How to secure an LTE-network: Just applying the 3GPP security standards and that's it?

Telco Security Day @ Troopers 2012

Peter Schneider

Nokia Siemens Networks Research

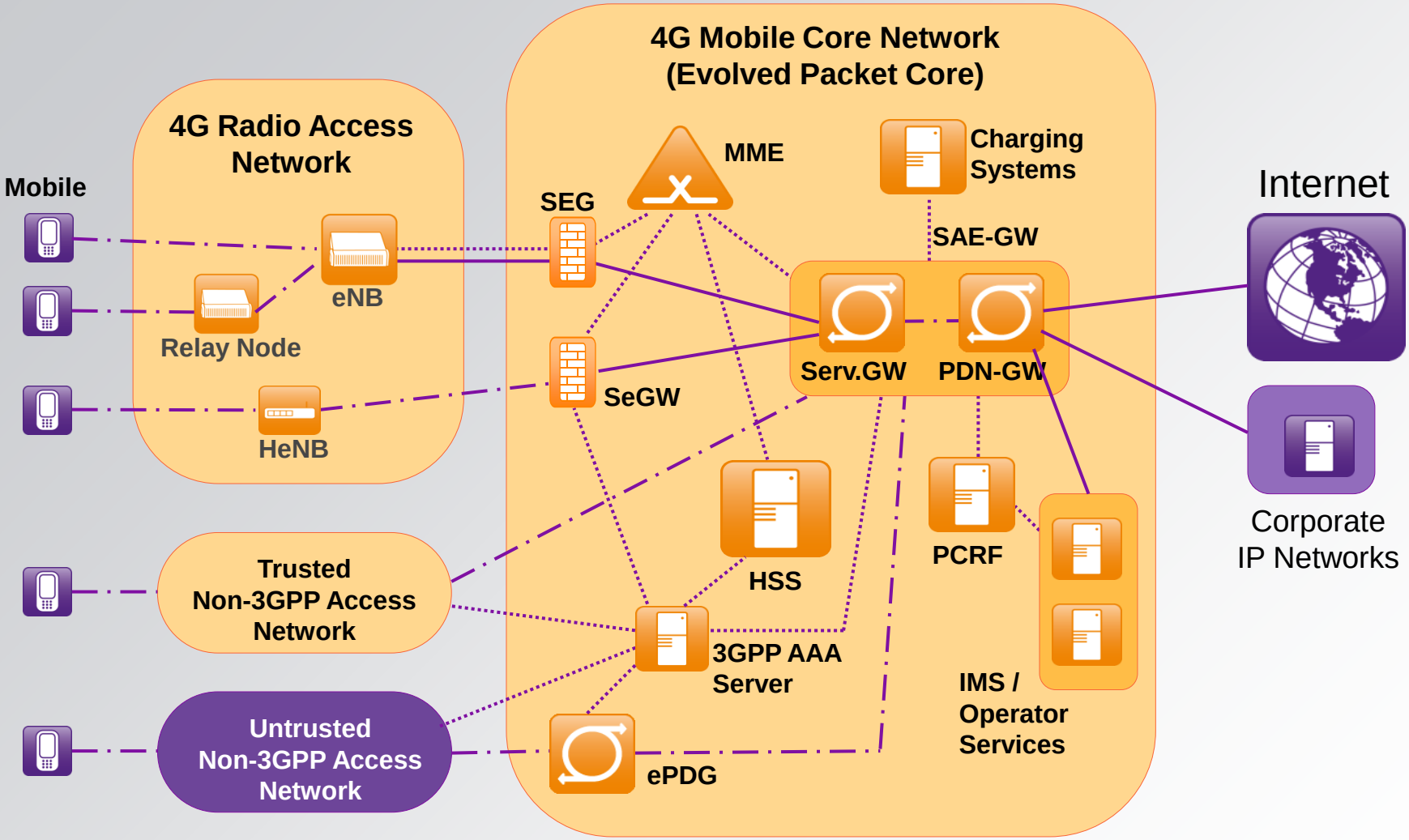
for a world in motion™

Intro / Agenda

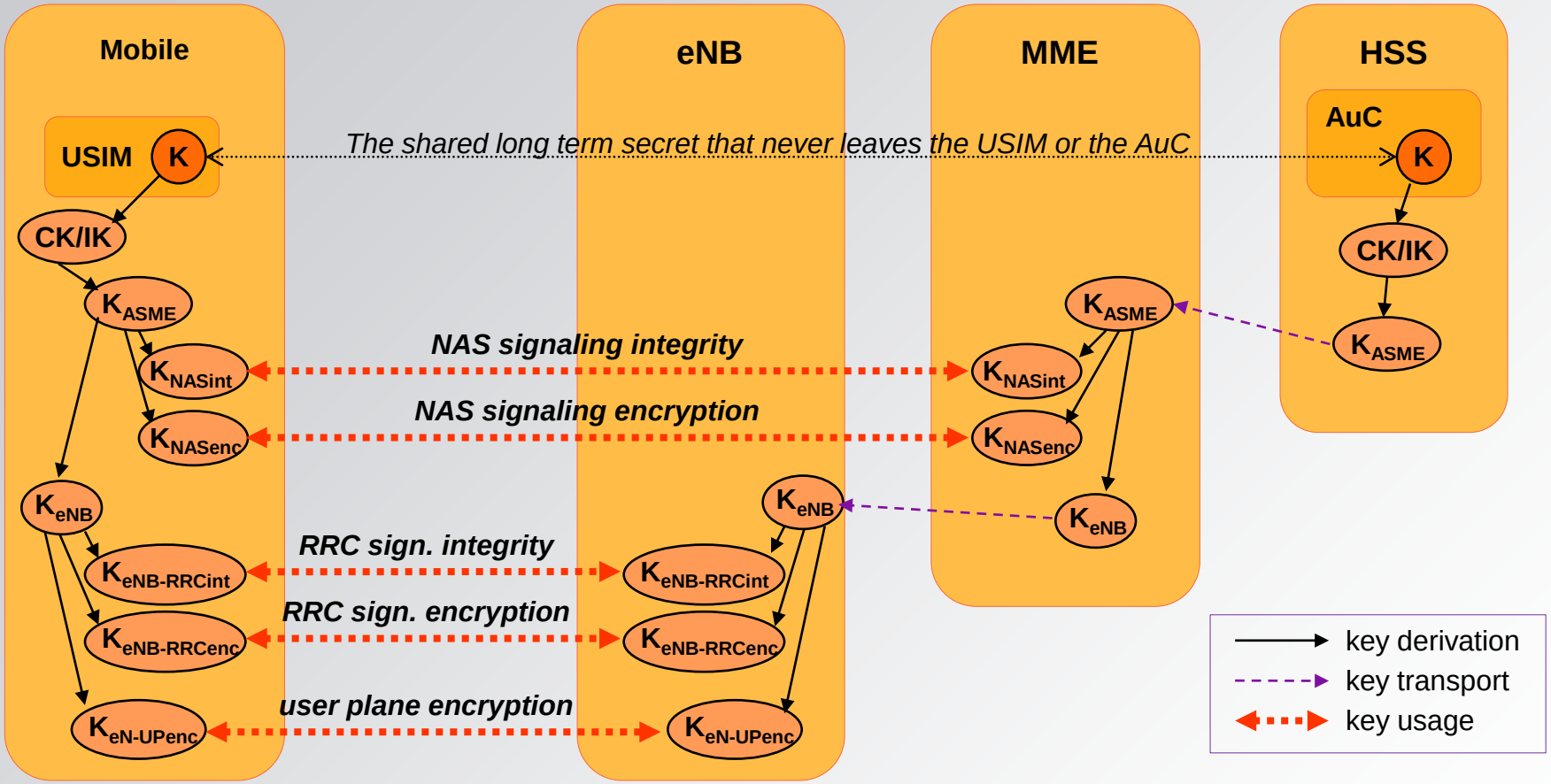
- answer the title question:
  → not only a simple “obviously not”
- 3GPP security architecture of the Evolved Packet System, aka “(SAE/)LTE-network”, “4G mobile network”
- IP network security, network element security for the EPS
- many names:
  - 3GPP: 3.Generation Partnership Project
  - LTE: Long Term Evolution
  - SAE: System Architecture Evolution
  - EPS: Evolved Packet System
  - 4G Mobile Network

(List of 3GPP specific abbreviations at the end)

The Evolved Packet System (4G Mobile Network)



