

ETSI Security Activities Overview

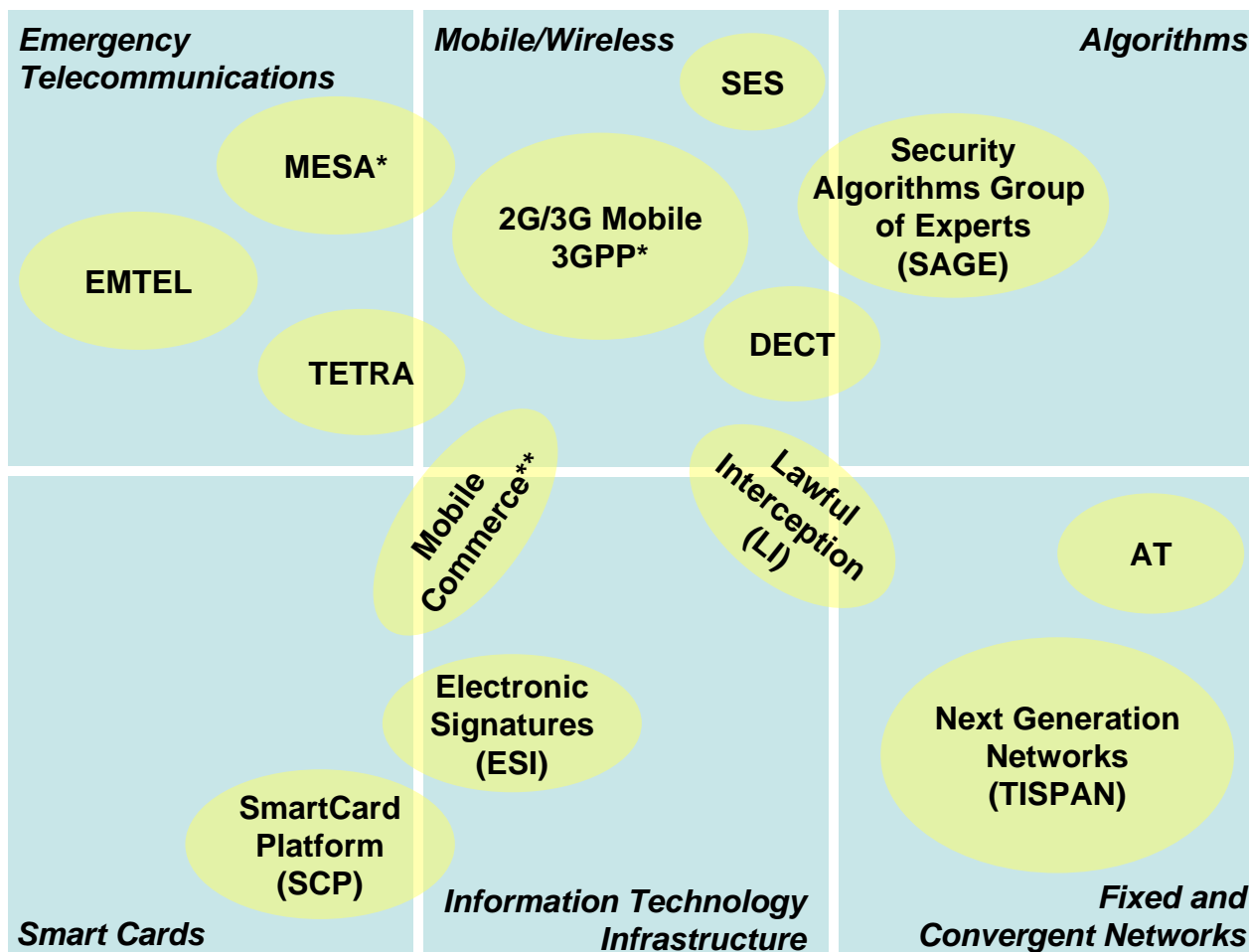
Charles Brookson
ETSI OCG Sec Chairman, UK DTI
cbrookson@iee.org

Dionisio Zumerle
ETSI Secretariat
dionisio.zumerle@etsi.org

Agenda

- Overview and OCG Security
- Mobile and Wireless Security
- Algorithms
- Smart Cards
- Next Generation Networks Security
- Lawful Interception
- Electronic Signatures
- Future Challenges

