ΕΛΛΗΝΙΚΗ ΔΗΜΟΚΡΑΤΙΑ
ΑΡΧΗ ΔΙΑΣΦΑΛΙΣΗΣ ΤΟΥ ΑΠΟΡΡΗΤΟΥ ΤΩΝ ΕΠΙΚΟΙΝΩΝΙΩΝ

Πλαίσιο ασφάλειας σε δικτυακό περιβάλλον Νόμιμης Συνακρόασης, καθώς και Διατήρησης και Παράδοσης των δεδομένων

"Security framework for an LI/DR infrastructure" ETSI TC LI - TR 102 661

Δρ. Βασίλειος Σταθόπουλος
ΕΕΠ/ΑΔΑΕ

Work so far

- **Ευρωπαϊκές ETSI/TC LI συναντήσεις για περισσότερο από 12 μήνες και συζήτηση με τα μέλη**
- **Περισσότεροι από 75 μέλη από παρόχους, κυβερνητικούς και εταιρείες κατασκευής**

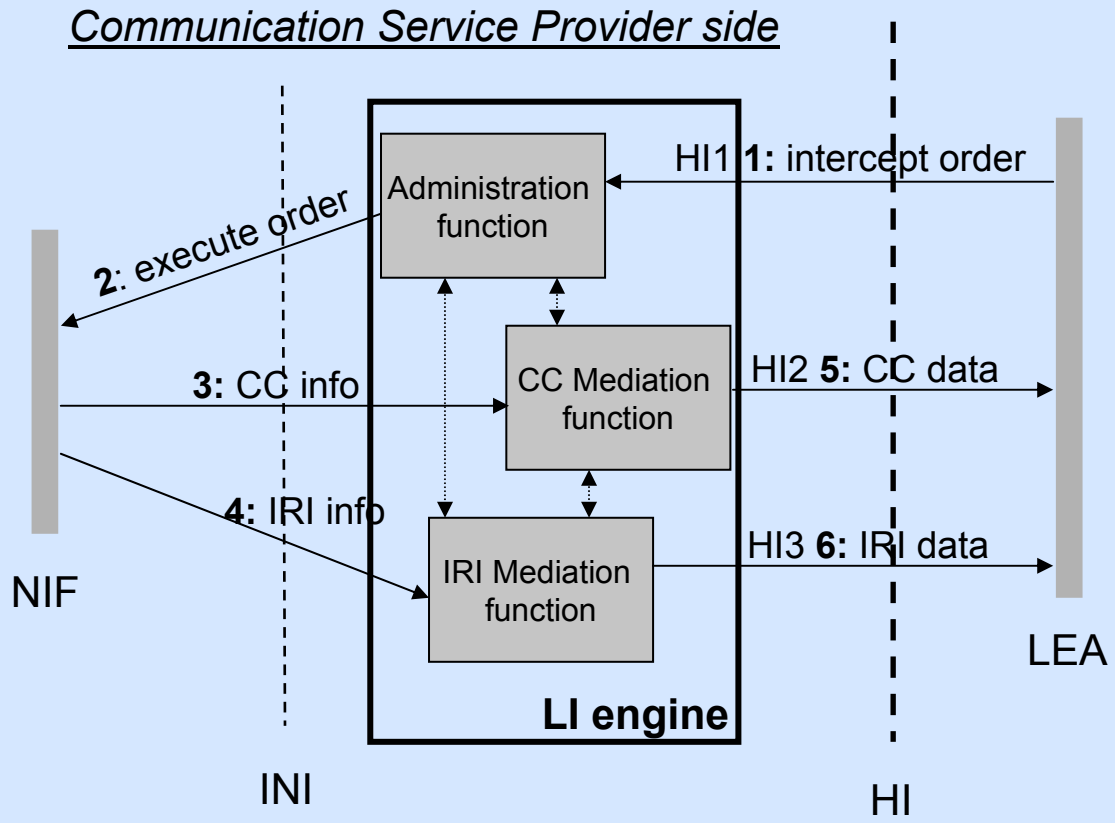
ETSI WI - DTR/LI-00044 ToC

- ***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 and delivery data
- **Annex D:** A Guide for cryptographic algorithms