EPS Key Hierarchy and Radio Interface Security



ASME	Access Security Mgmt. Entity	eNB	Evolved Node B	NAS	Non Access Stratum
AuC	Authentication Centre	IK	Integrity Key	RRC	Radio Resource Control
CK	Cipher Key	MME	Mobility Management Entity	USIM	UMTS Subscriber Identity Module

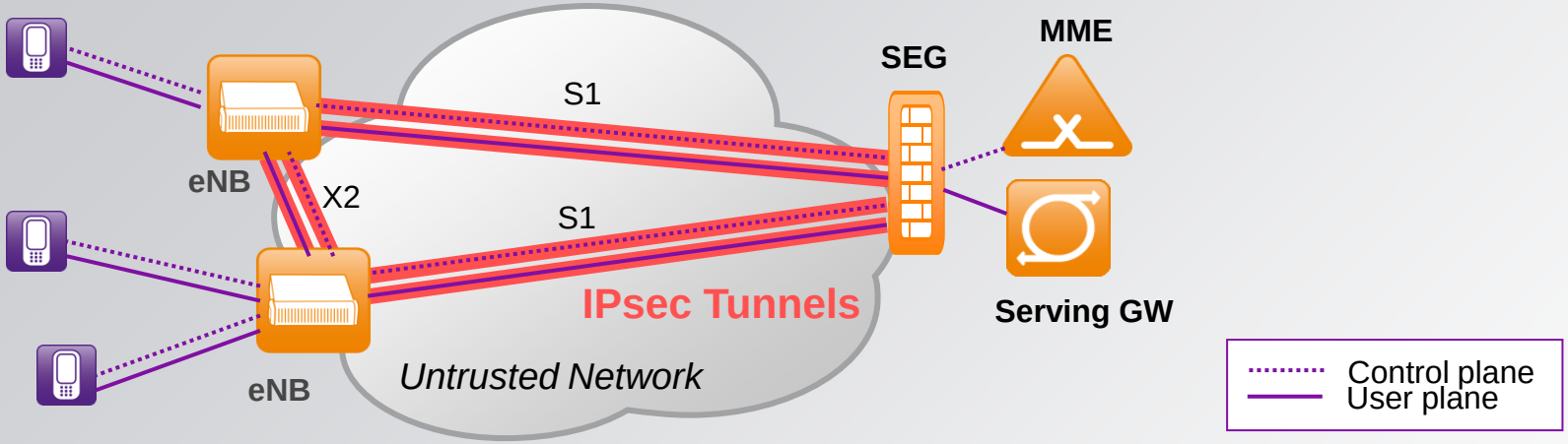
Nokia Siemens Networks

EPS Key Hierarchy and Radio Interface Security (continued)

- Authentication and Key Agreement (AKA) based on long term shared secrets (in USIM and AuC)
  - key hierarchy providing key separation
  - 5 independent 128bit keys
  - binding of keys to serving network identities
- integrity and confidentiality protection of Non Access Stratum (NAS) and Access Stratum (AS) signaling
- strong algorithms: SNOW 3G, AES, optionally ZUC
- integrity protection mandatory, encryption recommended
- no integrity for the user plane (issue with transmission errors)
- user and terminal identity confidentiality (against passive attacks only)

