ETSI Security Standardisation

Dr. Carmine Rizzo

CISA, CISM, CISSP, ITIL, PRINCE2

ETSI Technical Officer – ETSI Standardisation Projects
ETSI Security Standardisation

carmine.rizzo@etsi.org

Agenda

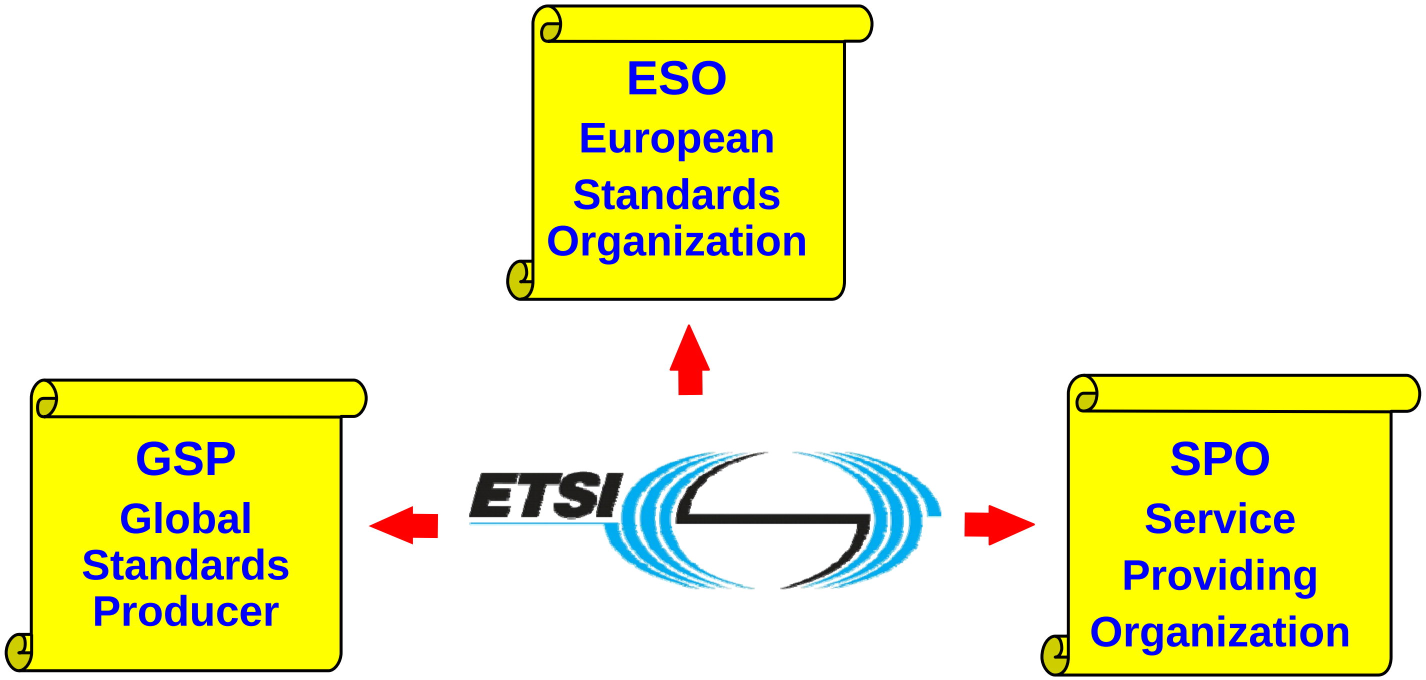
- ❑ Introduction
- ❑ ETSI Security activities in Technical Bodies
- ❑ ETSI Security horizontal activities

- ❑ Introduction

- ❑ ETSI Security activities in Technical Bodies

- ❑ ETSI Security horizontal activities

The three roles of ETSI



ESO
European
Standards
Organization

GSP
Global
Standards
Producer

SPO
Service
Providing
Organization

ESO (European Standards Organization): standardization for European needs
GSP (Global Standards Producer): standardization for the global level
SPO (Service Providing Organization): services such as interoperability testing, forum management etc.

