Welcome to the World of Standards

ETSI

World Class Standards

How secure is LTE?

Charles Brookson – Chairman ETSI OCG Security

Special thanks to Bengt Sahlin, 3GPP SA3 Chairman & Dionisio Zumerle, 3GPP SA3 Secretary

GSM Security – is it still secure?

- Chaos Computer Club – December 2010
  - GSM sniffing
  - Demonstration of how to fing GSM phones and decrypt calls
    - http://events.ccc.de/congress/2010/Fahrplan/attachments/1783_101228.27C3.GSM-Sniffing.Nohl_Munaut.pdf
  - For GSM, A5/1, only
  - Admits Operators can defend by using some methods …..

GSM Sniffing

Karsten Nohl, nohl@srlabs.de
Sylvain Munaut, 246tnt@gmail.com

SECURITY
RESEARCH
LABS

LTE – building on UMTS Security

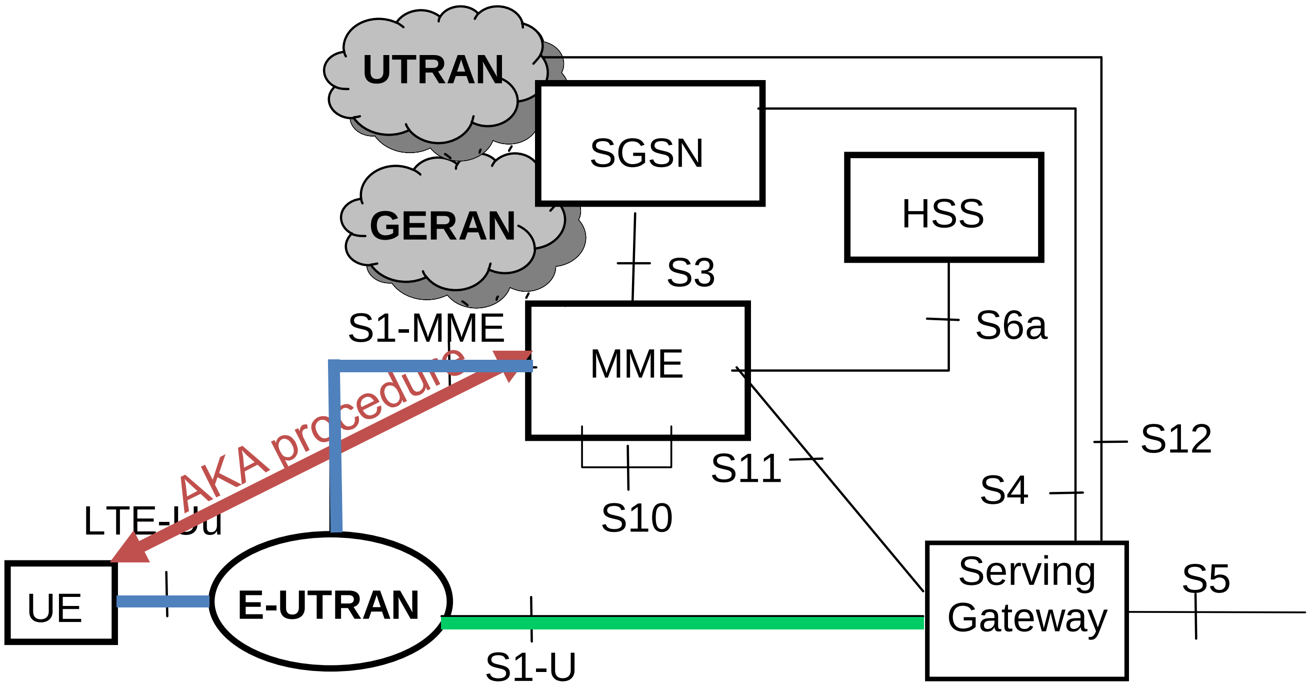
- UMTS is stronger than GSM in some ways:
  - Mutual authentication
  - Strong algorithms
  - Longer key length
  - Integrity keys

LTE implications on security

- Flat architecture: radio terminates in access network
- Interworking with a variety of legacy and non-3GPP networks
- Allowing eNB placement in untrusted locations
- Trying to keep security breaches as local as possible