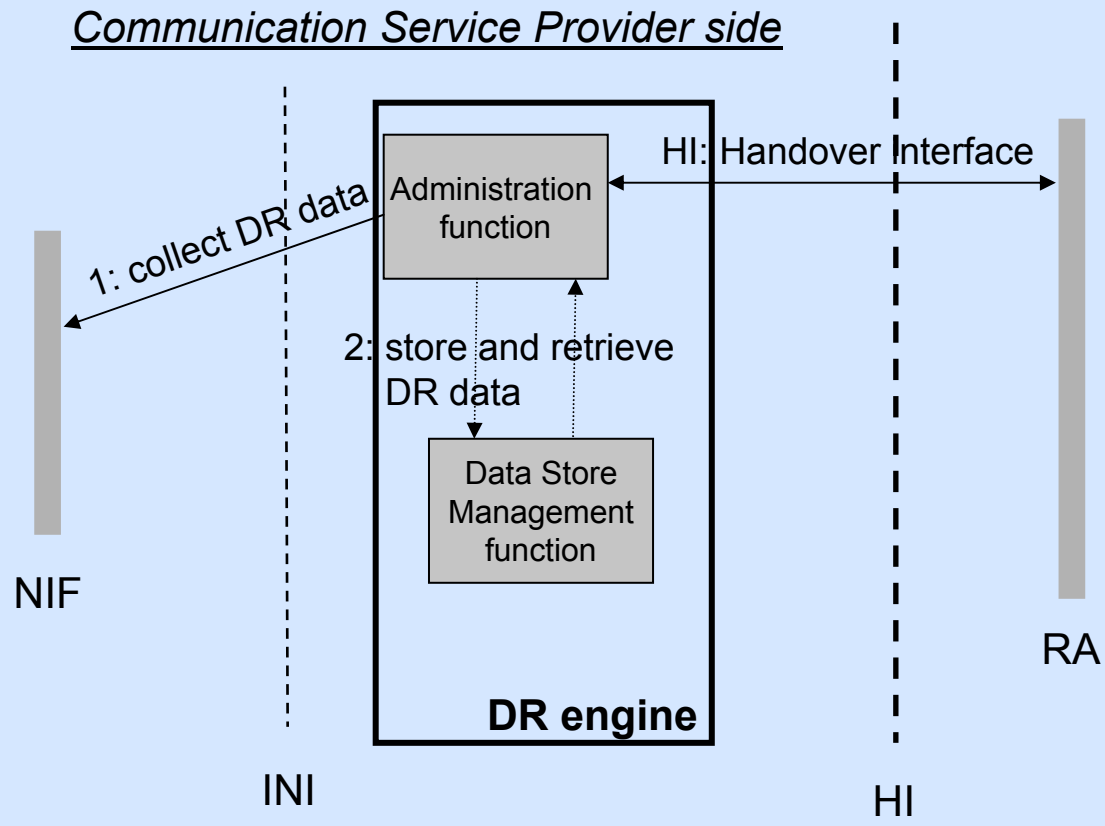
LI architecture



INI: Internal Network Interface
HI: Handover Interface
NIF: Network Internal Functions

CC: Content of Communication
IRI : Intercepted Related Information
LEA: Law Enforcement Agents

