

3GPP and ETSI Security Standards

Charles Brookson, ETSI OCG Security Chairman
Carmine Rizzo, ETSI Technical Officer
Dionisio Zumerle, 3GPP Technical Officer

© ETSI 2010. All rights reserved



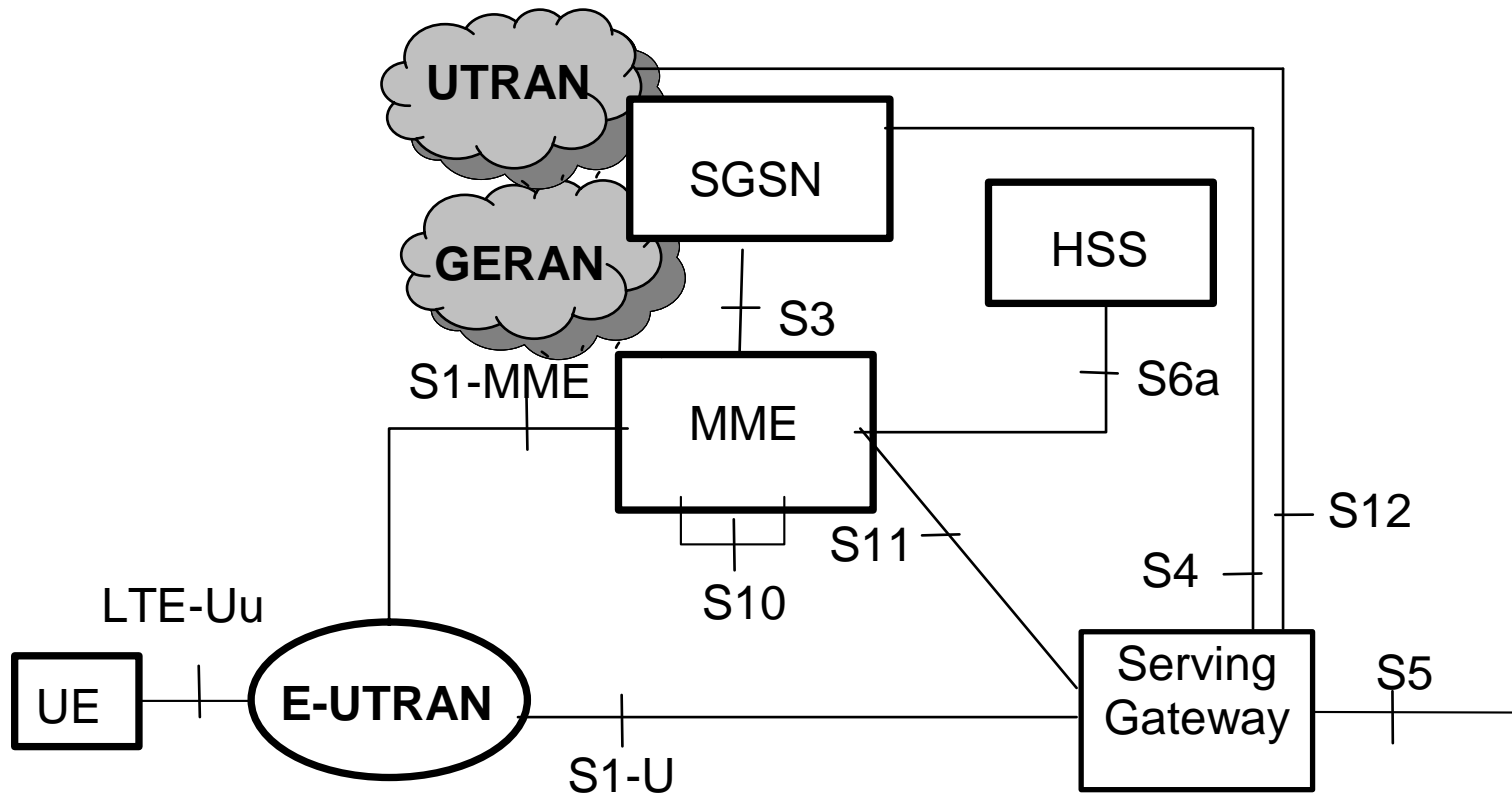
3GPP and ETSI Security Standards

- ❑ **3GPP Mobile security:**
 - **GSM, UMTS, LTE**
- ❑ **ETSI in other Security areas:**
 - **Next Generation Networks (TISPAN)**
 - **TETRA**
 - **Lawful Interception and Data Retention**
 - **Electronic Signatures**
 - **Smart Cards**
 - **Emergency Communications / Public Safety**
 - **RFID**
 - **Quantum Key Distribution (QKD)**