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

LTE Architecture

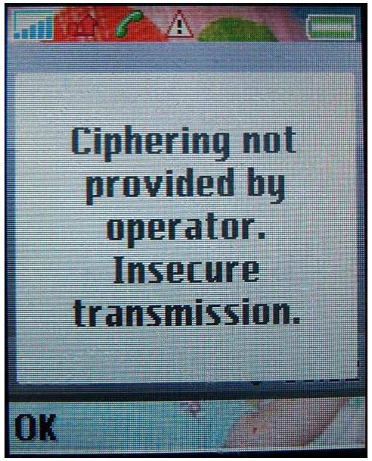


🟦 Confidentiality and integrity for signaling and user plane

🟩 Optional user plane protection (IPsec)

Encryption indication on phone

- Indication of access network encryption
  - user is informed whether confidentiality of user data is protected on the radio access link
  - in particular when non-ciphered calls are set-up

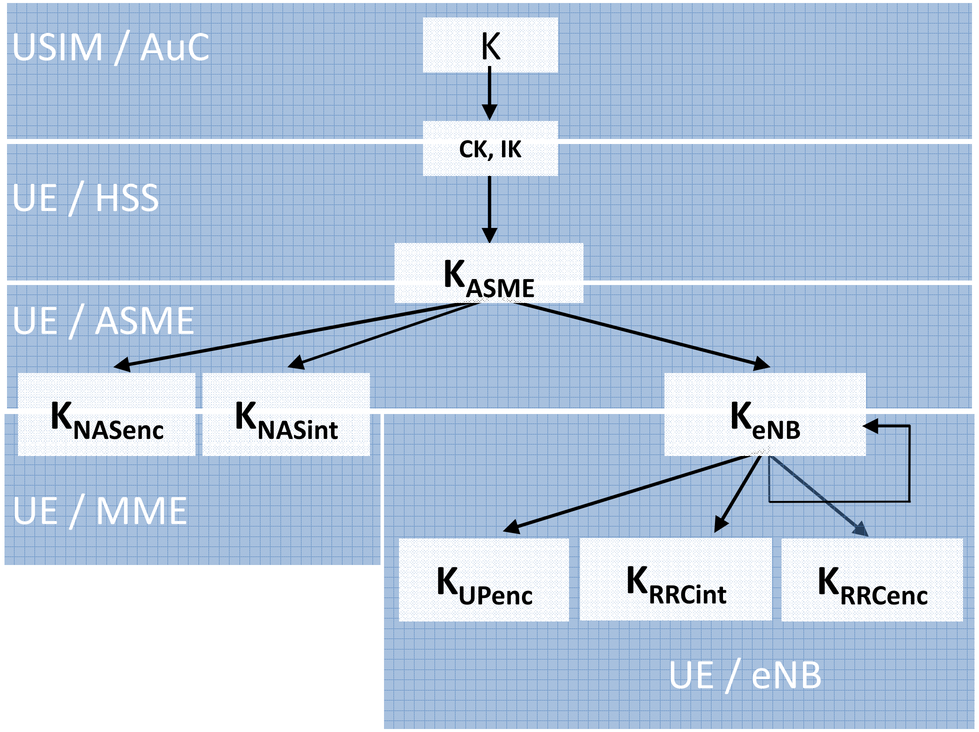


Ciphering not provided by operator. Insecure transmission.

LTE Security Algorithms

- Two sets: 128-EEA1/EIA1 & 128-EEA2/EIA2
  - AES and SNOW 3G chosen as basis
  - Different from each other as possible
    - Cracking one would not affect the other
- Third set EEA3/EIA3 under consideration
  - Based on Chinese ZUC (stream cipher)
  - Public evaluation ongoing! http://zucalg.forumotion.net/