DR architecture



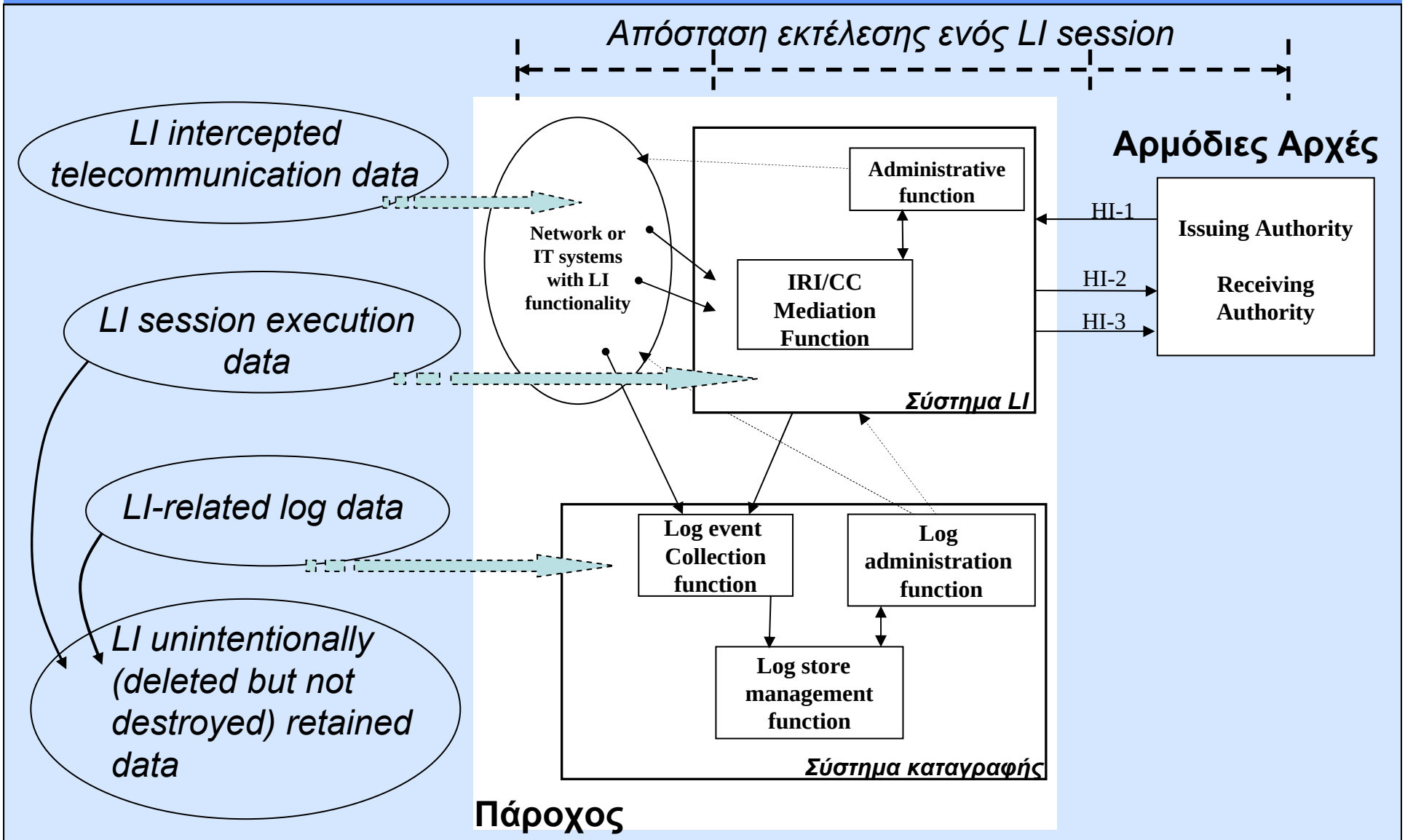
INI: Internal Network Interface
HI: Handover Interface

