LTE Radio Interface

and its

Security Mechanism

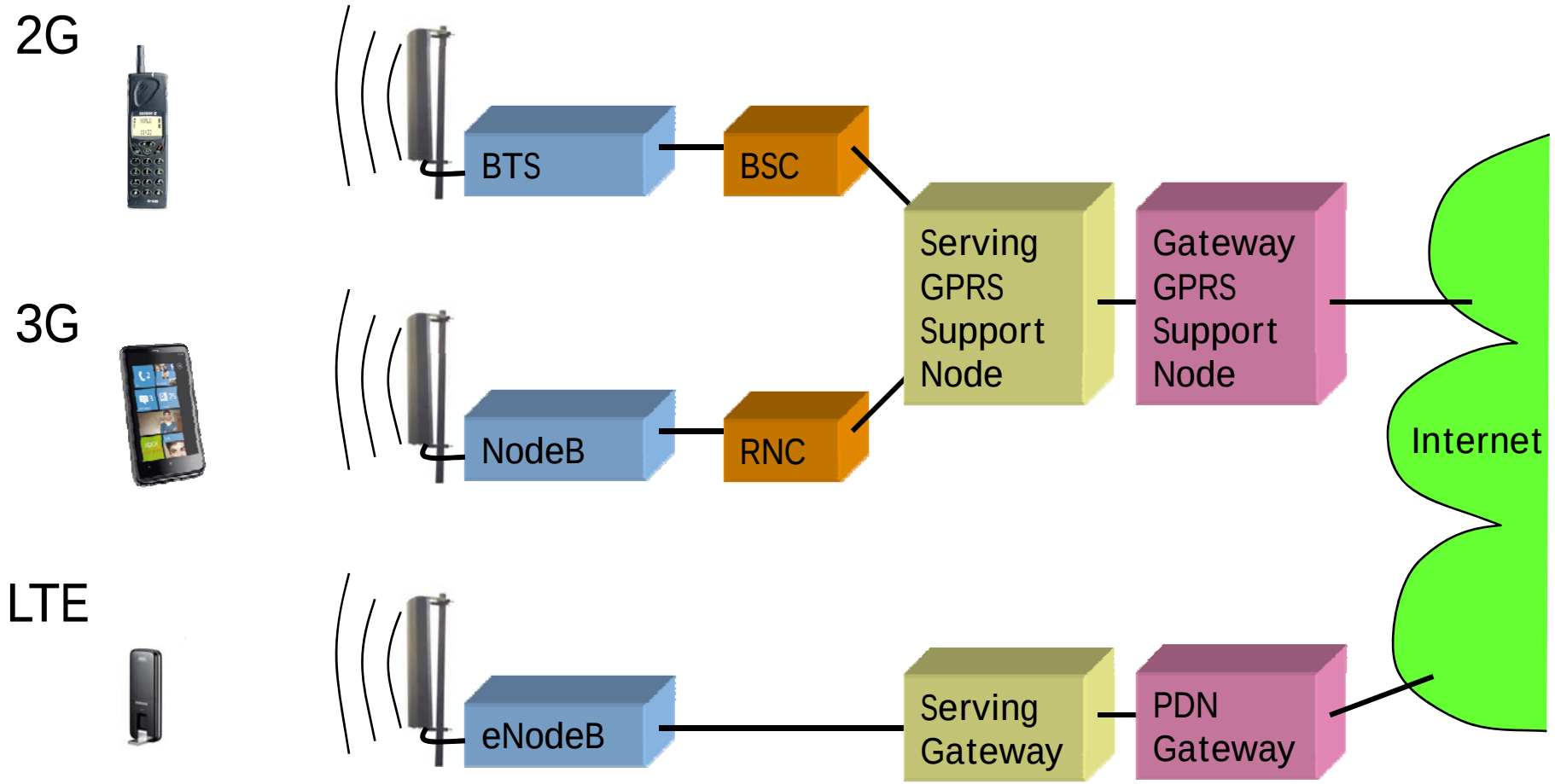
A1 Telekom Austria

Content

- Comparison of 2G,3G and LTE Packed Domain
- EPS
- LTE Requirements
- Main Characteristics of LTE Physical Layer
- The MME
- LTE and SAE ID´s
- Latency Considerations
- DL Resource Elements
- Keys in LTE
- Security for Voice over LTE
- Future

