Agenda

- What is ETSI & 3GPP
- Mobile and ETSI LI Standards
- Methodologies
- Challenges & Future Issues
A European standards organization
Active in all areas of ICT
Setting globally-applicable standards for
  • telecommunications
  • radio communications
  • broadcasting
  • related topics
Independent, not-for-profit organization, created in 1988
ISO 9001:2008 certified
Offering direct participation
750+ Member companies and organisations
We have over 30 000 publications - freely available!

http://www.etsi.org
http://portal.etsi.org
About 3GPP

• Formed 1998
• Partnership between
  • ARIB (Japan), ATIS (USA), CCSA (China), ETSI (Europe), TTA (Korea), TTC (Japan)
• Scope
  • Maintenance and development of the Global System for Mobile communication (GSM) Technical
    Specifications and Technical Reports including evolved radio access technologies
• Membership
  • Currently 390 list Member companies Must be a member of one the 6
    organisational partners (eg ETSI)
  • 48000 delegate days in 2011 (rising year on year).

TSG Structure

[Diagram of TSG Structure]
SA3-LI responsible for Lawful Interception within 3GPP
- Mobile Focus
- Standards 33.106 (Stage 1), 33.107 (Stage 2), 33.108 (Stage 3)
- IMS, LTE, VOIP
- Works in conjunction with ETSI, other regional standards group & GSMA.

TC-LI responsible for Lawful Interception within ETSI
- Recognised global expert group for LI and Data Retention.
- Primary Standards 102.232, 101 671.
- Focuses on Handover
- New areas
  - Cloud, Dynamic Triggering, E-Warranty
Basic Tool Set

Regulations.

Lawful Interception

Data Retention & Disclosure
Methodologies – Mobile Basics

- **MSISDN, IMSI, IMEI, IMPU, IMPI**

- **Subscriber Details**
  - Billing & Payment

- **Location**
  - Cell Site
  - E911 Enhanced Location
  - Cell Coverage
    - Macro
    - Pico
    - Cell Type
    - Cell Breathing.

- **Interception**
  - IRI and/or CC

Indirect link between telecoms usage and money.
Methodologies – Lawful Interception

**Partnership between CSPs and Law Enforcement**
- One Size does not fit all.
  - Retail vs Business vs Over the Top Providers.
- Regulatory framework needs to be flexible but respect privacy.
- Costs

**LEAs need to ask the right questions**
- Just because an approach made sense yesterday, doesn’t mean it will tomorrow.
  - Technology Changes

**Cloud and Over the Top Providers**
- Increasingly important
- Location and Identity
- Proportionality
Methodologies – Lawful Interception

Standards play a key part in this.

- Eg ETSI 102-232, 3GPP 33.108, ATIS 1000678

Standards Benefits

- Real-time delivery
- Correlation, Location, Identities
- Consistency
- Proportionality, with CSP control
- Lower end to end cost and timescales

Design for LI

- Important for governments to get involved in groups such as TC LI and SA3-LI.
- Very expensive and difficult to retrofit LI capabilities.
- Encryption
- Detectability
- Long duration design cycles.
- Privacy – Precise targeting.
Communications Data Retention

- EU Data Retention Directive (DRD) 2006
- CSPs required to retain basic CDR / Customer information.
  - 6 -24 months Retention, Specific legal purposes.
- Equivalents being considered in other states.

Mutual Legal Assistance Treaties (MLATs)

- Global communications don’t respect country boundaries
  - Neither do criminals.

Electronic Warrantry

- Speed and Auditability
- Real vs Digital Signatures.
Future Challenges

Apps & App Stores
- Outside of traditional operator control

Apps changes
- Monthly, weekly, daily

Reduced or Lack of Billing CDRs—eg
- Transaction self-destruction and anti-forensics.
- Lack of verifiable location information.

Identities
- No standards or globally accessible identity plan.
- Trust for evidential purposes?
Future Constant Service Mobility

IMS Service

Mobile CSP A

Other Operator

One common device multiple accesses,
One constant user session
**Future Challenges**

**Cloud**
- No centralisation of infrastructure.
- Where to serve the warrant.

**Over the Top Services.**
- Traditional operator acting as a bit pipe.
- Wifi or fixed access to mobile services.
- Who to serve the warrant on.
  - CSP Maturity & Suitability

**Jurisdiction**
- Location of physical servers / services
- Location of user relative to service provision

**Encryption**

**Traffic Offload & UE to UE Direct Mode.**
- Requires Dynamic Triggering.
Conclusions

Standards play a key roll.
- Ensures basic tools
- Long term activity
- Balanced Privacy vs National Security.

Industry Partnerships

Global Co-operation

Balanced National Security vs Privacy.
Thank You & Questions

Bringing it all together