ETSI Committees per Security Areas



* ETSI is a founding partner for this partnership project

** Closed Committee

OCG Security

- ❑ Operational Co-ordination ad hoc Group on Security
- ❑ Horizontal co-ordination structure for security issues
 - Ensuring security is properly considered in each ETSI Technical Body (TB)
 - Detecting any conflicting or duplicate work
- ❑ Participation:
 - TBs are free to nominate Members to participate in the work of the group
- ❑ Working methods:
 - Via email
 - When necessary co-sited “joint security” technical working meetings
 - Issues sent to SECsupport@etsi.org
 - Mailing list: OCG_SECURITY@LIST.ETSI.ORG

Agenda

- Overview and OCG Security
- Mobile and Wireless Security**
- Algorithms
- Smart Cards
- Next Generation Networks Security
- Lawful Interception
- Electronic Signatures
- Future Challenges

GSM and 3G

- **IMEI (International Mobile Equipment Identity)**
 - Protection against theft
 - Physical marking of the terminal
 - Blacklisted by operator if stolen
- **FIGS (Fraud Information Gathering System)**
 - Monitors activities of roaming subscribers
 - Home network informed
 - Fraudulent calls identified terminated
- **Priority**
 - Public safety service
 - Allows for high priority access
- **Location**



TETRA

- ❑ TERrestrial Trunked Radio
- ❑ Mobile radio communications
 - Used for public safety services
- ❑ Security features include:
 - Mutual Authentication
 - Encryption
 - Anonymity

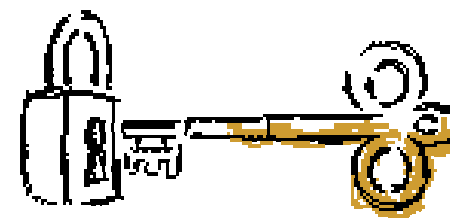


Agenda

- Overview and OCG Security
- Mobile and Wireless Security
- Algorithms
 - Smart Cards
 - Next Generation Networks Security
 - Lawful Interception
 - Electronic Signatures
 - Future Challenges

Algorithms

- ❑ ETSI is a world leader in creating cryptographic algorithms and protocols to prevent fraud and unauthorised access to ICT and broadcast networks, and to protect customers' privacy
- ❑ ETSI SAGE (Security Algorithm Group of Experts)
 - Centre of competence for algorithms in ETSI
- ❑ Algorithms for:
 - DECT
 - GSM, GPRS, EDGE
 - TETRA
 - UMTS
 - ...



GSM and UMTS Algorithms

□ GSM and EDGE

- A3, A5 and A8 – used in most GSM networks all over the world

□ GPRS

- GEA3 – encryption algorithms used

□ UMTS radio interface (UTRA)

- UEA1 and UIA1
Providing Encryption and Integrity
- UEA2 and UIA2 just released
- For more info: ETSI TR 133 908



Agenda

- Overview and OCG Security
- Mobile and Wireless Security
- Algorithms
- Smart Cards**
- Next Generation Networks Security
- Lawful Interception
- Electronic Signatures
- Future Challenges

Smart cards

□ Smart cards

- **Micro-processor equipped Tokens**
- **Able to store and process information**
 - Private key
 - Biometric template
 - ...
- **Provide Strong Authentication**
- **Used in:**
 - Banking
 - Healthcare
 - Telecoms
 - IT
 - ...



Smart Card Standardization

□ ETSI Smart Card Standardization

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

□ Current challenges

- Expand the smart card platform
- Implement Extensible Authentication Protocol (EAP) in Smart Cards
- Allow users access to global roaming
- UICC platform in secure financial transactions over mobile communications systems

Agenda

- Overview and OCG Security
- Mobile and Wireless Security
- Algorithms
- Smart Cards
- Next Generation Networks Security**
- Lawful Interception
- Electronic Signatures
- Future Challenges

