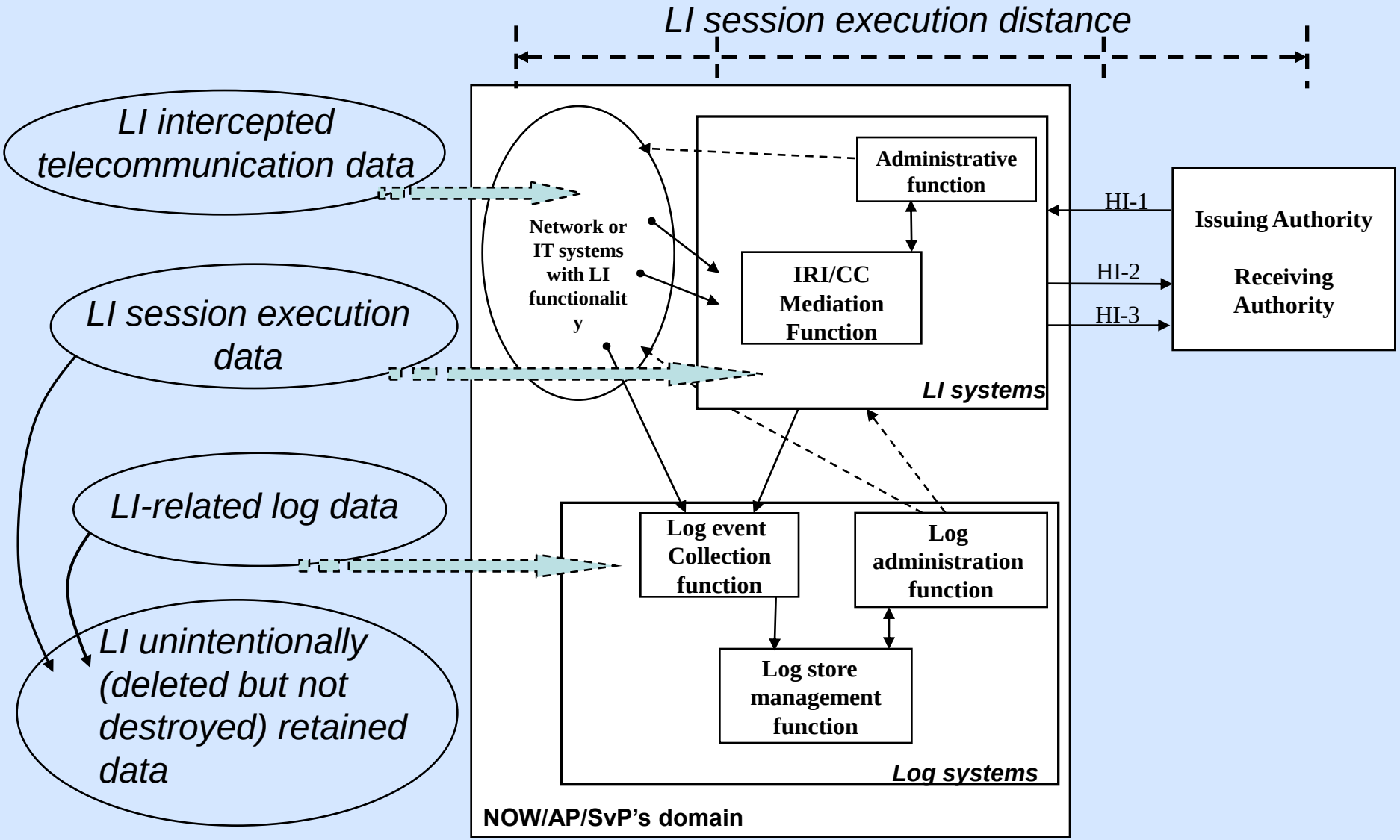
ETSI WI - DTR/LI-00044 ToC

- **Annex A :** table that associates security measures with
  - threats and
  - system functionalities
- **Annex B:** secure logging policy in a LI/DR environment
- **Annex C:** Protection of retained data
- **Annex D:** A Guide for cryptographic algorithms