NIF: Network Internal Functions
RA: Requested Authority

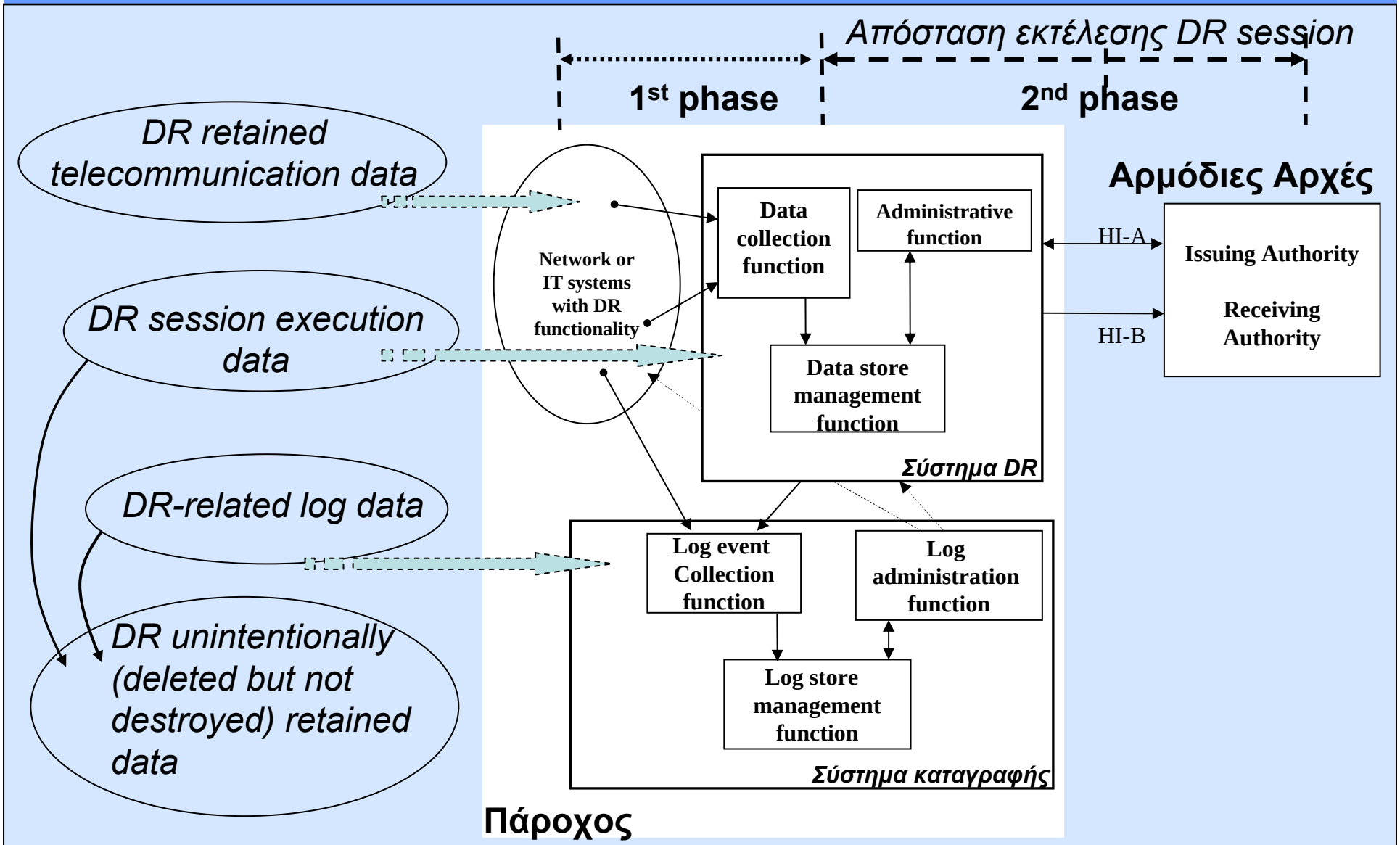
LI/DR data

- ***Ένα γεγονός Lawful Interception (LI)***
  - αποτελεί διαδικασία ***μίας φάσης***
  - αφορά τις ***μελλοντικές ενέργειες*** ενός «στόχου» κάθε φορά
  - παράγονται δεδομένα LI στους ***δικτυακούς και πληροφοριακούς κόμβους*** του παρόχου και λαμβάνονται σε πραγματικό χρόνο από αυτά
  - η απόρρητη ή η προς μετάδοση LI πληροφορία ***δεν διατηρείται και δεν αποθηκεύεται πουθενά*** στο πάροχο παρά μόνο στις Αρμόδιες Αρχές
    - διατηρούνται μονάχα τα *ίχνη εκτέλεσης και προσδιορισμού* της πληροφορίας
- ***Ένα γεγονός Data Retention (DR)***
  - αποτελεί διαδικασία ***δύο φάσεων***
  - αφορά τις ***παρελθοντικές ενέργειες*** ενός «στόχου» κάθε φορά
  - τα δεδομένα επικοινωνίας (ή δεδομένα DR) λαμβάνονται από το ***σύστημα αποθήκευσης*** που υπάρχουν ήδη αποθηκευμένα
  - Τα δεδομένα DR όλων των χρηστών-πελατών ***διατηρούνται σε συστήματα αποθήκευσης*** από όπου εν δυνάμει ανακτώνται.
    - Δεν διατηρείται η πληροφορία παρακολούθησης αλλά μόνο τα ίχνη εκτέλεσης και προσδιορισμού της πληροφορίας

