



**Future Security Workshop:  
the threats, risks and opportunities**

**ETSI**

**Sophia Antipolis, France**

**16-17 Jan 2006**

# NGN Network Security Forensics and the Data Retention Directive



Anthony M Rutkowski

Vice President for Regulatory Affairs and Standards

Dulles VA USA

tel: +1 703.948.4305

mailto:trutkowski@verisign.com

Where it all comes together:

# Summary

---

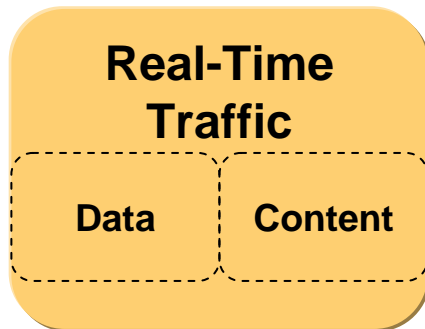
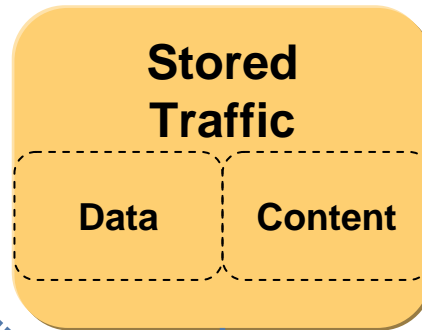
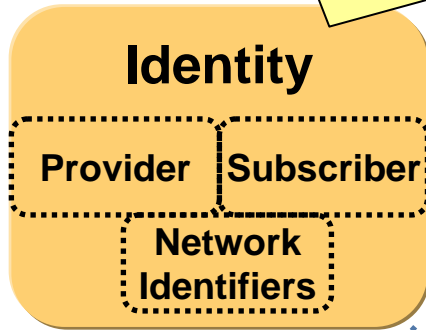
- + NGN Public Network Security Forensics
  - Forensic components
  - Forensic requirements
- + The Data Retention Directive
  - Relationship to forensics
  - Directive requirements
- + Needed standards-based capabilities and related activities
  - Authoritative global provider identification and directory interoperability
  - Authoritative global user/subscriber identification and directory interoperability
  - Common architecture and protocol for request and delivery of stored data
  - Ancillary support: authentication, authenticated timestamps, extensibility and localisation mechanisms
- + Directive provisions: significant implementation choices
- + Possible gaps and future work items
  - Common provider identification, resolver, and directory standards in Europe
  - Common user/subscriber/object identification, resolver, and directory standards in Europe
  - Common stored data handover standards in Europe

---

# NGN Public Network Security Forensics

# The network forensics Rosetta Stone

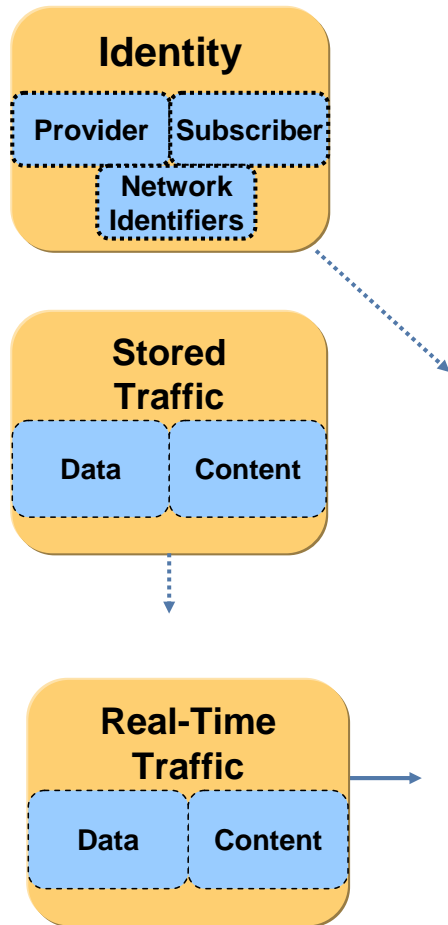
*Additionally necessary for a broad array of operational, public interest and commercial needs*



**Necessary for**

- + **Law Enforcement**
- + **Homeland Security**
- + **Infrastructure Protection**
- + **Network Management**