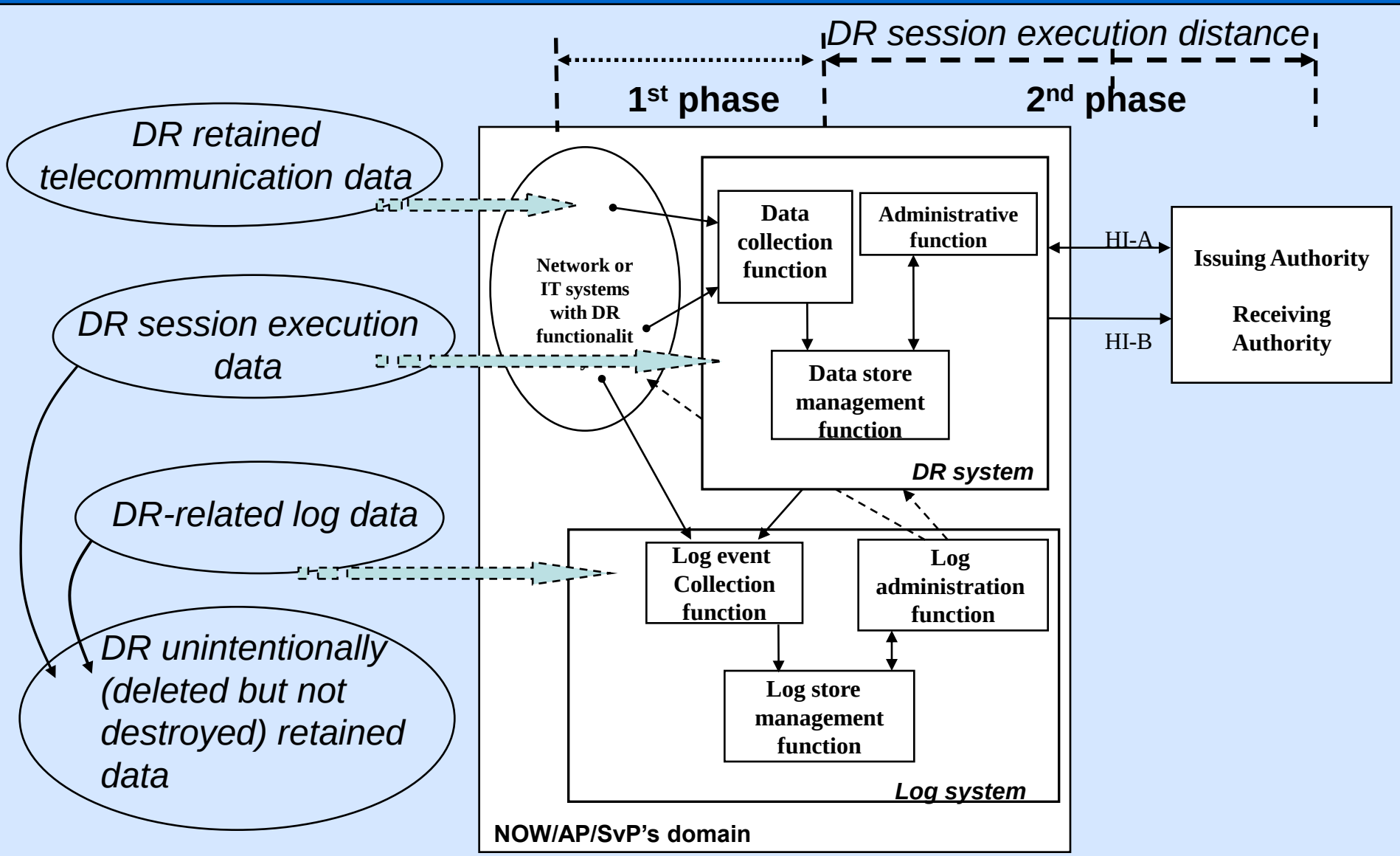
LI/DR data

- ***a lawful interception (LI) session***
  - *is an **one phase procedure***
  - *concerns **oncoming** activities of **one** target*
  - *produce LI data that are retrieved from the **network or the IT systems** at real time.*
  - ***no information** (CC or IRI) **is retained** or stored*
- ***a Data Retention session***
  - *is a **two phase procedure***
  - *concerns **past** activities of **one** target*
  - *produce DR data that are retrieved from the **storing system***
  - ***personal information** of all customers **is retained** and can be implicitly retrieved.*