LI architecture with Secure Logging



DR architecture with secure Logging



Need to know

- ***Για την εφαρμογή ενός αποτελεσματικού πλαισίου ασφάλειας ο Πάροχος πρέπει να γνωρίζει***
  - *Την αρχιτεκτονική της LI/DR υποδομής*
  - *Την αρχιτεκτονική του συστήματος καταγραφής (log system)*
  - *Την λίστα των προς διασφάλιση στοιχείων (πληροφορία, εφαρμογές, συστήματα)*
  - *Τις απειλές που υπάρχουν στο δίκτυο*
  - *ανάλυση κάποιων σεναρίων επίθεσης*

Threats

- ***Λίστα απειλών***
  - *(T1) αποκάλυψη των στοιχείων πληροφορίας*
  - *(T2) τροποποίηση των στοιχείων πληροφορίας*
  - *(T3) αναρμόδια πρόσβαση σε δεδομένα LI/DR*
  - *(T4) αναρμόδια πρόσβαση σε LI/DR υποδομή ή συστήματα καταγραφής*
  - *(T5) εξαπάτηση της υποδομής LI/DR (ή των υπηρεσιών)*
  - *(T6) παράνομη χρήση των DR δεδομένων*
  - *(T7) αποποίηση ευθύνης*
  - *(T8) παράταση χρήσης δεδομένων DR*
  - *(T9) ανάκτηση των αθέλητα διατηρουμένων δεδομένων.*
  - *(T10) Άρνηση παροχής της υπηρεσίας (Denial of Service)*

Attack Scenarios

- **Attack scenarios από εξωτερικούς ή τοπικούς χρήστες**
  - **Ο κακόβουλος χρήστης**
    - χρησιμοποιεί πιστοποιημένη πρόσβασή σε LI/DR υπηρεσίες και υποκλέπτει LI/DR δεδομένα
    - πρέπει να τροποποιήσει τα *access admin log files* and *command log files*
  - **Ο κακόβουλος χρήστης**
    - εγκαθιστά μία κακόβουλη εφαρμογή μέσα στους κόμβους του παρόχου ή αλλοιώνοντας την LI/DR μηχανή και υποκλέπτει LI/DR δεδομένα
    - πρέπει να τροποποιήσει τα σχετικά log files για installation policy και να διαγράψει όλα τα σχετικά alerts
  - **Ο κακόβουλος χρήστης**
    - αποστέλλει πλαστά DR requests (LEA side)
    - μπορεί να στείλει νόμιμες LI/DR απαντήσεις και ακολούθως να αρνηθεί αυτή τη αποστολή
  - **Ο κακόβουλος χρήστης**
    - Μπορεί να εκτελέσει forensic analysis σε ένα σύστημα αποθήκευσης και να αναπαράγει πληροφορίες (partial histories) από τα αθέλητα διατηρούμενα δεδομένα

Security Measures

- **Ασφάλεια προσωπικού (Personnel Security)**
  - Ορίσει ρόλους (roles)
    - i.e. team leader, auditor, system user, system administrator, Log system administrator
  - Ορίσει τα καθήκοντά τους
- **Διαχείριση περιστατικών ασφάλειας**
  - Πλάνο περιστατικών ασφάλειας
- **Φυσική ασφάλεια**
  - Κανόνες, συστήματα και μέτρα ασφάλειας, για την αποφυγή της μη εξουσιοδοτημένης φυσικής πρόσβασης
    - Π.χ. The δωμάτιο LI/DR πρέπει να προστατεύεται με μηχανισμούς ασφάλειας (μπάρες, κλειδαριές, σε όλες τις πόρτες και στα παράθυρα)

Security Measures

- **Διαχείριση μέσων (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
- **Έλεγχος πρόσβασης (Access Control)**
  - Κριτήρια πιστοποίησης
    - strong cryptographic authentication mechanisms για τοπική ή απομακρυσμένη πρόσβαση
  - Κριτήρια εξουσιοδότησης να συνδέονται με ρόλους και ομάδες χρηστών
  - Γενικές αρχές πρόσβασης
    - Π.χ. προτείνεται συγκεκριμένος αριθμός με μέγιστες προσπάθειες πρόσβασης, καταγραφή των προσπαθειών πρόσβασης, κ.τ.λ