➔ a sound concept, assumed to be strong enough for the next decade

Backhaul Link Security

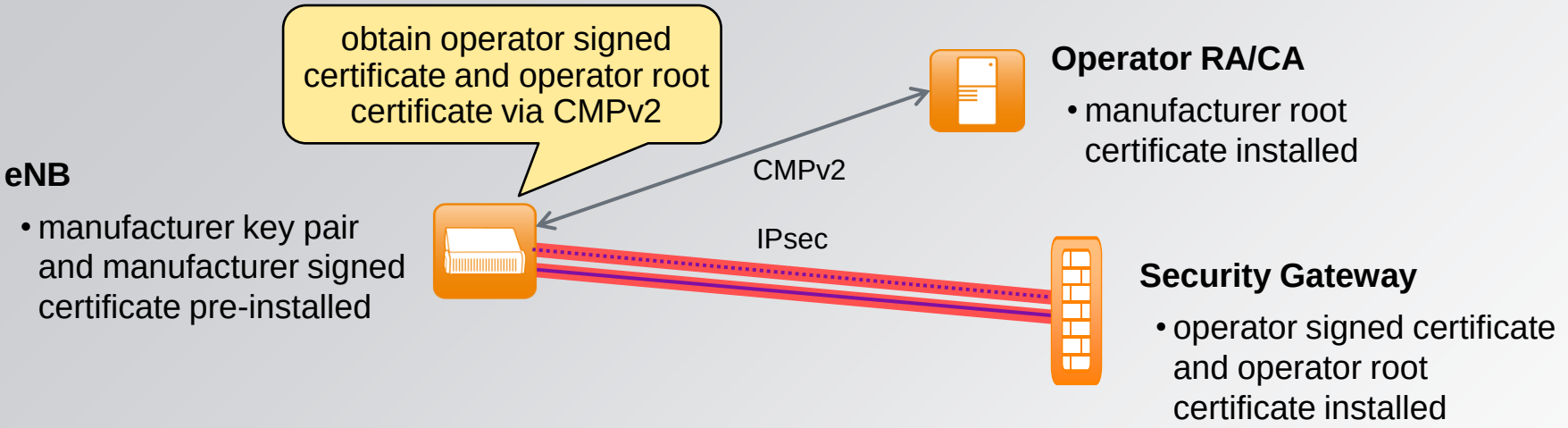


- IKEv2/IPsec with integrity and confidentiality protection mandatory for all traffic (control/user/management plane)
- well, not mandatory in all cases:

  "In case S1 and X2 user plane interfaces are trusted (e.g. physically protected), the use of IPsec/IKEv2 based protection is not needed." [3GPP TS 33.401 V11.2.0 (2011-12)]

  and this holds also for control and management traffic

Backhaul Link Security (continued)



- profiling of IKEv2/IPsec specified; IKEv2 based on certificates
- eNB comes equipped with id, private/public key pair, manufacturer certificate, can be integrated into the operator PKI via certificate enrolment
  - "plug and play" solution
  - alternatively: pre-installed operator certificate for mutual authentication when initially connecting to the core network → more secure and more expensive

→ a highly secure backhauling solution is specified (but less secure ones are not excluded)

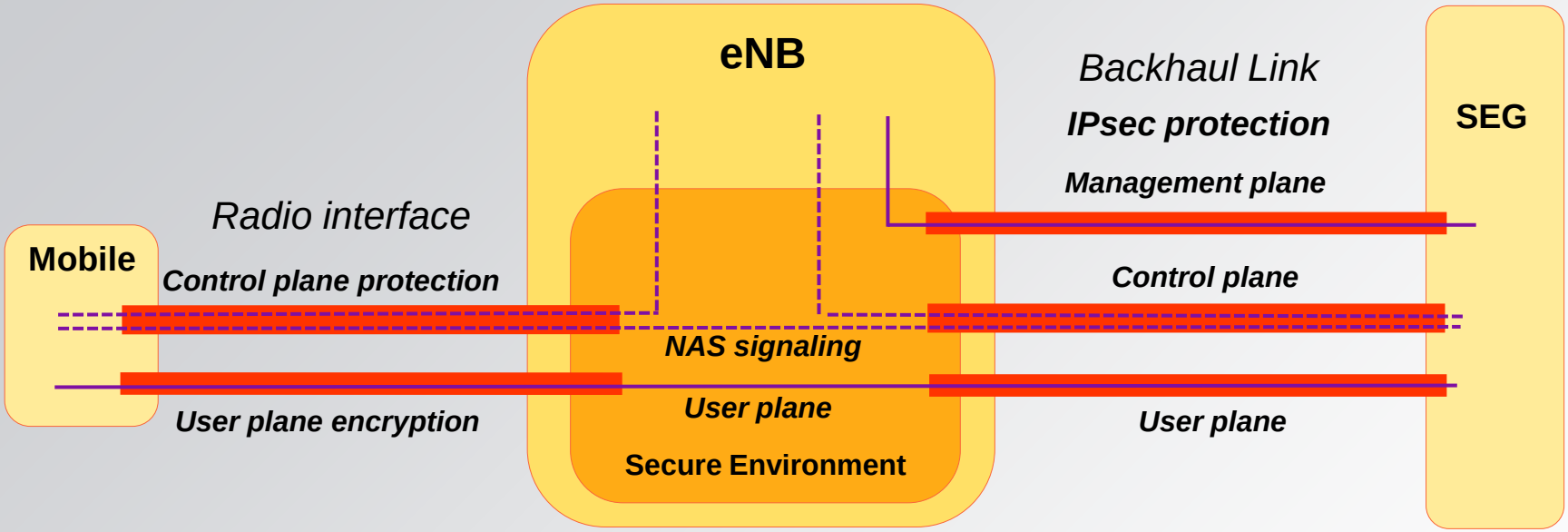
Security for Core Interfaces (NDS/IP – Network Domain Security for IP)