3GPP Mobile Security: EPS and Home (e) Node B Security



LTE™: the EPS Architecture



EPS implications on security

- ❑ Security implications due to
 - *Flat architecture*: radio protocols terminate in access network (eNB)
 - Interworking with legacy and non-3GPP networks
 - Allowing e Node B (eNB) placement in untrusted locations
 - New business environments with less trusted networks involved
 - Trying to keep security breaches as local as possible



- ❑ Extended AKA (Authentication and Key Agreement)
- ❑ More complex key hierarchy
- ❑ More complex interworking security
- ❑ Additional security for eNB (compared to NB/BTS/RNC)

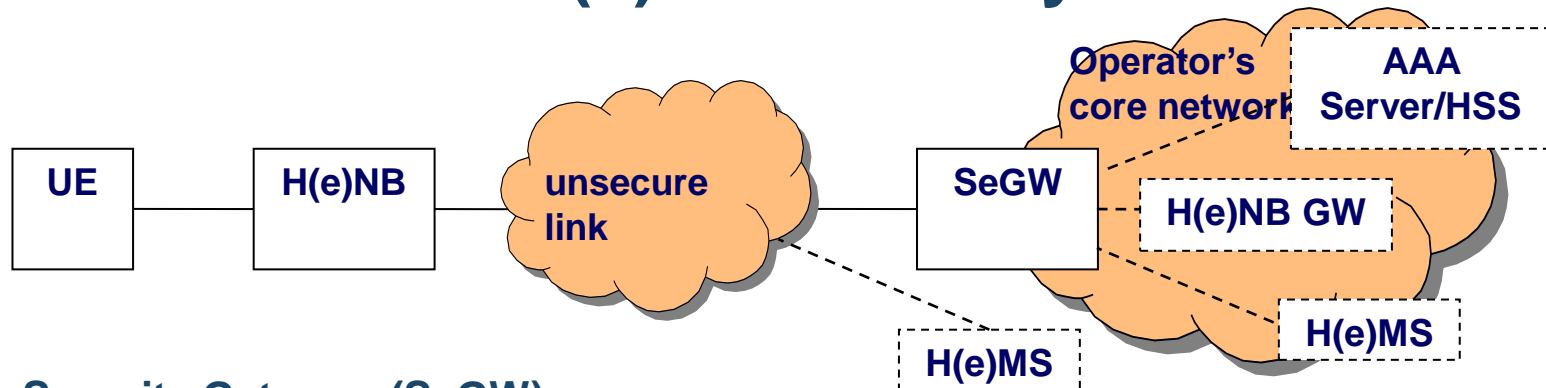
Security functions

- ❑ **Authentication and key agreement**
 - UMTS AKA re-used for SAE
 - SIM usage is explicitly excluded (USIM R99 onwards allowed)
- ❑ **Signalling protection**
 - For core network (NAS) signalling, integrity and confidentiality protection terminates in MME (Mobility Management Entity)
 - For radio network (RRC) signalling, integrity and confidentiality protection terminates in eNodeB
- ❑ **User plane protection**
 - Encryption terminates in eNodeB
 - Separate protection in on network interfaces
- ❑ **Network domain security (NDS/IP)**
 - used for network internal interfaces

Confidentiality and Integrity Algorithms

- ❑ **Two sets in Release 9:**
 - **128-EEA1 and 128-EIA1 (identical to UEA2 and UIA2 for UMTS)**
 - **128-EEA2 and 128-EIA2 (based on AES)**
 - **AES and SNOW 3G chosen as basis**
 - Principle: should be as different from each other as possible
- ❑ **Third set of algorithms under development for Release 10**
 - **128-EEA3 and 128-EIA3**
 - **Based on ZUC**
- ❑ **Rel-99 USIM is sufficient**
 - **Key length 128 bits**
 - included possibility to use 256-bit keys
 - **Deeper key hierarchy than UMTS**
 - **(one-way) key derivation function needed**
- ❑ **Public and open**
 - **Freely available from ETSI web site and GSMA web sites**