Security Measures

- **Εμπιστευτικότητα – Κρυπτογράφηση**
  - Για τα αποθηκευμένα LI/DR δεδομένα
    - Χρήση AES
  - Για τα μεταδιδόμενα LI/DR δεδομένα
    - Για τις εσωτερικές διεπαφές, τα δεδομένα συνίσταται να δρομολογούνται ανεξαρτητα από την υπόλοιπη κίνηση
    - Στις εξωτερικές διεπαφές, τα δεδομένα συνίσταται να προστατεύονται με strong encryption. Χρήση του TLS protocol. **(ETSI TS102 232)**
- **Ακεραιότητα – Hashing**
  - Για το λογισμικό και το υλικό
    - Υπογράφοντας με χρήση recognized electronic signature
  - Για τα αποθηκευμένα LI/DR δεδομένα
    - Χρήση hashing (SHA-1 or HMAC) για LI/DR δεδομένα και τεχνικές ασφαλούς καταγραφής για τα log data
  - Για τα μεταδιδόμενα LI/DR δεδομένα
    - ETSI TS 102 232 analysis a technique for LI data
    - ***ETSI DTS/LI-00033*** describes a method for DR data integrity protection

Security Measures

- **Μη αποποίηση της ευθύνης του αποστολέα**
  - Για το LI, συνίσταται η χρήση ψηφιακών υπογραφών (RSA or DSA)
  - Για το DR, συνίσταται application level security technique

Secure Logging

- **Ασφαλής, Επιβεβαιώσιμης και κατανοητής πολιτικής καταγραφής δεδομένων**
  - Απαιτείται η ενσωμάτωση μίας πολιτικής LOGGING που θα καλύπτει τις παρακάτω απαιτήσεις:
    - Συλλογή των Log Events,
    - Δημιουργία των Log Files
    - Επίτευξη διαδικασιών ασφαλούς αποθήκευσης και διατήρησης των logs και
    - Σχεδίαση και αποτύπωση της υποδομής ενός δικτύου καταγραφής (LOG δίκτυο) και των σχεδίων υλοποίησής του

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**

Ασφαλής Καταγραφή

- **Απαιτήσεις :**
  - Συνεχόμενη καταγραφή,
  - Απλό και δομημένο format για τα log files,
  - *Ασφαλή αρχεία καταγραφής και ασφαλείς εγγραφές (*confidentiality and integrity*)*
  - Ασφαλής Αποθήκευση (i.e.προσδιορισμός της διάρκειας και της περιοχής αποθήκευσης),
  - Χρήση απομακρυσμένων log servers

Ασφαλής Καταγραφή

- **Περαιτέρω Απαιτήσεις:**
  - Κλειδιά Κρυπτογράφηση και υπογραφής πρέπει να προστατεύονται σε ασφαλής και απομονωμένους Signature Server
  - Οι διαχειριστές στους Log servers και τους Signature servers πρέπει να είναι διαφορετικοί.
  - Ο Πάροχος πρέπει να ορίσει τους απαιτούμενους κανόνες υλοποίησης και να προτείνει μία συγκεκριμένη αρχιτεκτονική καταγραφής
  - Ο Πάροχος πρέπει να ορίσει όλα τα σενάρια υλοποίησης κυρίως για την συλλογή της πληροφορίας (log entries, critical log entries)

Secure Destruction

- **Απαιτήσεις για την ασφαλή καταστροφή της πληροφορίας**
  - 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) :