- IKE/IPsec profiles specified similar as for backhaul link (IKEv2 or v1, peer authentication based on certificates, IPsec ESP in tunnel mode)
  - IPsec mandatory to use for integrity protection of control traffic between "security domains"
    - example: GTP-C traffic between serving network and home network when roaming
  - in specific cases, also encryption is mandatory
    - e.g. interface between core and 3G radio network controller, if they are in different security domains → protects 3G radio interface keys sent to the controller
    - seems that this has been forgotten (?) for the interface between MME in serving network and HSS in home network (S6a when roaming)
  - all other IPsec protection is optional
- Security Gateways (SEGs) to be used at security domain borders
  - terminate IKE/IPsec
  - not specified: firewall functions (not required for interoperability)

→ standard gives hints - but in the end the operator has to decide where and how to use NDS/IP

Nokia Siemens Networks

eNB (4G Base Station) Security



Nokia Siemens Networks

eNB (4G Base Station) Security (continued)

- performs the crypto specified for radio interface and backhaul link
- has access to the cleartext in the user plane
- may be exposed to tampering that can result in compromise - and then:
  - eavesdrop/modify user traffic, send maliciously crafted PDUs to the core, detach mobiles, discard traffic
  - mostly applicable to the local cell (possibly also to neighboring cells)
  - more to figure out …
- 3GPP requires a secure environment inside the eNB
  - stores keys, executes crypto, helps to secure boot
  - preserves integrity and confidentiality of its content
  - only authorized access

➔ standardized requirements, but no standardized solution for the secure environment (not required for interoperability)

HeNB (4G Femto Cell) Security

- relevant functions within the security architecture – like the regular eNBs
- even more exposed to tampering and compromise - and can be easily set up where required (increase transmission power if necessary)
  - ➔ targeted attack against victim users, e.g. “celebrity attack”: eavesdrop the celebrity’s calls
  - plus attacks against the core network (see eNB)
- 3GPP requires
  - a Trusted Environment inside the HeNB
    - built on a HW-based root of trust, secure boot, load only verified components
    - assure the eNB secure environment for crypto, key storage etc.
  - a device integrity check on boot (in case of failure no access to credentials)

➔ standardized strong requirements, but no standardized solution (not relevant for interoperability)

- a typical operator business case requires cheap HeNBs, low TCO
  - ➔ How secure will HeNBs be in practice?

Nokia Siemens Networks

HeNB (4G Femto Cell) Security (continued)

- HeNB may be in closed mode (can only be used by a CSG – Closed Subscriber Group) – this can protect other subscribers (in Rel 11)
- mutual authentication with IKEv2 when connecting to the core
- optional hosting party authentication
- IPsec used to be mandatory for all communication with the core network (in Rel 9), but in Rel 11 the standard says:

  "If the operator chooses not to use IPsec, mutual authentication between the H(e)NB device and the SeGW shall be performed and the interface between the H(e)NB and SeGW shall be secured with a mechanism that provides layer 2 security for confidentiality and integrity protection of communications. This mechanism then shall also bind this secure communications to device authentication … "
  [3GPP TS 33.320 V11.4.0 (2011-12)]

  ➔ Would you like to implement it this way?
- most of the above holds also for 3G femto cells