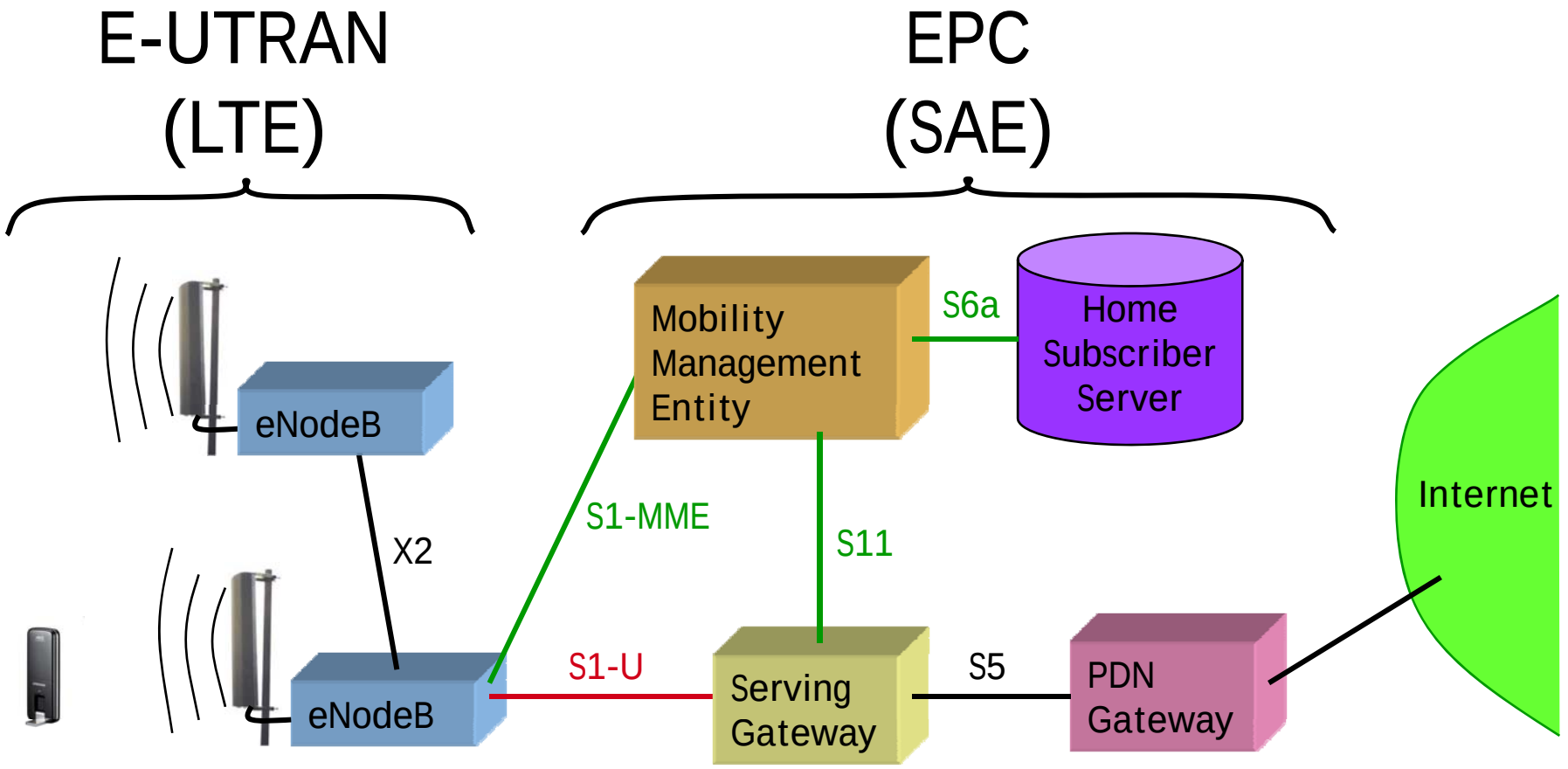
A1 Telekom Austria

Comparison of 2G, 3G, LTE – PACKET DOMAIN



A1 Telekom Austria

EPS – Evolved Packet System



A1 Telekom Austria

LTE Requirements

Services

Internet
Telephony
Mobility up to 250km/h
Broadcast (eg MBMS)