Key hierarchy in LTE



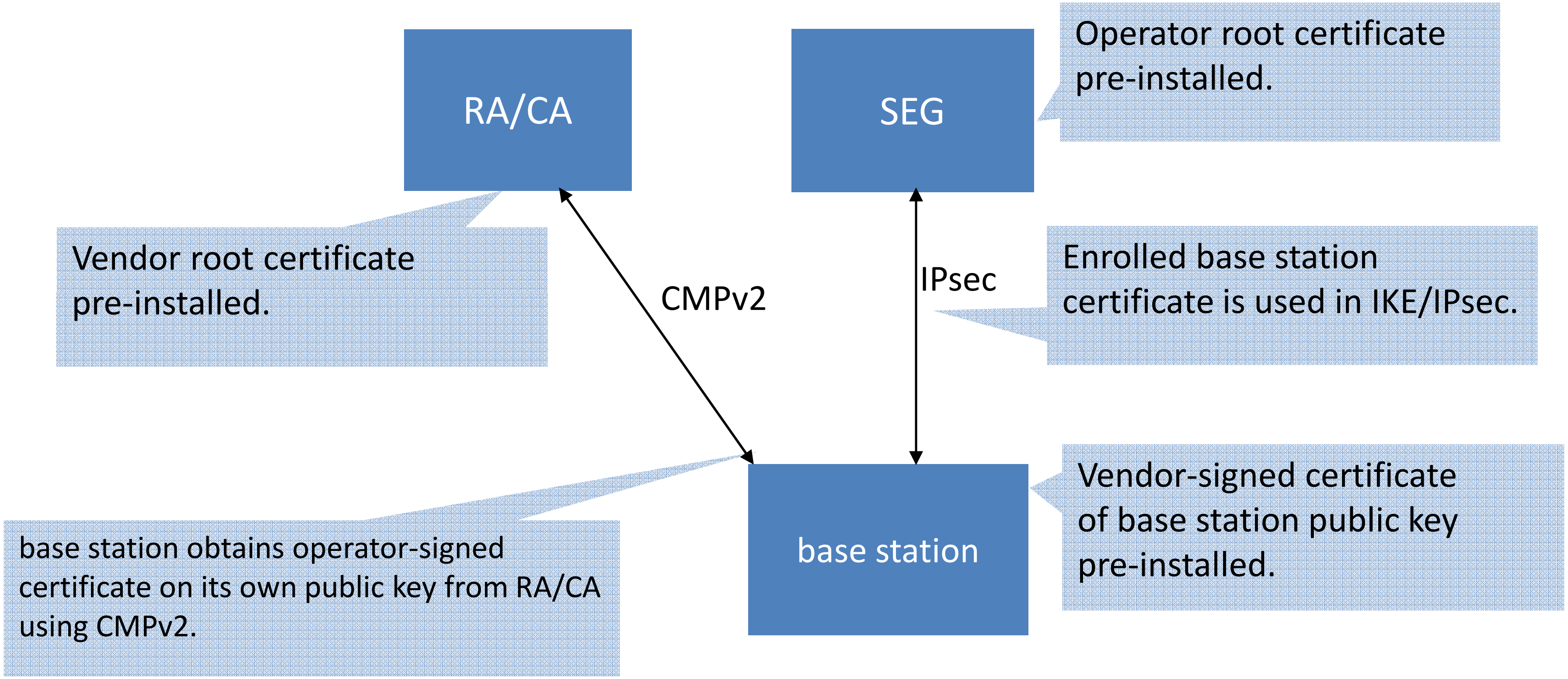
- Deeper key hierarchy than UMTS
  - Offers faster handovers
  - Keeps security breaches local
  - Adds complexity to handling of security contexts

Network Domain Security

- Base stations getting more and more powerful
  - LTE eNode B includes features of UMTS RNC
- Coverage needs grow constantly
  - Not always possible to trust physical security of location of deployment

- Greater backhaul link protection needed
- Certificate enrolment mechanisms for backhaul security

Certificate Enrollment for Base Stations



Operator root certificate pre-installed.

Vendor root certificate pre-installed.