# Public network forensic components



## + Identity

- Ability to authoritatively identify the service provider, obtain contact information and get to authoritative user/subscriber/object directories and network identifier bindings
- Key requirements established by law and regulation; and may be maintained in part by government agencies

## + Stored Traffic

- Any information generated by network processes that is relevant to a user/subscriber/object communication and has significant latency (i.e., is not real-time)
- Requirements and access controlled by law and regulation, and may include ad hoc requests (e.g., subpoena), preservation orders, and general data retention

## + Real-time Traffic

- Any information generated by network processes that is obtained in real-time
- Requirements and access controlled by law and regulation (lawful interception capabilities and execution of orders)

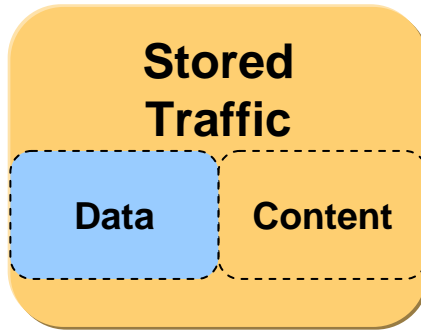
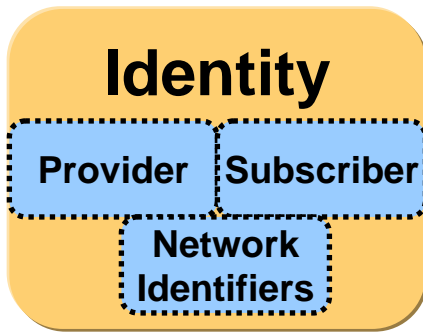
## + Analysis

- Network Operations, Administration, and Maintenance
- Fraud detection and prevention
- Infrastructure protection
- Law enforcement, public safety, and national security needs

---

# The Data Retention Directive

# EU Data Retention Directive



- + Harmonizes data retention and access across Europe
- + Applies to
  - Fixed network telephony
  - Mobile telephony
  - Internet access, messaging and telephony
- + Provides data necessary to
  - trace and identify the source of a communication
  - trace and identify the destination of a communication
  - identify the date, time and duration of a communication
  - identify the type of communication
  - identify the communication device or purported device
  - identify the location of mobile communication equipment
- + Does not include content
- + Includes privacy enhancement features
- + Adopted by European Parliament on 14 Dec 2005
- + Likely to be the subject of considerable implementation collaboration activities in 2006-2007

# EU Directive: communication record data elements (Art. 4)

For each of these communications

| Type                               | Source                     | Fixed Telephone                     | Mobile Telephony                          | Internet Access                         | Messaging                               | Internet Telephony                                  |
|------------------------------------|----------------------------|-------------------------------------|-------------------------------------------|-----------------------------------------|-----------------------------------------|-----------------------------------------------------|
| <b>calling party identifiers</b>   | Traffic data               | calling telephone number            | calling telephone number                  | calling user ID(s)/IP address allocated | calling user ID(s)/IP address allocated | calling user ID(s)/IP address allocated             |
| <b>calling party VoIP gateways</b> | Traffic data               |                                     |                                           |                                         |                                         | calling user ID and allocated PSTN telephone number |
| <b>calling party identity</b>      | Directory                  | calling subscriber name and address | calling subscriber name and address       | calling subscriber name and address     | calling subscriber name and address     | calling subscriber name and address                 |
| <b>called party identifiers</b>    | Traffic data               | called/forwarded telephone number   | called/forwarded telephone number         | called user ID(s)/IP address allocated  | called user ID(s)/IP address allocated  | called user ID(s)/IP address allocated              |
| <b>called party VoIP gateways</b>  | Traffic data               |                                     |                                           |                                         |                                         | Called user ID and allocated PSTN telephone number  |
| <b>called party identity</b>       | Directory                  | called subscriber name and address  | called subscriber name and address        | called subscriber name and address      | called subscriber name and address      | called subscriber name and address                  |
| <b>event timestamps</b>            | Traffic data               | start/stop of communication         | start/stop of communication               | login/logout of communication           | login/logout of service                 | login/logout of service                             |
| <b>services</b>                    | Traffic data               | Service type                        | Service type                              |                                         | Service type                            | Service type                                        |
| <b>equipment identifiers</b>       | Traffic data/<br>Directory | called/calling equipment identity   | called/calling equipment IMSI/IMEI        | end point identifier                    |                                         |                                                     |
| <b>prepaid time and location</b>   | Traffic data/<br>Directory |                                     | prepaid activation timestamp and cellsite |                                         |                                         |                                                     |
| <b>mobile location</b>             | Traffic data/<br>Directory |                                     | Start location                            | Start location                          |                                         |                                                     |