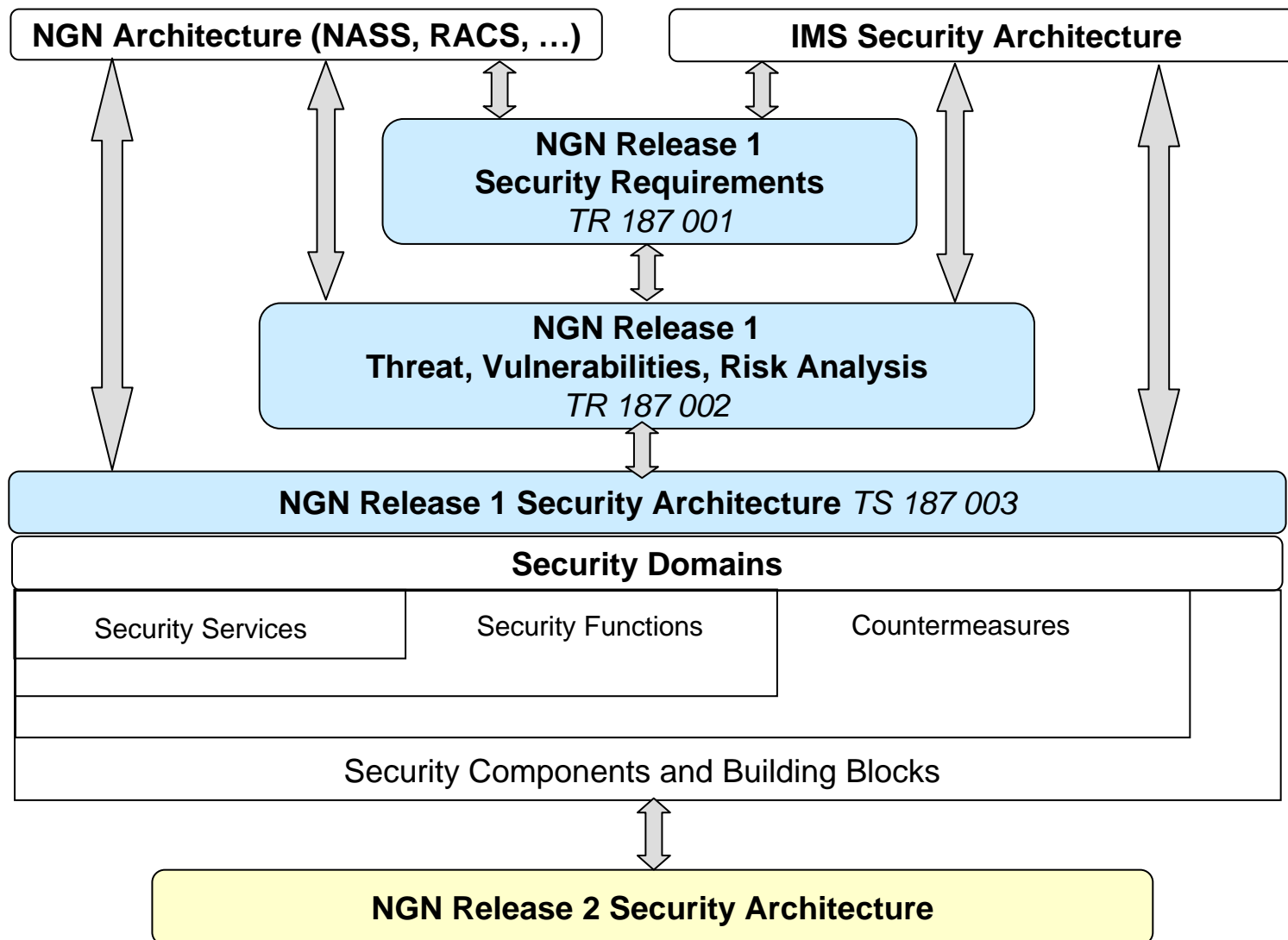
ETSI TISPAN WG7

- ❑ *NGN concept: fixed-mobile network convergence to packet-switched technology delivering multimedia services*
- ❑ **ETSI extending the 3GPP IMS concepts in TISPAN Committee designing NGN**
 - (TISPAN = **T**elecommunication and **I**nternet converged **S**ervices and **P**rotocols for **A**dvanced **N**etworking)
- ❑ **Working Group 7 NGN competence centre for security with a group of security experts**
- ❑ **WG7 standardizes NGN security**