High Data Rates

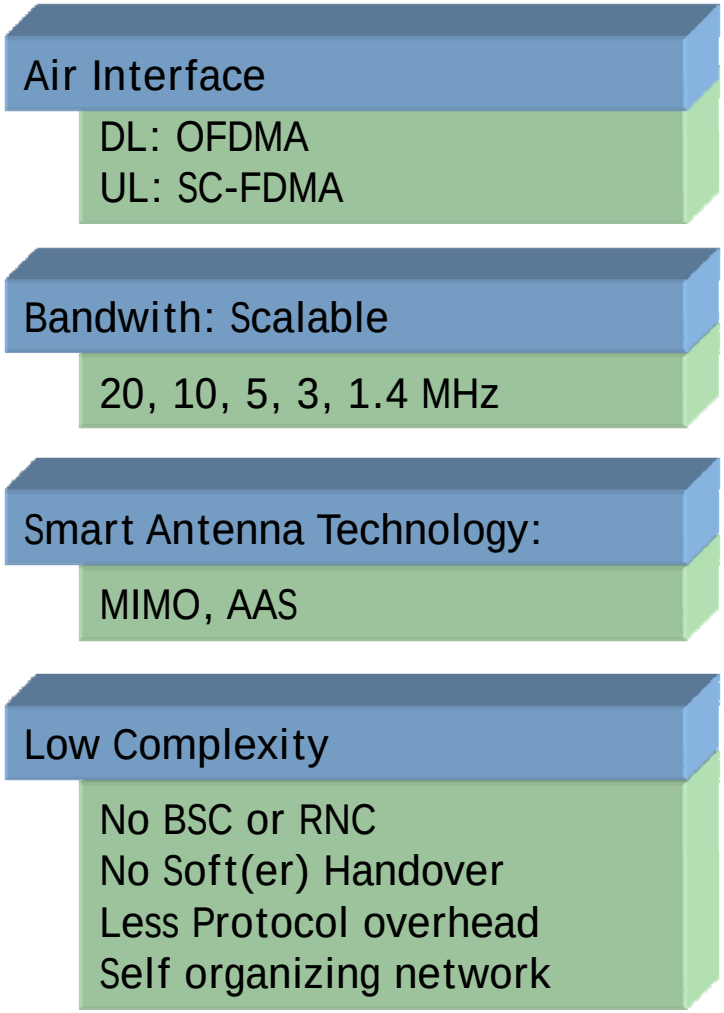
Up to >100 Mbit/s DL (2x2 Ant)
Up to >300 Mbit/s DL (4x4 Ant)
Up to >50 Mbit/s UL
Higher spectral Efficiency than R6