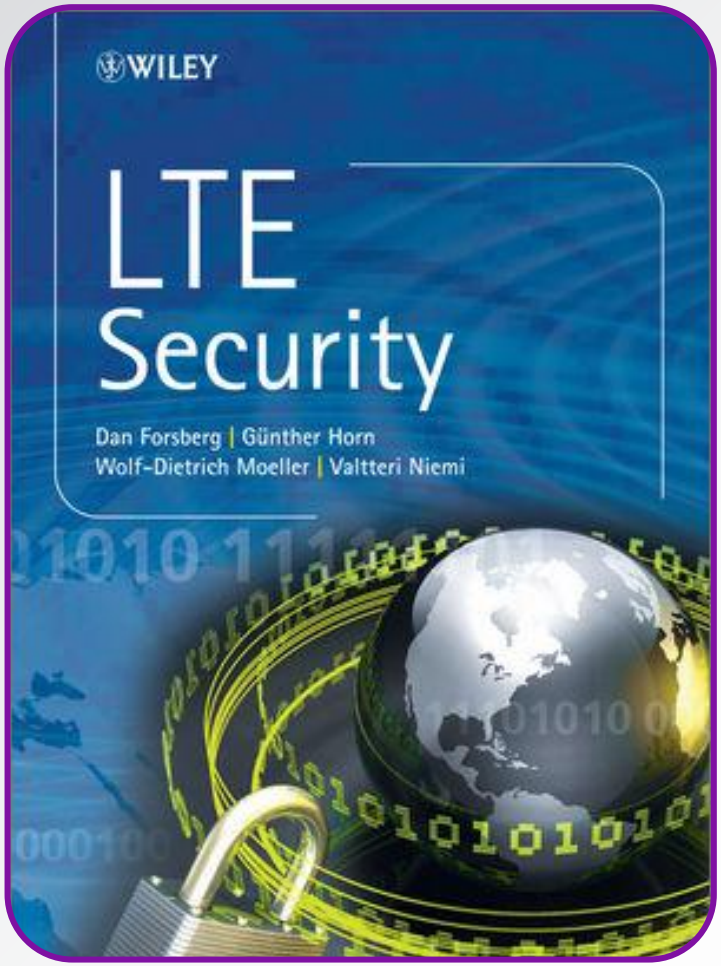
  ➔ How secure do you consider today's 3G femto cell deployments?

Other EPS Security Mechanisms

cover

- usage of relay nodes
- non-3GPP access to the core network
- mobility
  - intra LTE
  - between LTE and 2G/3G networks
  - between 3GPP and non-3GPP access networks
- security for the IP multimedia subsystem (→ voice over LTE)
- generic bootstrapping architecture
- and more

→ Buy you a good book to find out !



Nokia Siemens Networks

Threat mitigation

- 3GPP addresses security of interfaces mainly
  - security specified for radio interface, backhaul link, core interfaces
    →protects traffic against interception, modification, replay
  - subscriber authentication
    →protects against theft of service, impersonation of other subscribers, fraud
- there's a new trend in 3GPP to cover also platform security – by standardizing requirements (solutions are proprietary)