LI architecture



DR architecture



Need to know

- ***For applying an effective security framework a CSP needs to know***
  - *The architecture of LI/DR infrastructure*
  - *The architecture of the log system*
  - *The assets inventory (informational, functional, software, physical)*
  - *The threats that exist in the network*
  - *analyze the attack scenarios*

Threats

- ***Threat list***
  - *(T1) Disclosure of information assets*
  - *(T2) Modification of information assets*
  - *(T3) Unauthorized access to the LI/DR data*
  - *(T4) Unauthorized access to the LI/DR or Log infrastructure*
  - *(T5) LI/DR infrastructure(or service) abuse*
  - *(T6) Illegal use of the retained data*
  - *(T7) Repudiation*
  - *(T8) Prolonged interception or retention of data*
  - *(T9) Recovery of unintended data.*
  - *(T10) Denial of Service*

Attack Scenarios

- **Attack scenarios by remote or local users**
  - **a malicious user**
    - may use the authenticated LI/DR services to eavesdrop LI/DR data
    - needs to modify *access admin log files* and *command log files*
  - **a malicious user**
    - may install a malicious LI/DR application to eavesdrop LI/DR data
    - needs to modify log files related to installation policy and stop all related alerts
  - **a malicious user**
    - may issue fake DR requests (LEA side)
    - may send legal LI/DR answers and later deny this dispatch
  - **a malicious user**
    - may perform forensic analysis in a storing system and reproduce partial histories from the unintended traces

Security Measures

- **Personnel Security**
  - define roles
    - i.e. team leader, auditor, system user, system administrator, Log system administrator
  - define their duties
- **Incident Handling**
  - Incident plan
  - Essential measures and the personnel duties to encounter the incident
- **Physical and Environmental security**
  - Rules, systems and measures for preventing the unauthorized physical access
    - e.g. The LI/DR installation/room shall be protected by using all the necessary control mechanisms (barriers and locks, to all external doors and windows)

Security Measures

- **Media Handling**
  - restrictions in handling and moving the media when that is required
    - e.g. secure storages (that contain hard copies or electronic storage media) will be opened only by the team leader and the Log administrator
- **Access Control**
  - authentication criteria
    - strong cryptographic authentication mechanisms for local or remote users access
  - authorization criteria to be associated with roles and user groups
  - general access controls
    - e.g. recommends a specific number of maximum login attempts, log the login attempts

Security Measures

- **Confidentiality – Encryption**
  - for stored LI/DR data
    - is recommended to be encrypted by using AES during their storage
  - for transmitted LI/DR data
    - at internal interfaces, data are recommended to be routed independently of other traffic
    - at external interfaces, data are recommended to be protected with strong encryption. Use of TLS protocol. **(ETSI TS102 232)**
- **Integrity – Hashing**
  - for system software and services
    - are recommended to be signed by means of a recognized electronic signature
  - for stored LI/DR data
    - use hashing (SHA-1 or HMAC) for LI/DR data and secure logging techniques for their log data
  - for transmitted data
    - ETSI TS 102 232 analysis a technique for LI data
    - ***ETSI DTS/LI-00033*** describes a method for DR data integrity protection

Security Measures

- **Non repudiation of origin**
  - For LI case, digital signatures (RSA or DSA) are recommended
  - For DR case, an application level security technique is required

Secure Logging

- **Secure, Verifiable and Intelligible Logging**
  - A LOGGING POLICY is recommended with requirements for:
    - collecting Log Events,
    - creating Log Files
    - achieving secure Storing and Maintenance and
    - pointing out a log network infrastructure and its implementation design