www.tispan.org

NGN R1 Security Standards



Agenda

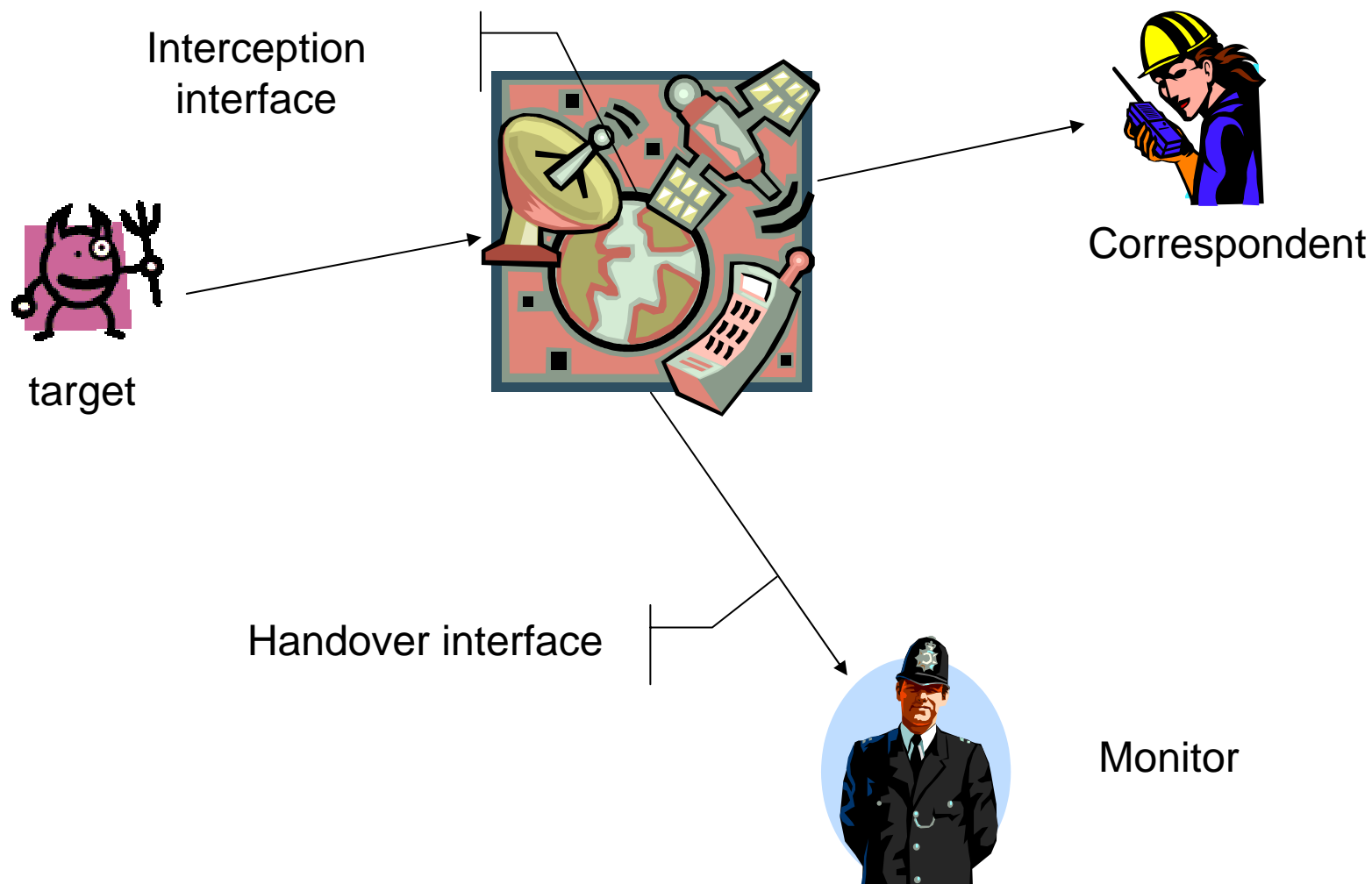
- Overview and OCG Security
- Mobile and Wireless Security
- Algorithms
- Smart Cards
- Next Generation Networks Security
- Lawful Interception**
- Electronic Signatures
- Future Challenges

What is Lawful Interception?

- ❑ Delivery of intercepted communications to Law Enforcement Authorities
 - To support criminal investigation
 - To counter terrorism
- ❑ Applies to data in transit
 - not a search of records
- ❑ Applied to any data in transit
 - Signalling
 - Speech
 - Video
 - Email
 - Web



Simple architecture



Agenda

- Overview and OCG Security
- Mobile and Wireless Security
- Algorithms
- Smart Cards
- Next Generation Networks Security
- Lawful Interception
- Electronic Signatures**
- Future Challenges

Electronic Signatures

- ❑ ETSI and CEN co-operation on the European Electronic Signature
- ❑ Goal: provide Europe with a reliable electronic signatures framework
 - Enabling electronic commerce
 - Supporting eSignature EC Directive
- ❑ Current challenges
 - eInvoicing
 - Registered EMail (REM)
- ❑ International collaboration
 - Certificate Policy mapped and aligned with US policy
 - XML Signature Standard adopted in Japan



Agenda

- Overview and OCG Security
- Mobile and Wireless Security
- Algorithms
- Smart Cards
- Next Generation Networks Security
- Lawful Interception
- Electronic Signatures
- Future Challenges**

Future Challenges

- ❑ A number of issues are open
 - Product Proofing
 - DRM
 - NGN
 - Retained Data
 - ...
- ❑ Security Standards for the Future Technologies are the Next Challenge
- ❑ ETSI can meet that challenge





Thank you for your attention

cbrookson@iee.org

dionisio.zumerle@etsi.org

OCG_SECURITY@LIST.ETSI.ORG