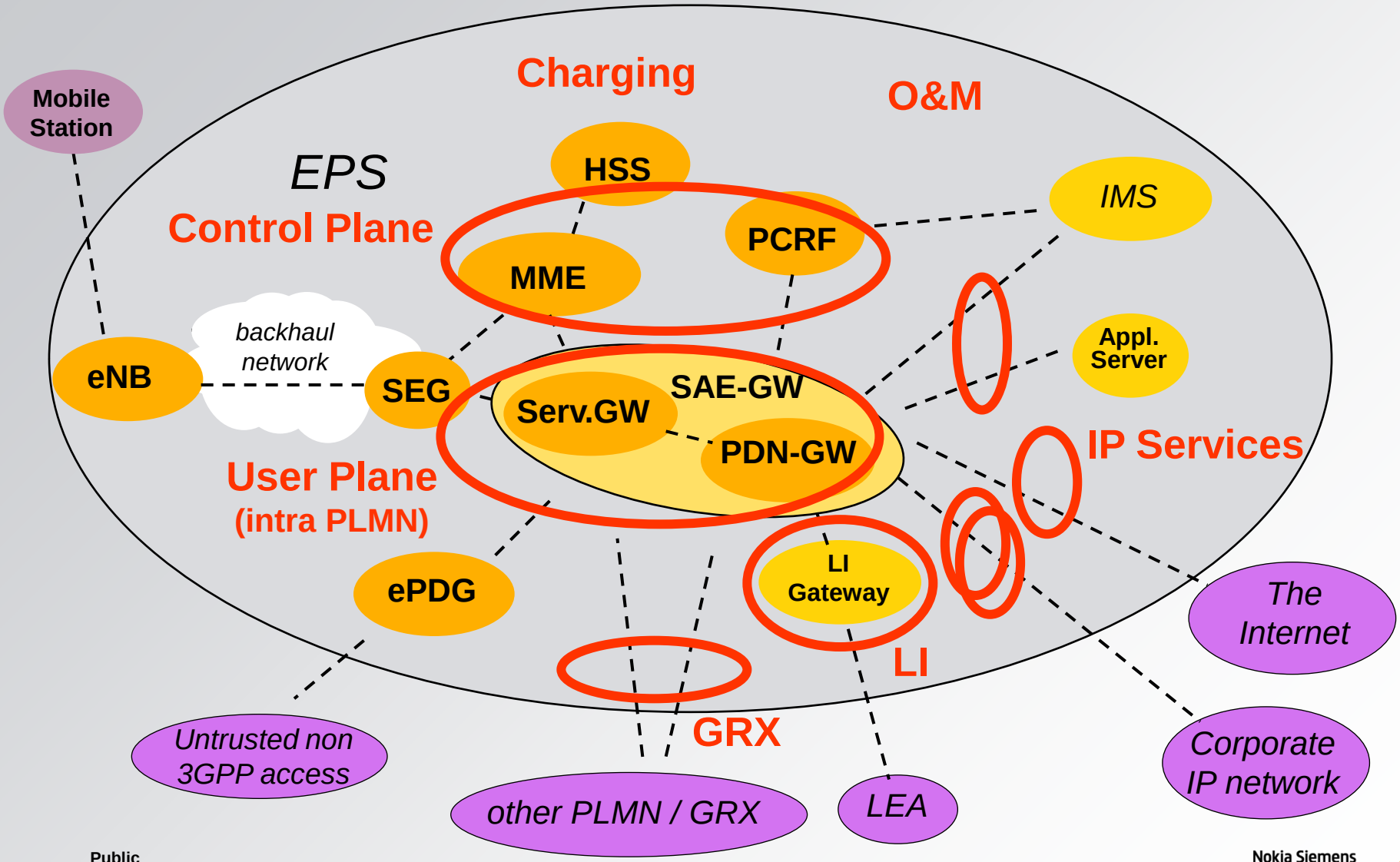
- this leaves a lot to address otherwise:
  - flooding, crashing or compromising nodes by exploiting implementation flaws, compromising network elements via weak O&M procedures, …

→ IP network security, network element security

- out of scope here: physical site protection, organizational security measures (e.g. malicious insider threat)