Secure Logging

- **List of functions that should be logged (4 categories):**
  - **LI/DR session functions.**
    - commands involved in initiating, monitoring, terminating and operating LI/DR sessions.
  - **Security functions.**
    - user access control functions, user authentication and authorization functions, user account management functions, etc..
  - **System services and OS management functions**
  - **Network management functions**

Secure Logging

- **Define requirements:**
  - Continuous Logging, log files format, storage (i.e. the form, duration and location of storage), use remote log servers
  - *Secure Log files*
  - *Secure log entries* and guaranty confidentiality and integrity
  - Define critical log events (e.g. system restart, modification of users, user roles, log files, e.t.c)
  - Secure Critical log events close to their generation systems

Secure Logging

- **Define more requirements:**
  - Encryption and signature keys should be protected in a secure and isolated Signature Server
  - Log servers and possible Signature servers should have separate administrators.
  - The Provider should identify the required implementation guidelines and propose a specific Log architecture.
  - The Provider should identify any required implementation scenarios

Secure Destruction

- **Requirements for secure information destruction**
  - Overwrite the logically deleted (but not destroyed) records that remain in the DB page.
  - B+Tree modifications should be overwritten.
  - Transaction log data. A strategy for expunction of these old log records is to encrypt the log data and following removing the encryption keys
  - Overwrite the storage medium with new data by using specific overwrite patterns.

Annex A

- The idea of Annex A is to create a “tick” list for helping the Provider to control its security measures in every system.
- Hence, Annex A lists
  - all security measures
  - associates security measures with threats and system functionalities

Annex B

- **Building a Secure Logging procedure**
  - **A Log Reference Model is proposed** (a guide for helping Providers to organize the collection of required Log information) :