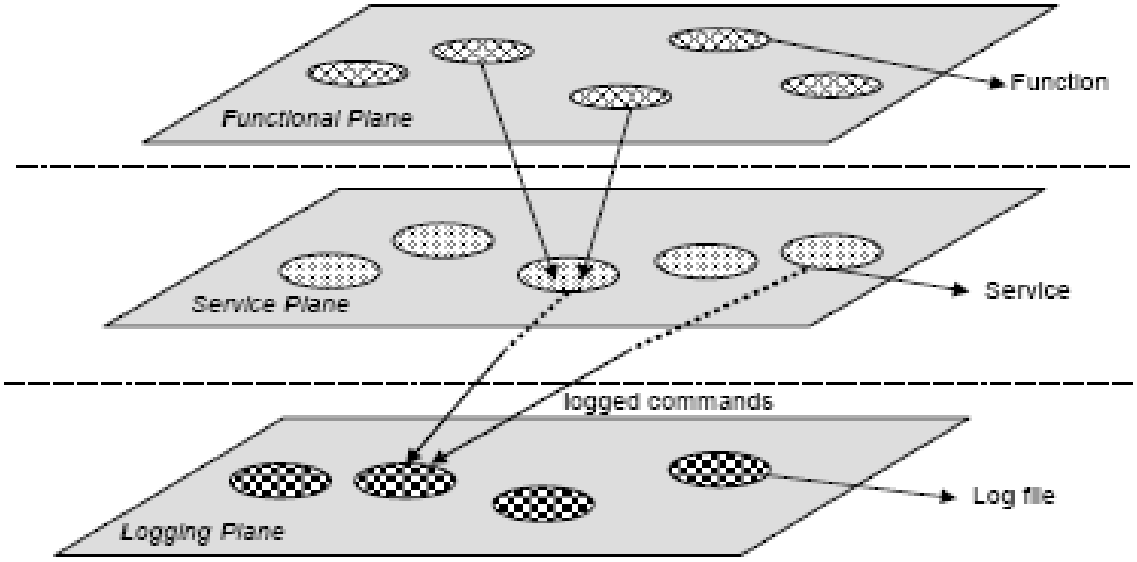


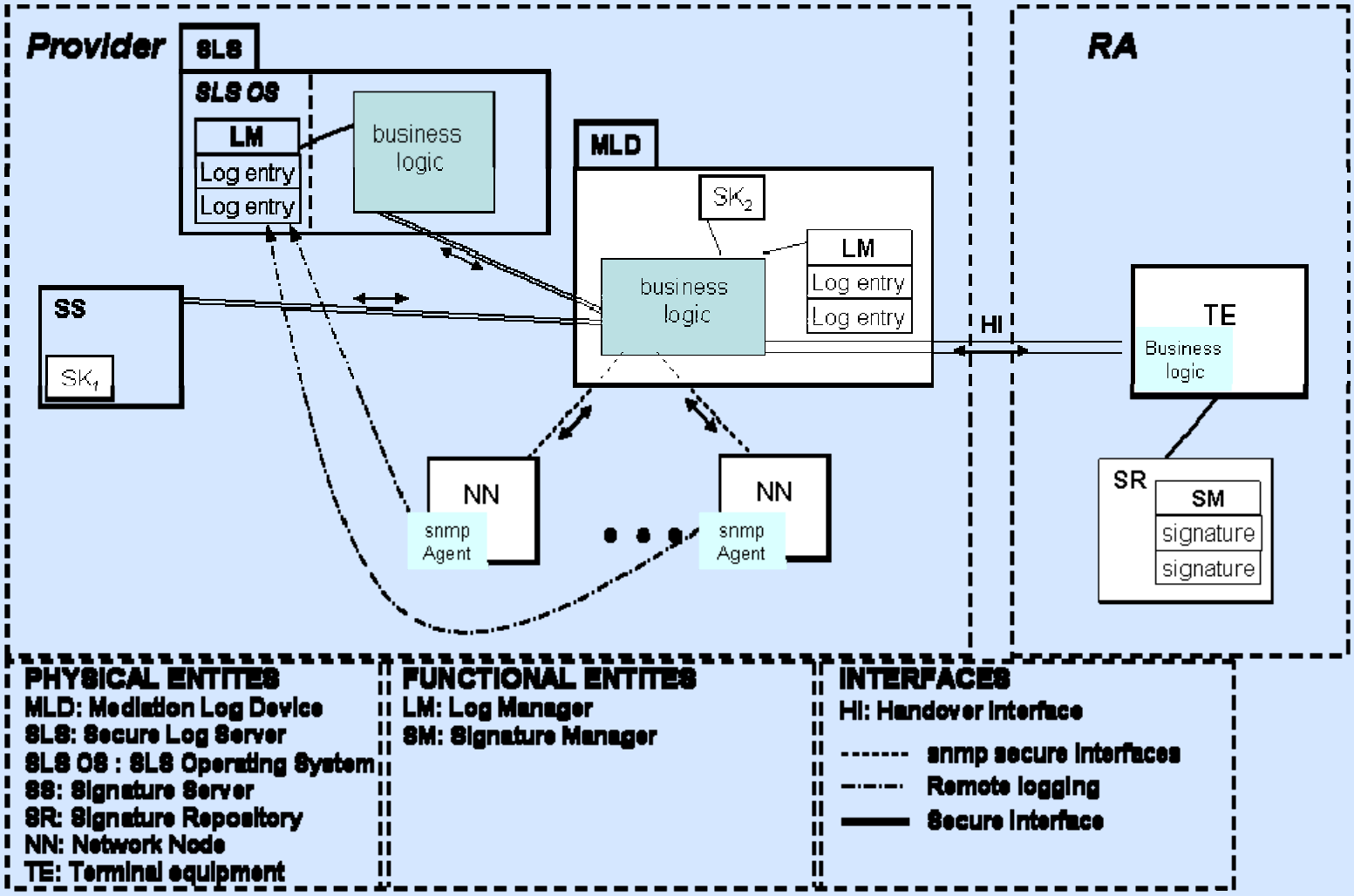
Fig. 1. An abstract representation of a Log Reference Model