PS Services only

User plane latency <10ms
Control plane latency < 100ms

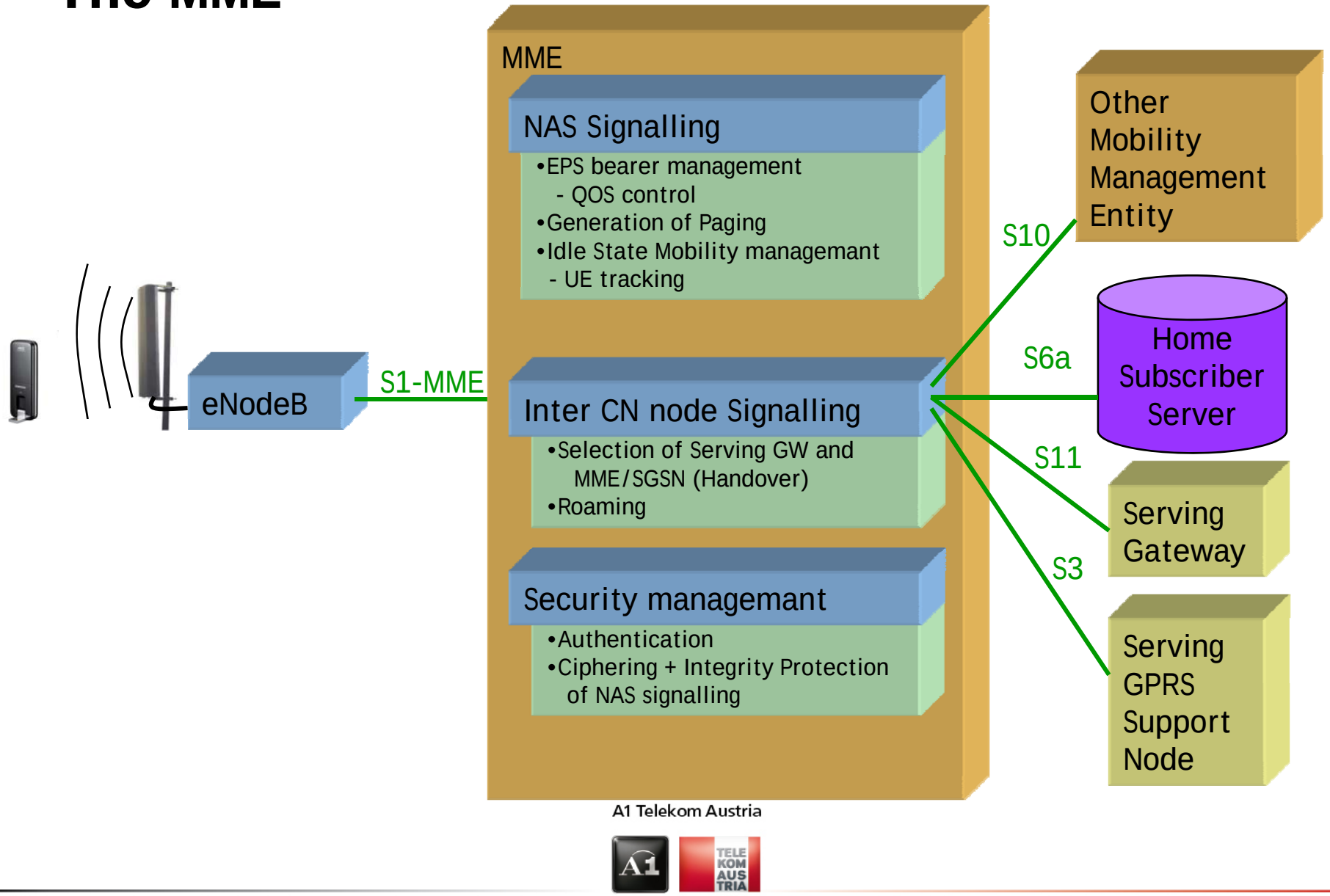
A1 Telekom Austria

Main characteristics of LTE Physical Layer



A1 Telekom Austria

The MME



A1 Telekom Austria

LTE and SAE ID´s

Network

PLMN ID (MCC + MNC) 24 bit
EPS BEarer ID

Network Entities

IMEI = MMEGI +MMEC 16 + 8 bit
GUMMEI = MCC + MNC + MMEI
Physical Cell ID 9bit
TAI = MCC + MNC + TAC 32bit