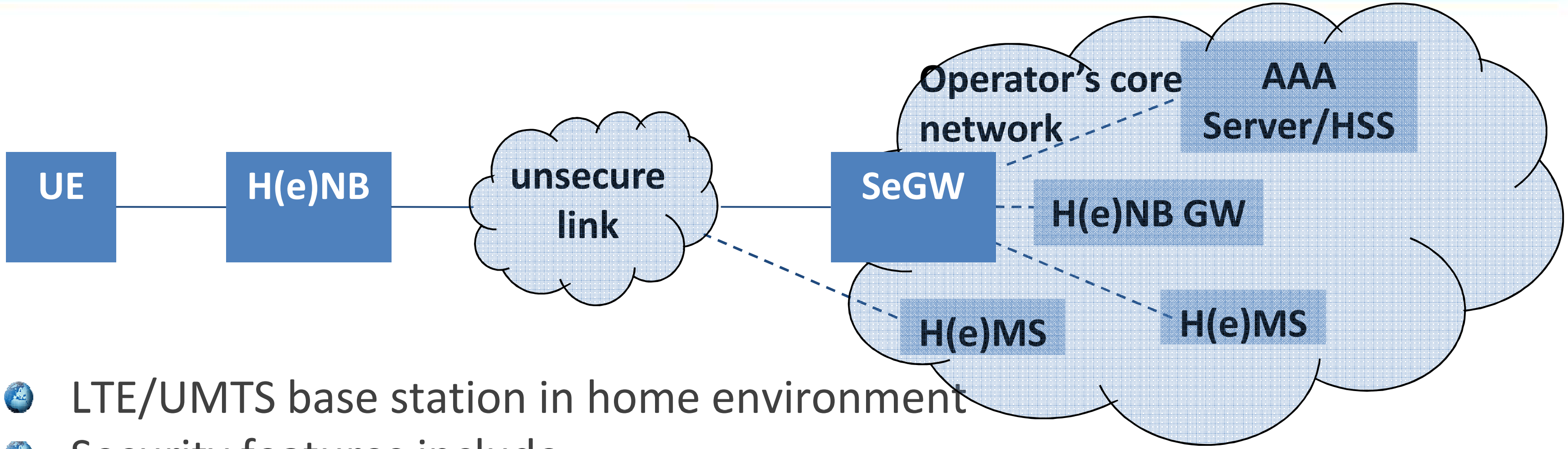
Enrolled base station certificate is used in IKE/IPsec.

Vendor-signed certificate of base station public key pre-installed.

base station obtains operator-signed certificate on its own public key from RA/CA using CMPv2.

Picture from 3GPP TS 33.310

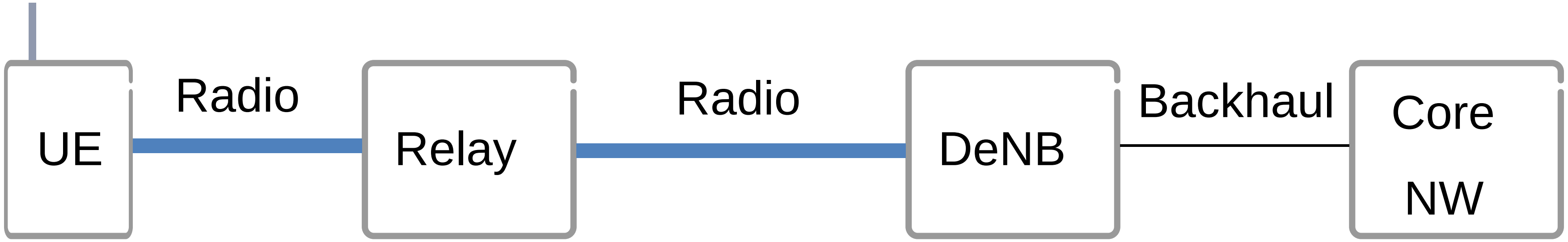
Home e Node B Security



- LTE/UMTS base station in home environment
- Security features include:
  - Integrity checking of device
  - Mutual authentication of H(e)NB and operator (SeGW) (certificate based)
  - Hosting party of the H(e)NB authentication (optional, EAP-AKA based)
  - H(e)MS (OAM server) authentication
  - Secure SW updates
  - Sensitive data not accessible in plaintext
  - Access Control Mechanism
  - Clock synchronization
  - Location locking
  - Unauthenticated traffic filtering

Relay Nodes

- e Node B that communicates directly with other eNBs over radio
- Does not require backhaul infrastructure
- Objectives
  - improve coverage of high data rates
  - improve cell edge throughput
  - augment ease of deployment
- Challenge:
  - Relay node “invisible” to the UE
  - Relay Node looks like a UE to the network in some aspects
- Basic Architecture:



