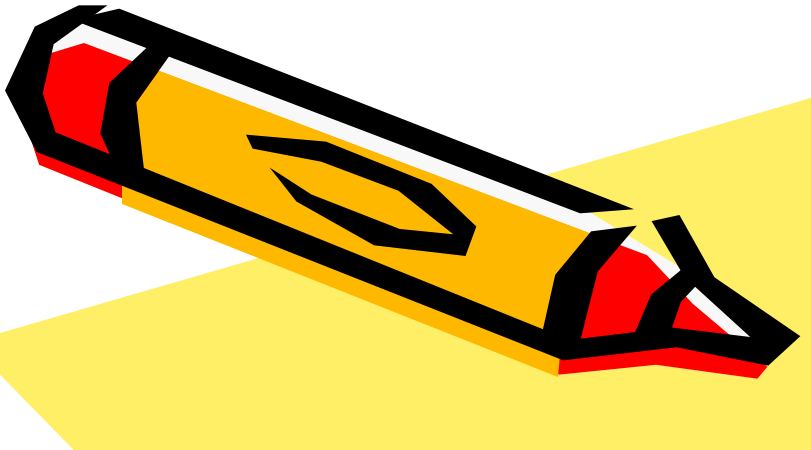


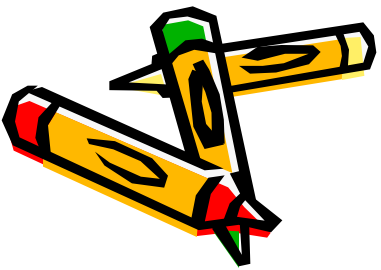
Data Retention Requirements

ETSI TC-LI

Content

- The use of RD
- History in the EU
- The requirements

Koen Jaspers
Ministry of Justice
Netherlands



Why do we need Retained Data

- Retained data is one (the) of the three pillars of crime investigation:
  - Witness
  - Forensics
  - Telecom
- Objective
  - Trace
  - Links, social network
  - Evidence

Why do we "Standardise"

- Strong development of telecommunications
  - One fixed Telephony provider, (cost, availability, personal)
  - Multiple services, multiple access, mobile, flat fee, personal
- Continuous increase in the:
  - Use of the telecommunication,
  - Number of different services used
  - Number of different access networks used

Why do we "Standardise"

- Retained Data increases in;
  - Quantity
  - Complexity
- Avoid manual processing,
  - Quantity, process time, interpretation, mistakes
  - Automation
- Automation requires:
  - Standardised formats
  - Standardised interfaces

EU Retained Data History before directives

- Retention for provider purposes
  - Use of data: Billing, Fraud, Marketing, Quality & Performance
  - Set of data: provider issue
- Retention period from "not" to decades
  - Mobile telephony: "permanent" retention,
  - Free or flat Fee: O&M temporary retention
- Access to Retained Data, provider issue

EU Retained Data History Privacy Directive

- 2002 EU adopts Telecom Privacy Directive
- 2004 it must be implemented
- Retention only for particular provider purposes
- Period limited to primary business purposes
  - Billing period, Complain period
  - Deleted or made anonymous
- Exceptions in National Regulation possible for:
  - Law Enforcement
  - State Security

EU Retained Data History Data Retention Directive

- March 2006 EU Data Retention Directive
- Reaction on the Privacy Directive 2002 (2004)
- 18 months to implement -> September 2007
- Harmonisation of Retained Data for international (EU) exchange
- 3rd pillar informative treaty to 1st pillar mandatory directive!
- Period 6 to 24 months
- Mandatory minimum set
- National extensions

ETSI and Retained data

- ETSI TC-LI basis Interception
- early industry initiative DR-WI
  - Standardisation items and format
  - No stage 1
- DRD triggers new DR-WI
  - Broader support
  - Requirements TS 102 656
  - RDHI

Retained Data Requirements

- Requirements TS 102 656 based on:
  - Mandatory set according to EU directive.
  - Extended data set according to ETSI.
  - National options and extensions to data sets
  - Generic issues bases on TS 101 331
- General requirements
  - Subscriber data
  - Subscriber related traffic data

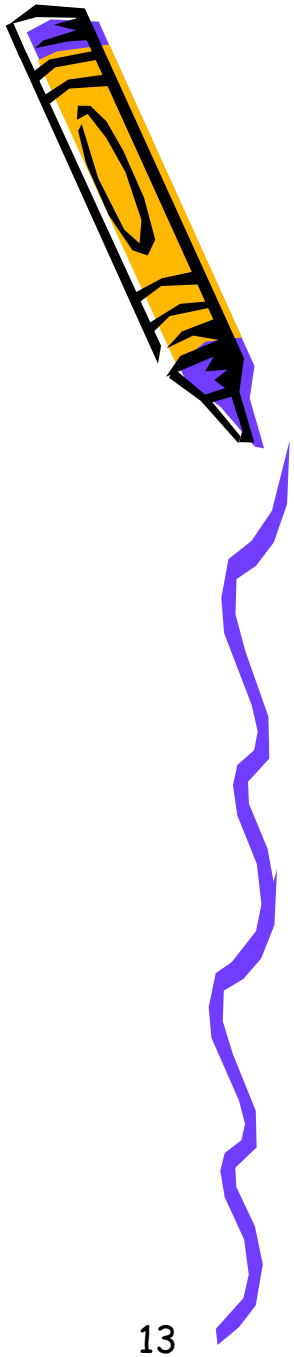
DR Requirements Requests

- Requests
  - Traffic data / Subscriber data
  - Request Criteria
  - Straight forward (no data mining or subjective decisions)
  - Lawful Authorisation (can combine more requests)
- Request for retained data
  - Subscriber data
    - Timestamp, time window
    - Service or network identifier, name, address
  - Communication data
    - Timestamp, time window
    - Number (source, destination, intermediate)
    - Location (e.g. base station)

DR Requirements Delivery

- Delivery
  - Complete
  - Auditable
- Content of delivery
  - Source/destination ID (service, equipment, network, name/address)
  - Communication start/end, type/service
  - Equipment ID
  - Location (e.g. base station for mobile)
  - Status/service changes

Retained Data Requirements



- Location information
  - Communication, Attempt, Service based
- Availability constraints
  - Without undue delay
- Information transmission and information protection requirements
  - Access, Staff, Requests, Handover, Authorisation, Authentication, Confidentiality, misuse logging, tamperproof
- Internal security

Retained Data Requirements

- Technical handover interfaces and format requirements
  - Open format, QoS, Correlation R&A, unique on HI, fault reporting, open architecture
- Temporary obstacles to transmission
- Identification of the request criteria
- Multiple requests
  - Multiple requests, HI handling, mutual confidentiality, different lawful authorisations, concurrent handling.
- Non discosure
  - Implementations, unauthoirized personel, co-operation between providers (e.g. access & service), CSP/manufacturers/3rd parties