User Equipment

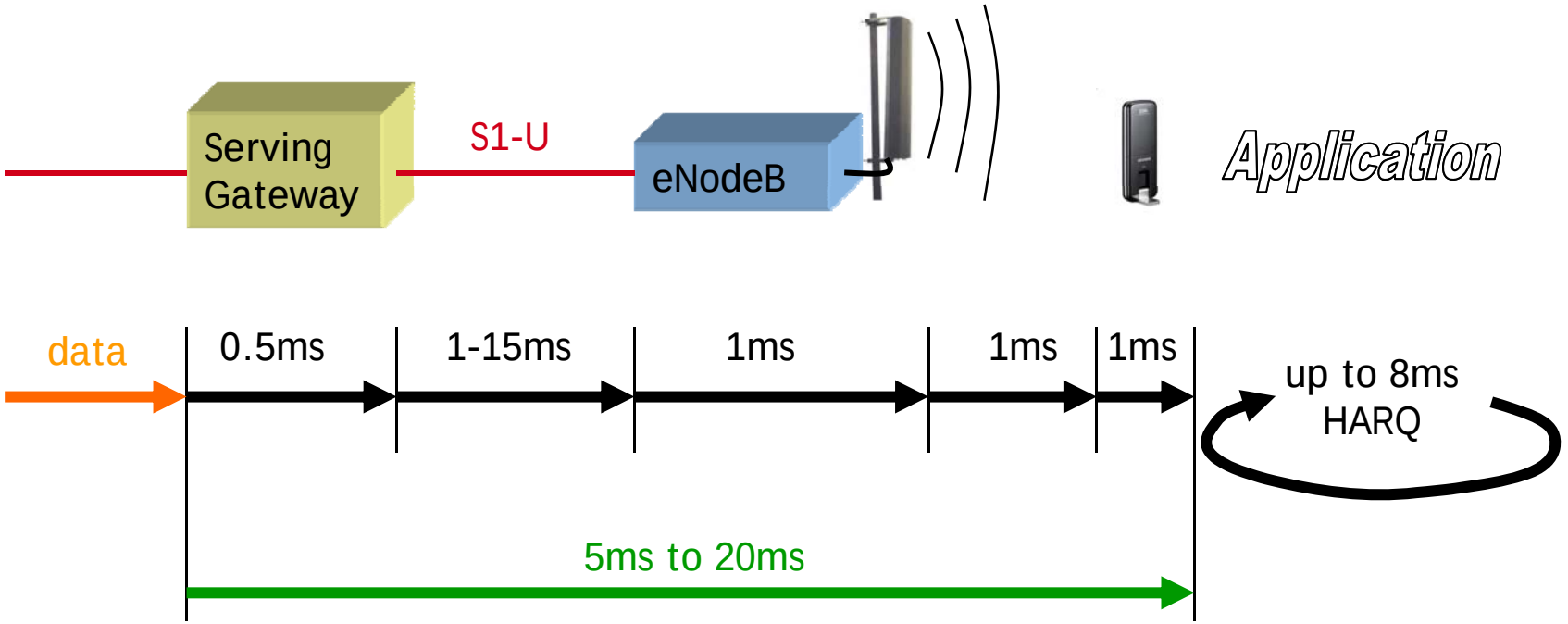
IMSI 60bit
S-TMSI = MMEC + M-TMSI
IMEI 60bit
GUTI = GUMMEI + M-TMSI

E-UTRAN

C-RNTI 16 bit
RA-RNTI 16bit
SI-RNTI 16bit
P-RNTI 16bit
TPC-PUCCH-RNTI 16bit
TPC-PUSCH-RNTI 16bit
Random Value 4bit