Relay Node Authentication

- Mutual authentication between Relay Node and network
    - AKA used
    - credentials stored on a UICC
- Relay node device authentication is mandatory
    - Binding these two authentications needed
- One-to-one binding of Relay Node and USIM
    - binding realized by
        - symmetric pre-shared keys (psk)
        - or by certificate

Relay Node Security

- Secure environment for storing and processing sensitive data
- Device integrity check
- Control plane traffic is integrity protected
- Optional integrity protection of user plane traffic
- Connection between Relay Node and network is confidentiality protected

Security for Machine-Type Communications

- Analysis of security aspects ongoing
  - identification and analysis of threats
  - identification of potential security impacts of the system improvements
  - identification of potential new security features needed

Single Sign On

- Two ongoing studies:
  - SSO Application Security for IMS (figure)
  - SSO frameworks with 3GPP networks for various operator authentication configurations

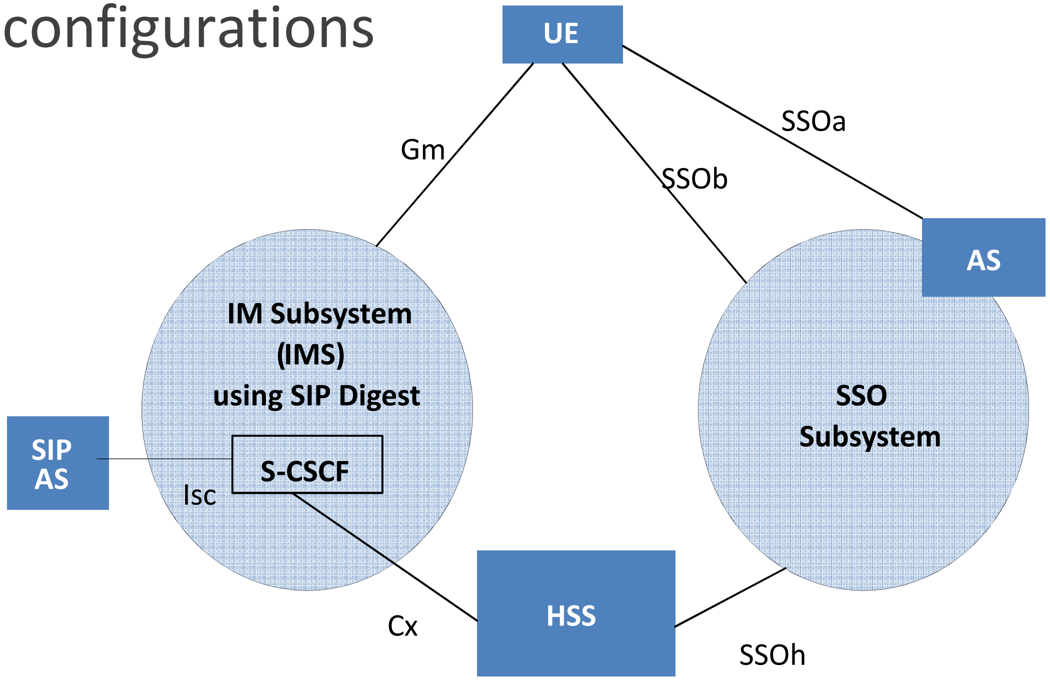
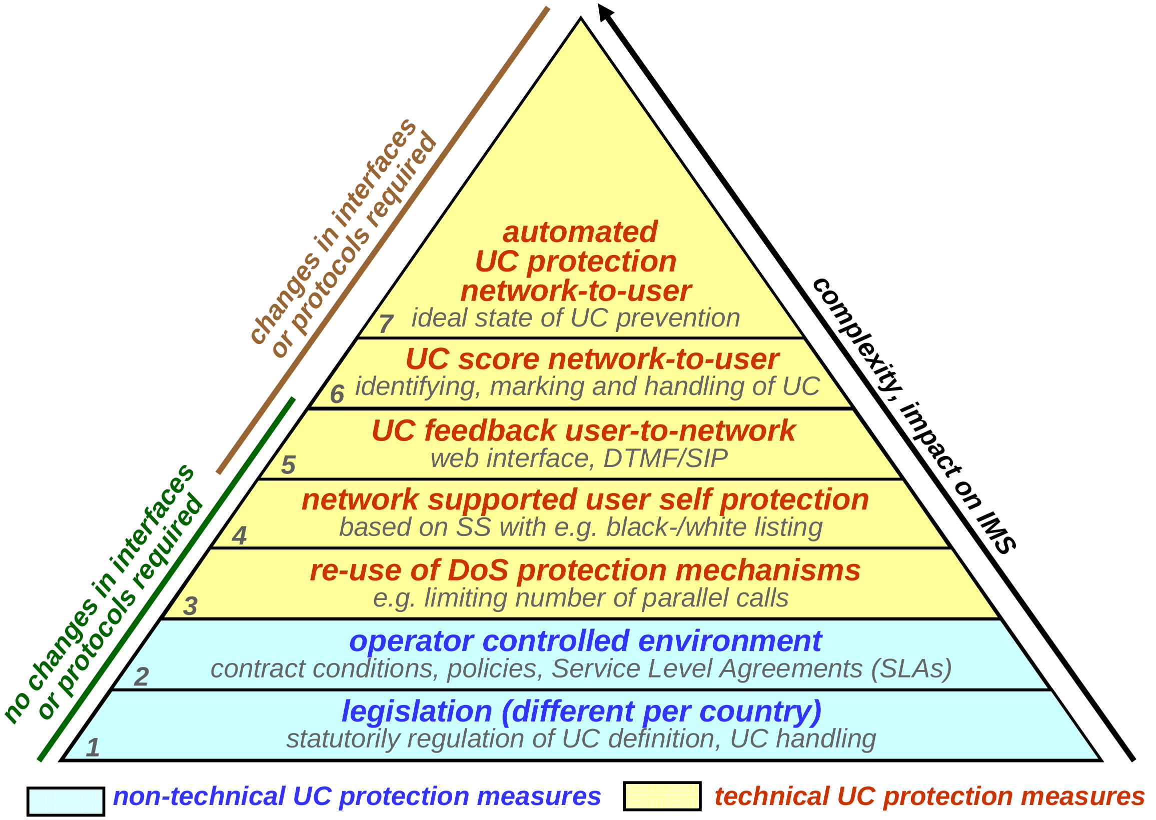