The role of Security Standards

- ❑ Information Security Standards are essential to ensure <u>interoperability</u>

- ❑ Standardisation ensures products are compliant with
  - ➢ Adequate levels of security
  - ➢ Legislations

- ❑ ETSI 1988-2009: over 20 years of experience in Security

- ❑ All ETSI Members participate directly in the standardisation process

- ❑ Introduction
- ❑ **ETSI Security activities in Technical Bodies**
- ❑ ETSI Security horizontal activities

Areas of security standardisation

- ❑ Next Generation Networks (NGN)
- ❑ Mobile/Wireless Communications (GSM/UMTS, TETRA, DECT…)
- ❑ Lawful Interception and Data Retention
- ❑ Electronic Signatures
- ❑ Smart Cards
- ❑ Algorithms
- ❑ Emergency Communications / Public Safety
- ❑ RFID
- ❑ Quantum Key Distribution (QKD)
- ❑ In 3GPP: SAE/LTE and Common IMS

NGN Security standardisation

- ❑ ETSI TISPAN WG7 standardizes NGN security

- ❑ Achievements
  - ➢ Security Requirements, Design Guide, Architecture
  - ➢ Analysis of risks and threats

- ❑ Current work
  - ➢ Lawful Interception / Data Retention
  - ➢ IPTV, RFID, safety services (emergency communications)

TISPAN:

Telecommunication and Internet converged Services and Protocols for Advanced Networking

GSM/UMTS

- ❑ Security Standardisation: key success factor for GSM
- ❑ IMEI (International Mobile Equipment Identity)
  - ➢ Protection/deterrent against theft
- ❑ FIGS (Fraud Information Gathering System)
  - ➢ Terminate fraudulent calls of roaming subscribers
- ❑ Safety Services (enhancements for UMTS)
  - ➢ Priority access for specific user categories
  - ➢ Location services

TETRA

- ❑ TErrestrial Trunked RAdio
- ❑ Mobile radio communications
  - ➢ Used for public safety services (e.g. emergency scenarios)
- ❑ Security features
  - ➢ Mutual Authentication
  - ➢ Encryption
  - ➢ Anonymity

Lawful Interception

- ❑ **Delivery of intercepted communications to Authorised Organisations**
  - ➢ To support criminal investigation, counter terrorism
  - ➢ Applies to data in transit

Data Retention

- ❑ **Directive 2006/24/EC**
  - ➢ Data generated/processed in electronic comms needs to be retained
  - ➢ Applies to data location

- ❑ **ETSI Data Retention standard published in 2008**

TB Lawful Interception (LI) works with both LI and DR

- Define Handover Interface from Operator to Authorised Organisation

Electronic Signatures

- ❑ TB ESI (Electronic Signatures and Infrastructures)
  - ➢ Supports eSignature EC Directive – in cooperation with CEN
  - ➢ Created ETSI electronic signatures
  - ➢ Successful international collaboration (US, Japan)

- ❑ Current work
  - ➢ Digital accounting (eInvoicing)
  - ➢ Registered EMail (REM) framework
  - ➢ ETSI electronic signatures in PDF documents

Smart Cards

- ETSI Smart Card Standardisation
  - TB Smart Card Platform (SCP)
  - GSM SIM Cards: among most widely deployed smart cards ever
  - Work extended with USIM Card and UICC Platform

- Current work
  - Further extend the smart card and UICC platforms
    - Global roaming
    - Secure financial transactions
    - Operate in M2M communications

USIM: UMTS Subscriber Identity Module
UICC: Universal Integrated Circuit Card
M2M: Machine-to-Machine

Algorithms

- ❑ **ETSI is world leader in creating cryptographic algorithms / protocols**
  - ➢ **ETSI SAGE (Security Algorithm Group of Experts)**
  - ➢ **ETSI is *owner and/or custodian* of a number of security algorithms**
- ❑ **Algorithms for GSM, GPRS, EDGE, UMTS, TETRA, DECT, 3GPP …**
- ❑ **Developed**
  - ➢ **UEA1 (standard algorithm for confidentiality)**
  - ➢ **UIA1 (standard algorithm for integrity)**
- ❑ **Developed also a second set of algorithms**
  - ➢ **UEA2 and UIA2, fundamentally different in nature from UEA1 and UIA1**
  - ➢ **Advances in cryptanalysis are unlikely to impact both sets of algorithm**