# Directive: additional details

- + **Scope (Art. 1)**
  - harmonise the provisions of the Member States concerning obligations on the providers of publicly available electronic communications services or of a public communications network
  - applies to traffic and location data of both private and legal persons, as well as the related data necessary to identify the subscriber or registered user
- + **Obligation (Arts. 3, 13)**
  - Member States shall adopt measures to ensure that the data specified...to the extent it is generated or processed by providers of publicly available electronic communications services or of a public communications network within their jurisdiction in the process of supplying the communication services concerned
  - Member States shall bring into force the laws, regulations and administrative provisions necessary to comply with this Directive by no later than 18 months after its adoption at the latest
  - unsuccessful call attempts where that data is generated or processed, and stored
- + **Access Process (Art. 3a)**
  - The process to be followed and the conditions to be fulfilled in order to get access to retained data in accordance...shall be defined by each Member State in national law, subject to relevant provisions of Union law
- + **Periods (Arts. 7, 11a)**
  - not less than 6 months and for a maximum of two years from the date of the communication
  - Individual States may petition for extensions to maximum retention period
- + **Security (Art. 7a)**
  - retained data shall be of the same quality and shall be subject to the same security and protection as those data on the network
  - the data shall be subject to appropriate technical and organisational measures to protect the data against accidental or unlawful destruction, or accidental loss or alteration, unauthorised or unlawful storage, processing, access or disclosure
  - the data shall be subject to appropriate technical and organisational measures to ensure that access to the data is undertaken only by specially authorised personnel; and
  - the data shall be destroyed at the end of the period for retention except those data which have been accessed and preserved
- + **Availability (Art. 8)**
  - the data retained and any other necessary information related to such data can be transmitted upon request to the competent authorities without undue delay
- + **Statistics and Evaluation (Arts. 9, 12)**
  - Usage provided annually to the European Commission
  - Re-evaluation of requirements at 3 year intervals

⊛

# Needed standards-based capabilities and related activities

# Major Directive implementation choices

- + How to efficiently obtain, store, and make available remote called/calling party identification, equipment, and gateway information
  - How to reconcile Art. 4 remote party directory information obligation with the Art. 3 “generated or processed...within [Member] jurisdiction” limitation? Is roaming included?
  - For a domestic provider: Is there an implied obligation to facilitate remote directory information? To authenticate remote identities? To block anonymous communication?
  - For a foreign provider: If interconnected with national network, are they within the Member’s jurisdiction?
- + Does Art. 2 user definition include objects and their communication?
- + Are common European-wide standards essential for effective implementation of the Directive provisions?
  - Does Art. 8 availability to competent authority requirement imply common standards
- + Are encryption and authentication essential for data integrity?

# Needed standards-based capabilities and related activities

---

- + Authoritative global provider identification
  - Registration and discovery of authoritative information sources (possibly ITU-T M.1400 plus resolver mechanism)
  - Directory interoperability (standard(s) do not exist)
- + Authoritative global user/subscriber/object identification
  - Discovery of authoritative information sources (standard(s) do not exist)
  - Directory interoperability (ITU-T E.115v2, IRISv2, Open LDAP)
- + Retained traffic data
  - Common architecture and protocol for request and delivery (ETSI SDHA)
  - Art. 4 schema development, registration, publication (standard(s) do not exist)
- + Ancillary support
  - Art. 7a data integrity
  - Art. 7a authentication
    - Authenticated timestamps
  - Art. 9 statistics generation



# Possible gaps and future work items

# Possible gaps and future work items

- + Ways to turn *Directive* and other forensic implementation capabilities into service opportunities
  - Fraud management
  - Presence and availability management
  - Extended roaming and easy “sign-on”
  - Personal and public safety support
  - Authenticated calling name
  - DoNotCall
  - Priority access and enhanced QOS
  - Language and disability support
  - Push services
  - Intercarrier compensation
  
- + Principal security and *Directive* forensic needs
  - Discovery and access to authoritative European provider information
  - Discovery and access to authoritative user/subscriber/object information
  - Stored Data Handover Architecture with discovery and access to authoritative information handover schema
  - Harmonisation of Data Retention Directive provisions