3GPP Home (e)NB Security architecture



- ❑ **Security Gateway (SeGW)**
 - element terminating security association(s) for backhaul link between H(e)NB and core network
- ❑ **H(e)MS – Home (e) NodeB Management System**
 - server that configures and installs SW updates on H(e)NB according to operator's policy
- ❑ **CSG (Closed Subscriber Group)**
 - group permitted to access one or more cells of the PLMN with restricted access
- ❑ **H(e)NB access operator's core network via a Security Gateway (SeGW)**
 - Backhaul between H(e)NB and SeGW may be unsecure
- ❑ **Security tunnel established between H(e)NB and SeGW**
 - to protect information transmitted in backhaul link

Home (e)NB Authentication

Two separate concepts of authentication:

- ❑ **Mutual authentication of H(e)NB and operator (SeGW) (mandatory)**
 - **Certificate based**
 - **Credentials stored in TrE in H(e)NB**
- ❑ **Authentication of hosting party by operator's network (optional)**
 - **EAP-AKA based**
 - **credentials contained in separate Hosting Party Module (HPM) in H(e)NB**
 - **bundled with the device authentication (one step)**
- ❑ **Backhaul link protection**
 - **IPSec, IKEv2, based on H(e)NB/SeGW authentication**

EPS and H(e)NB Security Specifications

EPS (LTE™) security

➤ TS 33.401: Security Architecture for LTE™

- New architecture and environment require enhancements to 3G security
- Radio interface user plane security terminates in base station site
- Cryptographic separation of keys
- Forward/backward security in handovers

➤ TS 33.402: Security aspects of non-3GPP accesses

- Different security mechanisms in many interworking cases with non-3GPP access networks

Home (e)NB security

➤ TR 33.820: Study on Security of Home (e) Node B (informative)

➤ TS 33.320: Security Aspects of Home (e) NodeB (normative)

- Architecture and Certificate-based Device Authentication

Freely available at: www.3gpp.org

Other mobile security work

- ❑ **Security algorithms for GSM, GPRS, EDGE, UMTS, ...**
 - In collaboration with ETSI Security Algorithms Group of Experts
 - ETSI acts as Custodian

- ❑ **GSM Security: key to worldwide success**
 - IMEI (International Mobile Equipment Identity)
 - FIGS (Fraud Information Gathering System)

- ❑ **UMTS Security**
 - Security architecture and mechanisms
 - Safety Services (enhancements for UMTS)
 - Priority access, Location services, ...

- ❑ **GSM for public safety**
 - GSM onboard aircrafts
 - GSM eCalls
 - GSM Direct Mode Operations (DMO)

A dark blue world map is centered in the background of the slide, showing the outlines of continents and oceans.

ETSI Standards in Security

NGN Security

❑ Achievements

- Requirements, Design, Architecture, Analysis of risks and threats

❑ Current work

- Lawful Interception / Data Retention
- IPTV, RFID, safety services (emergency communications)

❑ Work done in ETSI TISPAN

- www.tispan.org



TETRA

❑ TERrestrial Trunked Radio

- Mobile radio communications
- Public safety services (e.g. emergency scenarios)
- Mutual Authentication, Encryption, Anonymity



Lawful Interception (LI) & Data Retention (DR)

- ❑ Delivery of intercepted data in transit (LI) and location (DR)
 - To support criminal investigation, counter terrorism
 - Define Handover Interface from Operator to Authorised Organisation

Electronic Signatures

- Digital accounting, Registered EMail (REM)
- Electronic signatures in PDF documents
- Extended Validation Certificates

Smart Cards

- GSM SIM Cards: among most widely deployed smart cards ever
- Work extended with USIM Card and UICC Platform
- Global roaming, Secure financial transactions, M2M communications



Emergency Communications / Public Safety

- ❑ **EMTEL** (ETSI Special Committee on Emergency Telecommunications)
 - Requirements for telecommunications infrastructure
- ❑ **MESA** (Mobility for Emergency and Safety Application)
 - Define digital mobile broadband