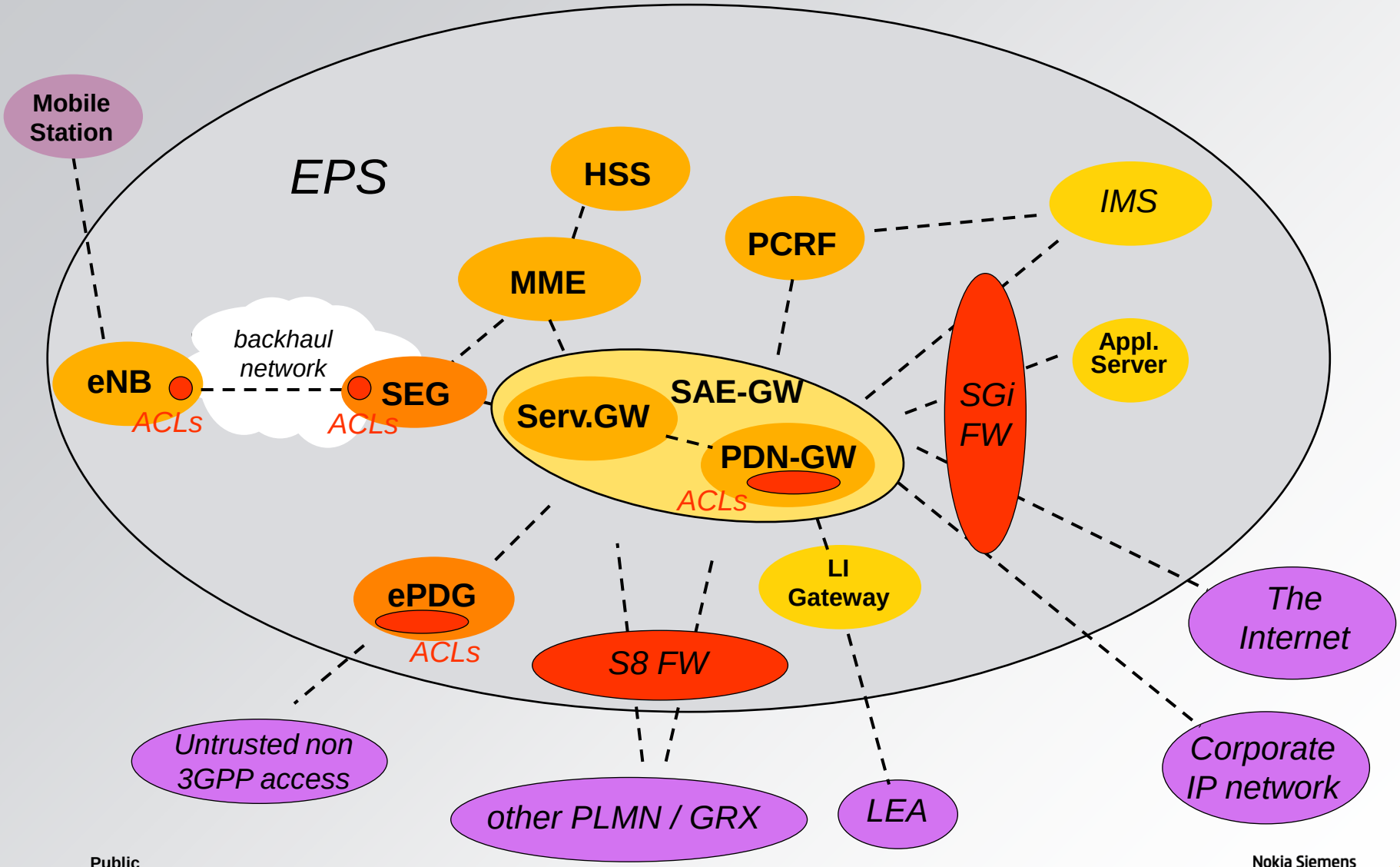
Nokia Siemens Networks

EPS Traffic Separation Example



Nokia Siemens Networks

EPS Perimeter Security Example



IP Network Security Measures

- traffic separation
- perimeter security
- secure operation and maintenance (O&M)
- secure operation of services/protocols like DNS, NTP, IP routing etc.

- additional, enhanced security measures
  - if required to mitigate a specific threat scenario
  - if enhanced security is part of the service the MNO offers to the subscribers
- examples:
  - enhanced packet inspection, intrusion detection and prevention
  - enhanced security support for IP based mobile stations (e.g. antivirus, antiphishing, parental control, health check etc.)

Network Element Security

- threat and risk analysis per network element
- network element security architecture
- secure coding
- hardening
- security testing
- security audit
- security vulnerability monitoring
- process for timely patching
- …

➔ This is really essential!

but out of the scope of this presentation …

Nokia Siemens Networks

Summary: How to Secure an LTE-Network?

- Comply with the 3GPP recommendations

  … and choose the good options!

- Do all the other stuff:
  - use IP network security mechanisms
  - use network elements designed and implemented with security in mind
  - organizational security measures, physical site protection, …
  - monitor your network

  … security is a process!

Nokia Siemens Networks

Some Abbreviations

3GPP	3. Generation Partnership Project
ASME	Access Security Management Entity
AuC	Authentication Centre
CA	Certificate Authority
CMP	Certificate Management Protocol
CK	Cipher Key
eNB	Evolved Node B
enc	Encryption
EPC	Evolved Packet Core
ePDG	Evolved Packet Data Gateway
EPS	Evolved Packet System
ESP	Encapsulating Security Payload
GRX	GPRS Roaming eXchange Network
GTP-C	GPRS Tunneling Protocol - Control
GW	Gateway
HeNB	Home eNB
HNB	Home Node B
HSS	Home Subscriber Server
IK	Integrity Key
IMS	IP Multimedia System
int	Integrity
K	Key
LEA	Law Enforcement Agency
LI	Lawful Interception
LTE	Long Term Evolution
MME	Mobility Management Entity
NAS	Non Access Stratum
PCRF	Policy and Charging Rules Function
PDN	Packet Data Network
PKI	Public Key Infrastructure
PLMN	Public Land Mobile Network
RA	Registration Authority
RRC	Radio Resource Control
SAE	System Architecture Evolution
SEG	Security Gateway
SeGW	Security Gateway
Serv.GW	Serving Gateway
UMTS	Universal Mobile Telecomunication System
UP	User Plane
USIM	UMTS Subscriber Identity Module

Nokia Siemens Networks