

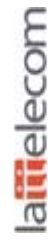


etno

**the leading trade association of
European Telecom Operators**

**Ing. J. Heijblom KPN security and fraud prevention
ETNO fraud control and network security**





ETNO Working Groups

Employment, health & safety

(Laurent Zylberberg, France telecom)

external trade issues

(Tilmann Kupfer, BT)

international telecommunications union

(Dominique Würges, France telecom)

research and development

(Geoff Scott, BT)

sustainability

(Danilo Riva, telecom Italia)

frequency management

(Massimiliano Simoni, telecom Italia)

naming, addressing and numbering

(Christina Kelaidi, OTE)

Fraud control and network security ←←←

FC&NS

(Luis Sousa Cardoso, Portugal telecom)

data protection and information security

(Cristina vela, Telefonica)

Joint task force on security issues

European Information Society

(Pablo Pfof, Telefonica)

Internet Governance

(Konstantin Kladouras, OTE)

eInclusion and Digital Divide Task Force

(Henk Mannekens, BT / Paula Sunjic, Croatian Telecom)

Benchmarking

(Jacques Tamisier, France Telecom)

Content issues

(Neil Gibbs, BT)

Regulatory Policy

(Ralf Nigge, Deutsche Telekom)

Regulatory Economics Task Force

(Paul Richards, BT)

Tax issues

(Dave Taylor, BT)

Communications

Security functions & providers (1/2)

Provider industry from telecom operator to.... telecom service provider

- 1. Original applications / networks (telecom) well standardized...
- 2. Co-operation (interconnection) requires industry standards too...
- 3. Now many new providers of which many just buy in... and sell...

New communication services offering issues...

- 1. Service development: follow (short) end equipment Life Time (LT).
- 2. End equipment and software Life Time: limited to... 1-3 years.
- 3. New application networks: standards not stable... (e.g. WiFi).
- 4. Terminal software and applications: change- patching rate... high.
- 5. Security functions: usually not (yet) considered as a selling point.
- 6. Cost limitation requirements: so limit not direct cost (=overhead).
- 7. Competition pressure, cost limitation and short implementation time: does leave little effort for security functions.

Security functions & providers (2/2)

Examples:

Response on a Criminal or Abuse Incident ?

Often a criminal response effort is considered as not to be justified !

- Choices for response: limit damage, repair and-OR investigate & report.

Provider co-operation: security info considered sensitive information !

- So, information sharing requires earned trust.
- Info-sharing is often experienced risky and as not being allowed.

ETNO FC&NS working group.

- Has (still) a telecom focus, a fraud focus and operational view.
- Specialist (security) participation: maintain / changes fast too.
- Group supportive to information sharing, best practices, standards.
- Subjects dynamic follow user demand and new technologies.

Coverage IP / CIP

ETNO FC&NS coverage: statements and common position.

- 1. Based on the ARECI study (version January-2007).
- 2. Workgroup recognizes the need for CIP in general.
- 3. (Re-) Actions for CIP needs specialist resources.

- 4. Company requires efficiency contribution to make CIP-measures
- 5. Criteria needed for EU CI to prevent an over-inclusive approach.
- 6. ARECI suggestions: many of them are already ongoing business.

Currently used standards:

- ITU T standards and practice guidelines are the common reference.
- ITU has developed a security standard for service providers.
- IETF guidelines are increasingly used.

Responses on ARECI (see CP079) 1/2

Public offered Network Services (P.N.S.).

- 1. PNS Optimised for a general public and big scale usage.
- 2. Customer wishes: rel. easy to use and relative affordable to use.
- 3. Equipment: Standarized and a minimum quantities need.
- 4. Design and sizing based on (normal statistical) usage patterns.
- 5. Support for special service access (for emergency reporting).
- 6. PNS has service limitations (and increasing dependability).

User groups and network functions determine “their wish list”.

- Trend is: Open multi functional network and more complex CPE.
- Applications are in CPE and Server sites... with little registrations...
- Main security functions in the CPE (Customer Premises Equipment).
- Usage mobility: via heterogeneous and interconnected networks.

Responses on ARECI (see CP079) 2/2

- 01 –Emergency Preparedness – positive.
- 02 –Priority Communications on P.N. – positive. Follow ITU Recommendations.
- 03 –Formal Mutual Aid – positive. Practical issues to solve.
- 04 –Critical Infrastructure Info-Sharing – positive. Is common practice through formalized groups (e.g. ETNO and other fora). LE and Regulator input experienced improvable.
- 05 –Inter-Infrastructure Dependency – positive. National approach must be the starting point.
- 06 –Supply Chain Integrity and Trusted Operation clean networks. -positive
- 07 –Unified European Voice in Standards - ETNO Members are not in agreement. Common standards are often adopted should remain an industry-lead activity.
- 08 –Interoperability Testing - a level playing field.- very positive New standards on interoperability testing being developed by ITU.
- 09 –Vigorous Ownership of Partnering Health – positive, especially if support of nationally with an equal division of efforts.
- 10–Discretionary European Expert Best Practices harnessing expertise. – positive is practice among ETNO Members.
- ETNO Members reaffirm their position to support, maintain and improve co-operation and collaboration with EU programmes to develop a possible common approach.
- ETNO Members have already adopted the common practice to prepare business continuity plans (BCP's).
- They are working in a sector possessing recognised security/safety obligations, proportionality checks needed for new ones.

Remarks and Advices

- Future development are expected to have an IP-based network...
- The current DNS concept is considered susceptible for attacks...
- Increasing regulatory overhead muffles new developments...
- Service chains require basic security in every chain (provider)...
- Provider security contact may be effective with an authorization...
- Security contact could motivate if it adds recognised value back...
- Advice to leave standards to be an industry sector effort...
- Non-sector standard organisation is expected to increase confusion...
- Assessments: finding risks, -dependencies needs user action too...
- Some dependencies can not be solved without end-user action...

Questions ?

- Thank You.