figure from draft 3GPP TR 33.914

Protection against Unsolicited Communication (UC)

- Protect mobile subscribers from receiving unsolicited communication (aka SPIT) over IMS
- Current work analyses possible solutions



changes in interfaces or protocols required

no changes in interfaces or protocols required

complexity, impact on IMS

7 **automated UC protection network-to-user**
ideal state of UC prevention

6 **UC score network-to-user**
identifying, marking and handling of UC

5 **UC feedback user-to-network**
web interface, DTMF/SIP

4 **network supported user self protection**
based on SS with e.g. black-/white listing

3 **re-use of DoS protection mechanisms**
e.g. limiting number of parallel calls

2 **operator controlled environment**
contract conditions, policies, Service Level Agreements (SLAs)

1 **legislation (different per country)**
statutorily regulation of UC definition, UC handling

▭ *non-technical UC protection measures* ▭ *technical UC protection measures*

Selection of 3GPP Security Standards

LTE:
33.401 System Architecture Evolution (SAE); Security architecture
33.402 System Architecture Evolution (SAE); Security aspects of non-3GPP
Home (e) Node B:
33.320 Security Home (evolved) Node B (H(e)NB)
General and 3G:
33.102 Security architecture
33.203 Access security for IP-based services
Lawful Interception:
33.106 Lawful interception requirements
33.107 Lawful interception architecture and functions
33.108 Handover interface for Lawful Interception
GBA:
33.220 GAA: Generic Bootstrapping Architecture (GBA)
Network Domain Security:
33.310 Network Domain Security (NDS); Authentication Framework (AF)
SSO:
33.914 Single Sign On for Application Security for IMS
33.924 Interworking of GBA and OpenID
33.980 Interworking of GBA and Liberty Alliance

How secure is LTE?

- Building on GSM and UMTS Security
- Newer security algorithms, longer keys
- Extended key hierarchy
- New features, addressing new scenarios
  - Home evolved Node B
  - Relay Node
- New topics
  - Machine-Type Communication, Single Sign-On, Protection against Unsolicited Communication over IMS

Questions?