RFID

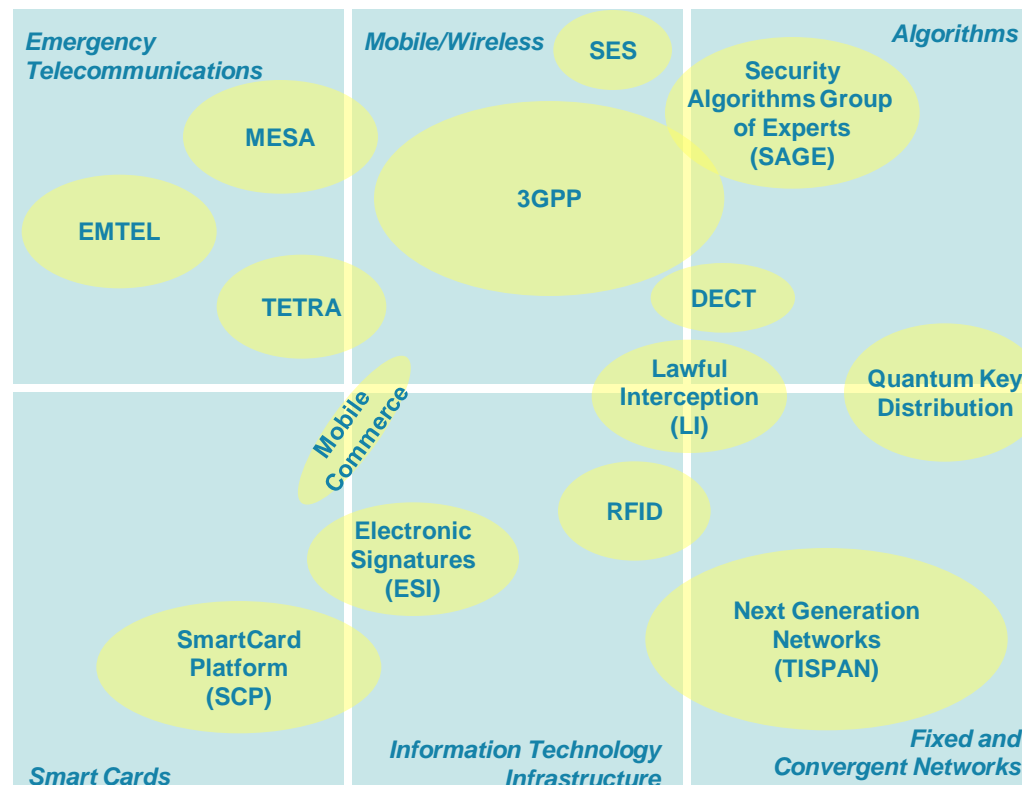
- ❑ **RFID Security and Privacy by design**
 - RFID as gateway for the future “Internet of Things” (IoT)
- ❑ **Intelligent Transport Systems**

Quantum Key Distribution

- ❑ **Quantum Cryptography environment for ICT networks**
- ❑ **Security assurance requirements**

OCG Security

- ❑ Operational Co-ordination ad hoc Group on Security (OCG Sec)
 - Horizontal co-ordination structure for security issues



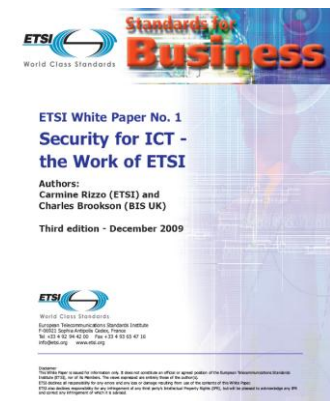
ETSI Security Workshop

- ❑ Yearly event hosted at ETSI premises, Sophia-Antipolis, France
- ❑ Comprehensive overview of standards bodies activities in Security
- ❑ www.etsi.org/SECURITYWORKSHOP



ETSI Security White Paper

- ❑ Freely available at: www.etsi.org/securitywhitepaper
- ❑ ETSI achievements and current work in all security areas
- ❑ List of all security-related ETSI publications



Thank you!

For more information:

www.etsi.org

www.3gpp.org



cbrookson@iee.org

Carmine.Rizzo@etsi.org

Dionisio.Zumerle@etsi.org