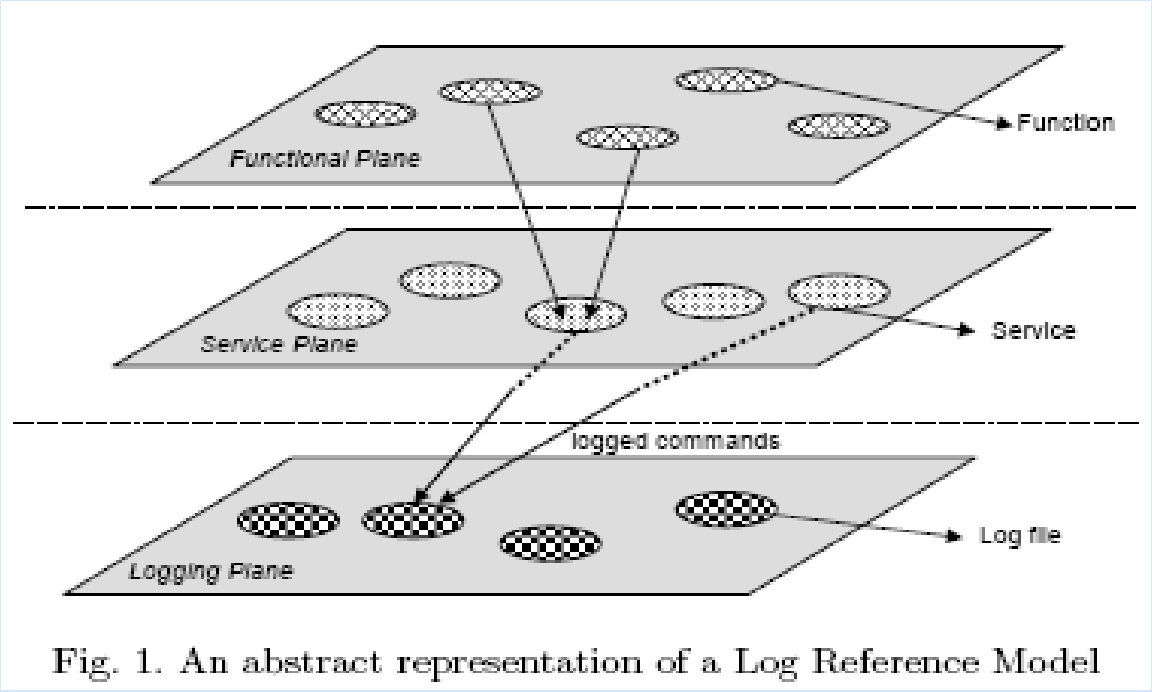


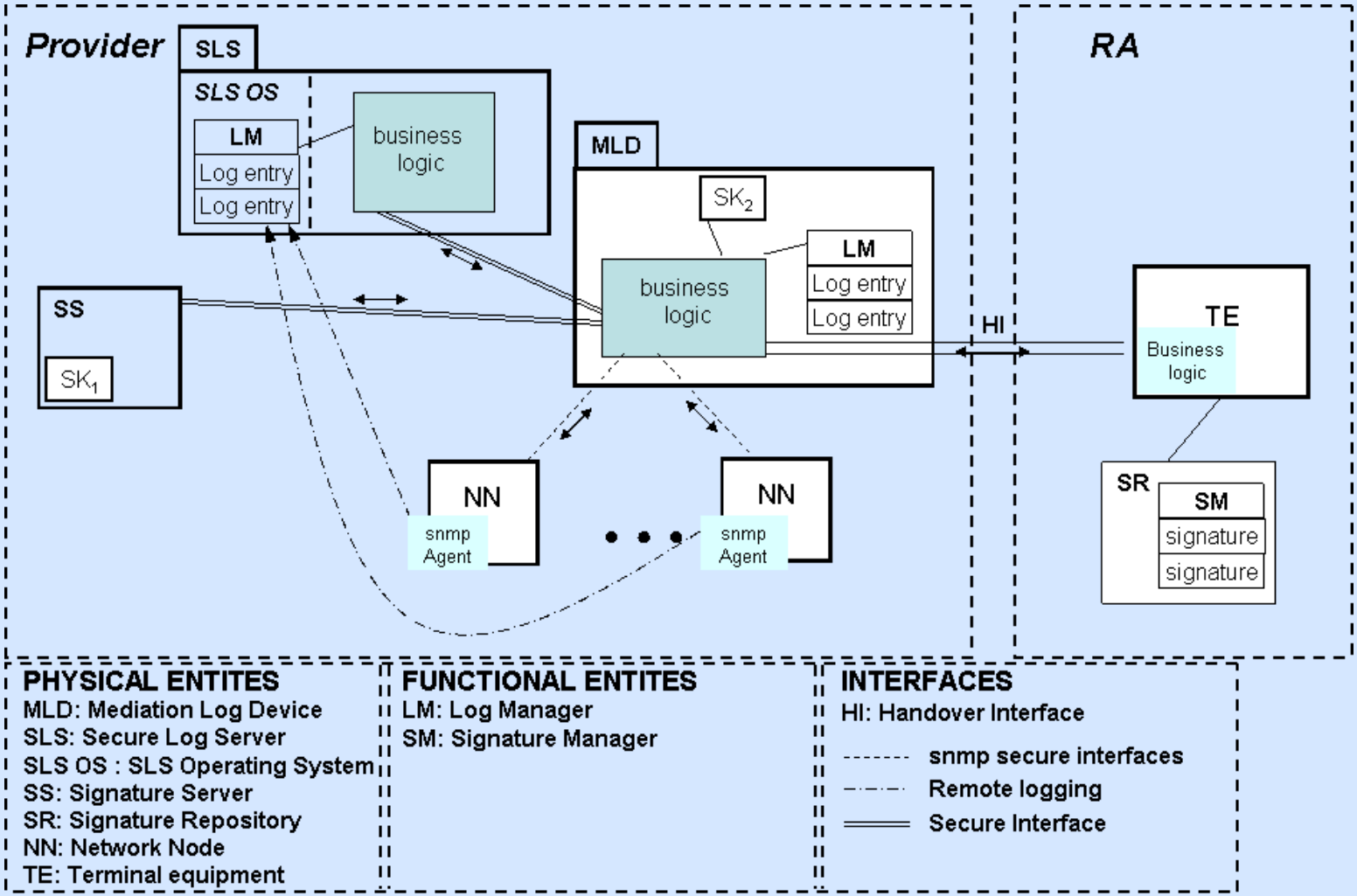
Fig. 1. An abstract representation of a Log Reference Model

Annex B (cont.)