UEA: U̲MTS E̲ncryption A̲lgorithm
UIA: U̲MTS I̲ntegrity A̲lgorithm

Emergency Communications / Public Safety

- ❑ **EMTEL (ETSI Special Committee on Emergency Telecommunications)**
  - ➢ **Co-operation with other TBs and partnership projects, including 3GPP**
  - ➢ **Requirements for telecommunications infrastructure**

- ❑ **MESA (Mobility for Emergency and Safety Applications)**
  - ➢ **Partnership project: ETSI, TIA (USA), other members globally**
  - ➢ **Define digital mobile broadband “system of systems” (interoperability is key!)**

GSM ongoing work (public safety)

- GSM onboard aircrafts
  - Prevent undesired communications
    - Between terrestrial networks and handheld terminals on aircrafts!
- GSM eCalls
  - Automatic emergency calls from vehicles
    - In case of crash or other catastrophic events
- GSM Direct Mode Operations (DMO)
  - Terminals to communicate directly
    - In tunnels (e.g. railways) or breakdown of telecomms network infrastructure

SAE/LTE and Common IMS (in 3GPP)

- ❑ System Architecture Evolution / Long Term Evolution (SAE/LTE)
  - ➢ Deliver Global Mobile Broadband at increased data throughput
  - ➢ Security features: integrity and confidentiality
    - Developed in 3GPP and ETSI SAGE

- ❑ Common IP Multimedia Subsystem (IMS)
  - ➢ Architectural framework to deliver IP multimedia to mobile users
  - ➢ Security requirements from TISPAN, CableLabs and 3GPP2

RFID

- ❑ **RFID Security and Privacy by design**
  - ➢ **In TISPAN WG7 to act on EC Mandate December 2008 (M 436)**
    - **RFID as gateway for the future “Internet of Things” (IoT)**

- ❑ **More RFID work in other TBs**
  - ➢ **Intelligent Transport Systems (ITS)**

Quantum Key Distribution

- ❑ New ETSI Industry Specification Group (ISG)
  - ➢ Create an environment for quantum cryptography in ICT networks
  - ➢ Security Assurance Requirements
    - Requirements for users, components, applications
    - Security certification of quantum cryptographic equipment

- ❑ Introduction
- ❑ ETSI Security activities in Technical Bodies
- ❑ **ETSI Security horizontal activities**

OCG Security

- ❑ **Operational Co-ordination ad hoc Group on Security (OCG Sec)**
  - ➢ Chairman: Charles Brookson
  - ➢ Technical Officer: Carmine Rizzo

- ❑ **Horizontal co-ordination structure for security issues**
  - ➢ Ensure new work is addressed by proper TB
  - ➢ Detect any conflicting or duplicate work

Future Challenges

- ❑ **ETSI to address open issues on security**
  - ➢ Prioritization in security standardisation
  - ➢ Security Metrics
  - ➢ Privacy
  - ➢ How to “evaluate” security standards in implementation
  - ➢ …

- ❑ **ETSI is ready to address these challenges**
  - ➢ Proactively supporting its Members according to requirements and trends
  - ➢ Proactively promoting security standardisation
  - ➢ In collaboration with other SDOs

ETSI Security Workshop

- ❑ Yearly event hosted at ETSI premises, Sophia Antipolis, France

- ❑ Security standardisation keeps evolving
  - ➢ New threats arising

- ❑ ETSI needs feedback to:
  - ➢ Ensure timely standardisation on gaps or hot topics
  - ➢ Initiate new work according to the requirements of ETSI Membership

- ❑ Next, to be confirmed
  - ➢ 5th ETSI Security Workshop 2010 (possibly 19-21 January)
  - ➢ Watch for the Call for Papers

- ❑ www.etsi.org/SECURITYWORKSHOP
  - ➢ Reports and presentations of all ETSI Security Workshops

ETSI Security White Paper

- ❑ ETSI achievements and current work in all security areas
- ❑ List of all security-related ETSI publications
- ❑ Edition No. 2 published in October 2008
  - ➢ Carmine Rizzo (ETSI Security point of reference)
  - ➢ Charles Brookson (Chairman of ETSI OCG Security)
- ❑ www.etsi.org/WebSite/document/Technologies/ETSI-WP1_Security_Edition2.pdf
- ❑ Freely downloadable

Thanks!

Available for your ?

carmine.rizzo@etsi.org