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”, accepted for publication 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



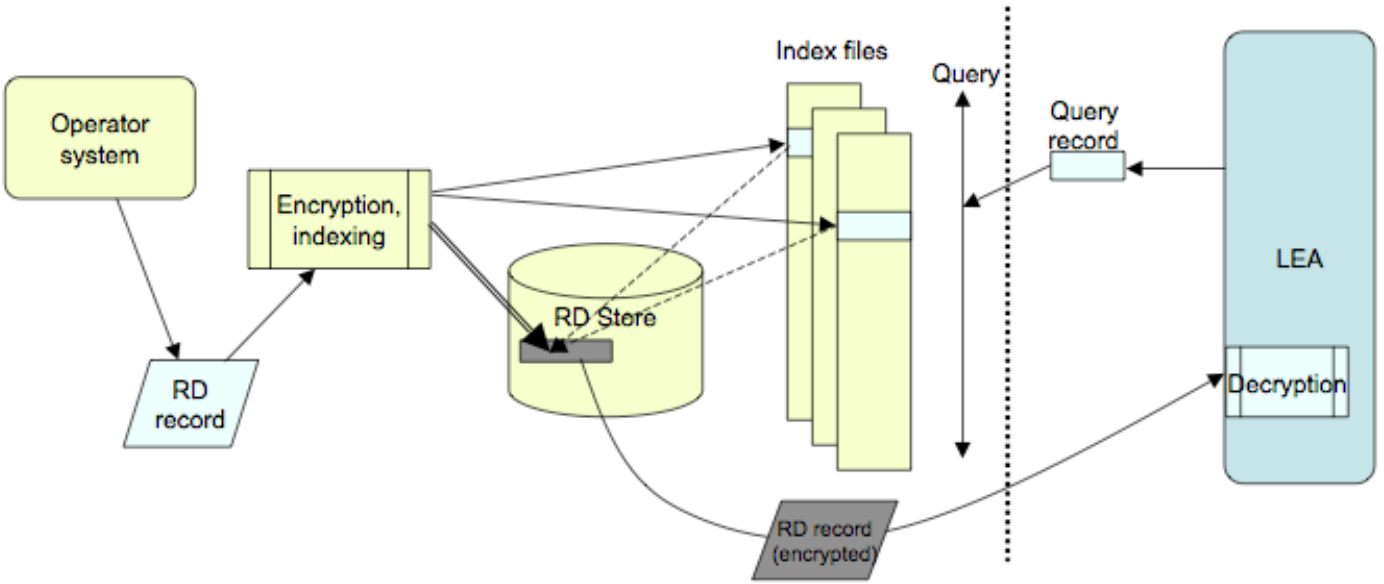
Annex C

ΕΛΛΗΝΙΚΗ ΔΗΜΟΚΡΑΤΙΑ
ΑΡΧΗ ΔΙΑΣΦΑΛΙΣΗΣ ΤΟΥ ΑΠΟΡΡΗΤΟΥ ΤΩΝ ΕΠΙΚΟΙΝΩΝΙΩΝ

- **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

Ερωτήσεις