- **Attack scenario**
  - attack into encrypted log events.
- **Solutions**
  - encrypted log files or log events is recommended to be additionally **signed** with asymmetric keys.
- **analysis can be found in papers**
  - V. Stathopoulos, P. Kotzanikolaou, E. Magkos, “Secure Log management for privacy assurance in electronic communications”, ready to be appeared in Computers and Security, Elsevier journal, 2008.
  - 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 B (cont.)

- a skeleton for implementing a secure log environment

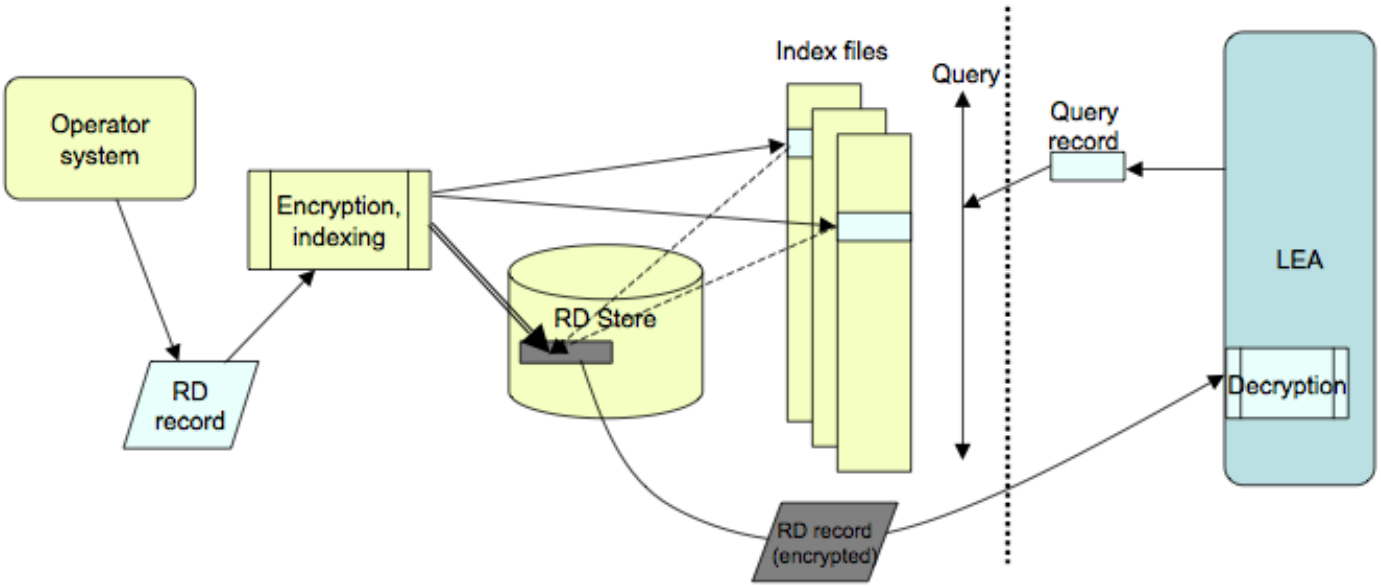


Annex C

- **Protection of Retained Data**
  - **Basic requirements regarding storage of retained data**
    - must not be any leakage of information from the data repository
    - must be secured that retained data remain authentic, ie non-reputable
    - Information about investigated cases must be protected

Annex C

- **Overview of the proposed system**



Annex C

- **implementation**
  - RD record will be encrypted and index values will be created
  - On request
    - request key values will pass through hashing by creating lookup values
  - On arrival
    - retrieved records will be decrypt by LEAs with his private key

Annex D

- **Guide for selecting cryptographic algorithms and minimum key sizes in LI/DR systems**
  - **It guides you with the appropriate algorithm and keys for the required level of security**
  - **It contains**
    - information classification
    - Guide for measure the cryptographic security strength called “bits of security”
    - Cryptographic algorithms and key sizes
    - Hash functions

Questions