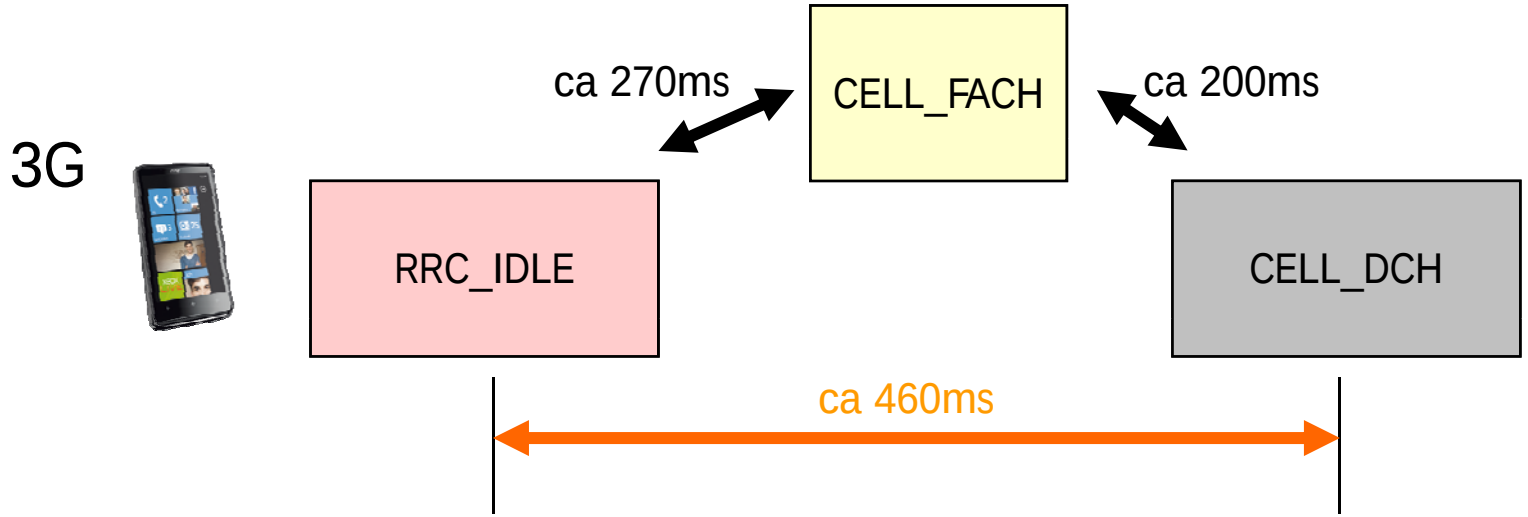
elekom Austria

User Plane Latency



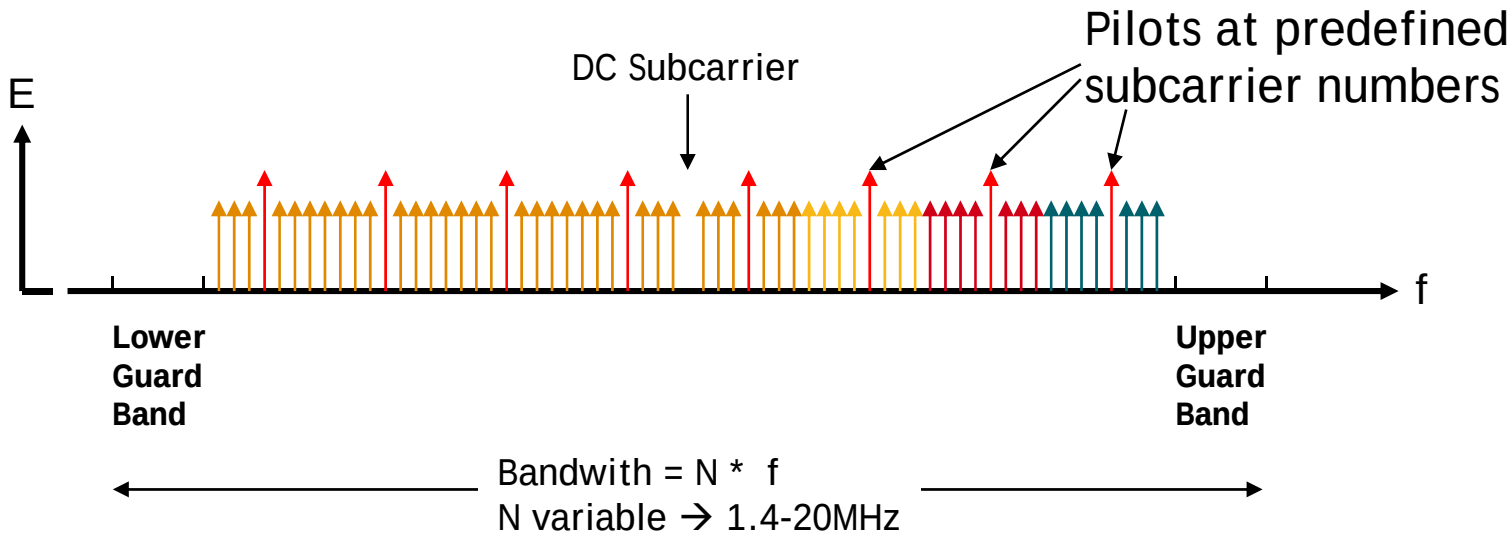
A1 Telekom Austria

Control Plane Latency compared to 3G



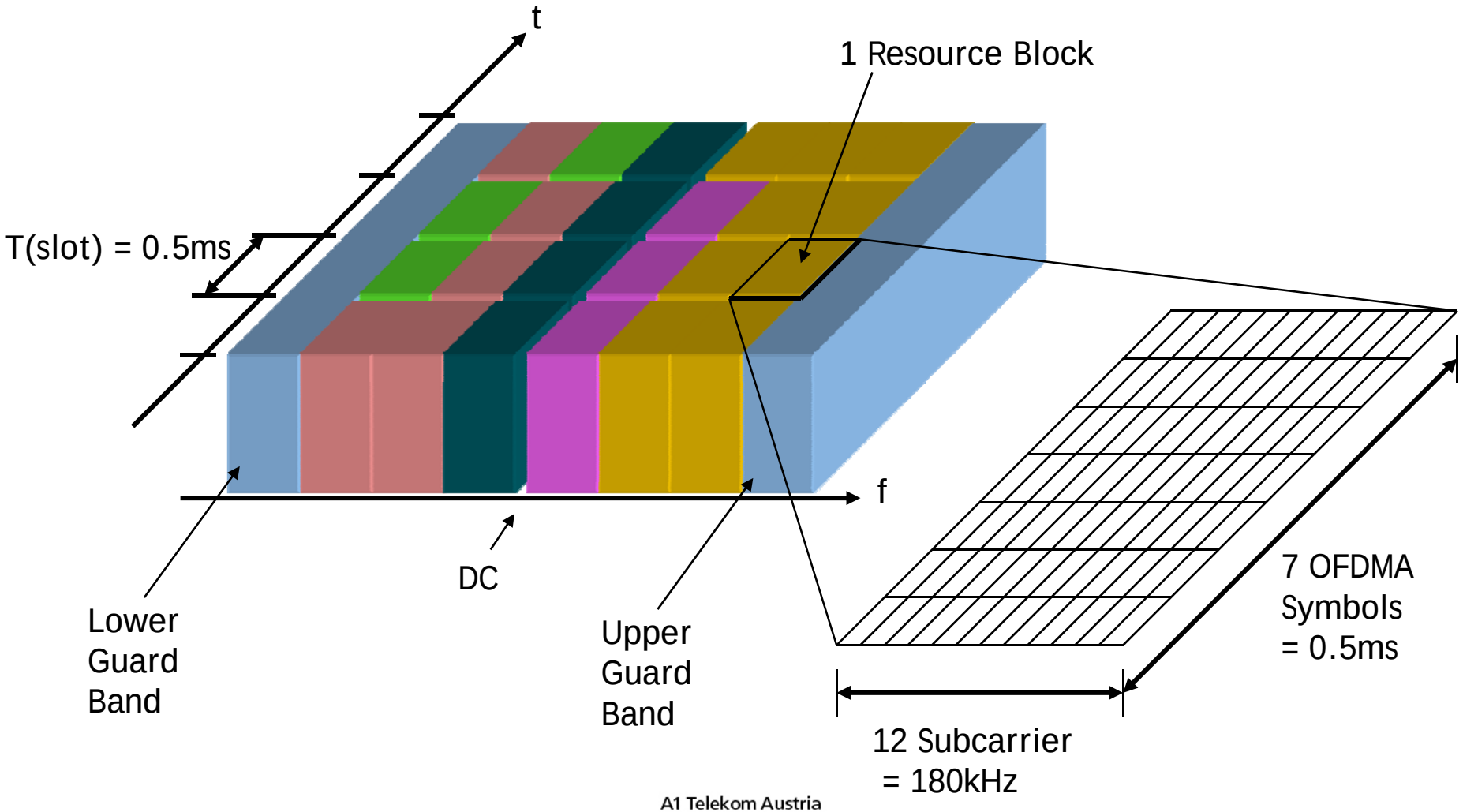
A1 Telekom Austria

DL Spectrum Layout - OFDMA



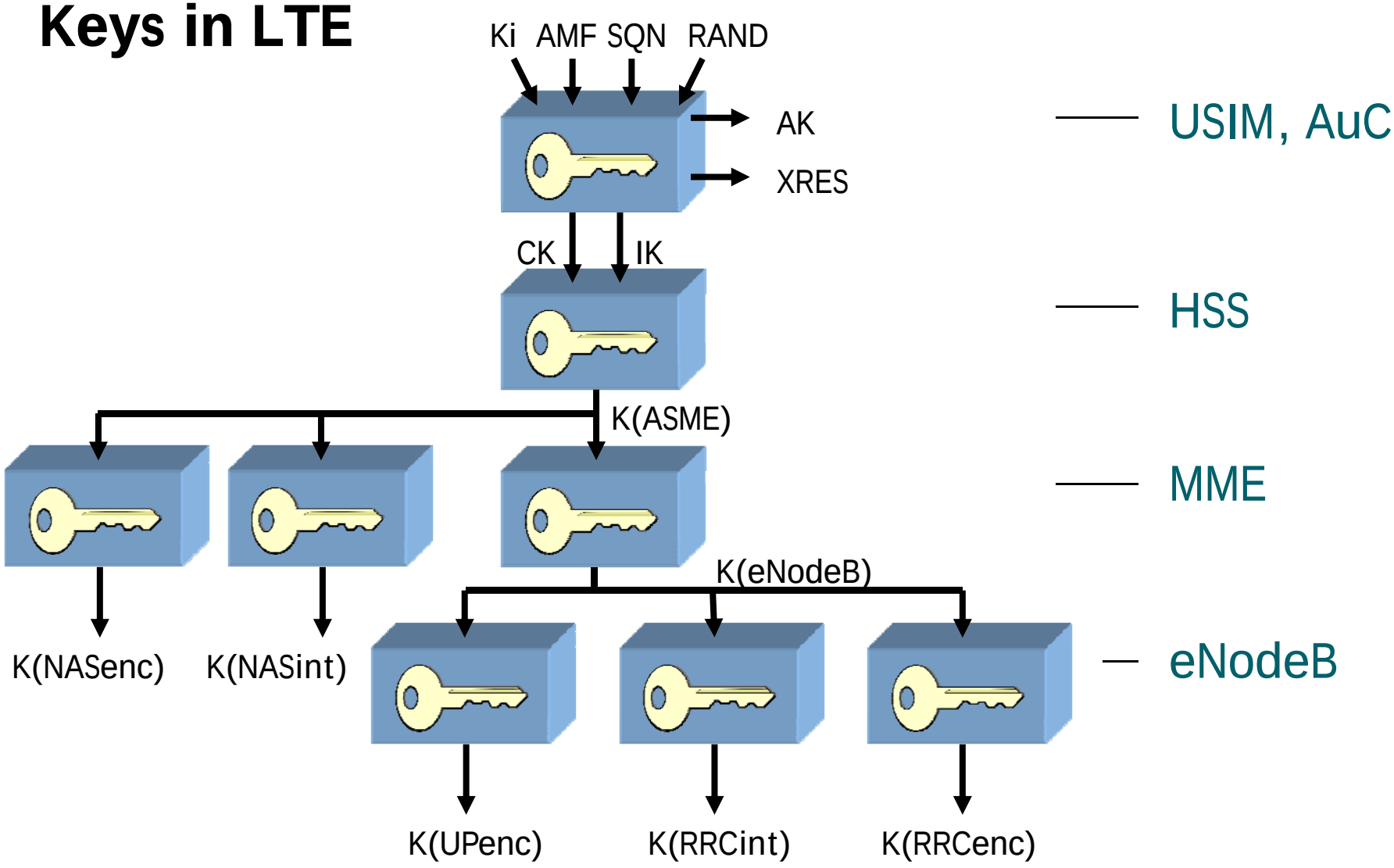
A1 Telekom Austria

DL Resource Element and Resource Blocks



A1 Telekom Austria

Keys in LTE



A1 Telekom Austria

Cryptographic Key Separation

Purpos

Differenciate User Traffic from Signalling
Keys stored in different locations
Key Renewal (Key change on the fly)
Variable Security
More Independence of Radio Interface

Negotiations

2 mandatory sets of Security
- 128-EEA1 and 128-EIA1 based ond SNOW 3G
- 128-EEA2 and 128-EIA2 based on FIPS 197

Supported by all UE, eNodeB and MME
Algorithm negotiated separately between UE and eNodeB
Algorithm negotiated separately between UE and MME (eg. NAS level)
UE Security Capabilities sent in Setup procedure
Algorithm can only change during Handover

A1 Telekom Austria

Security for Voice over LTE

Methods for voice over LTE

IMS over LTE
- IP Multimedia Subsystem is an independent service control architecture

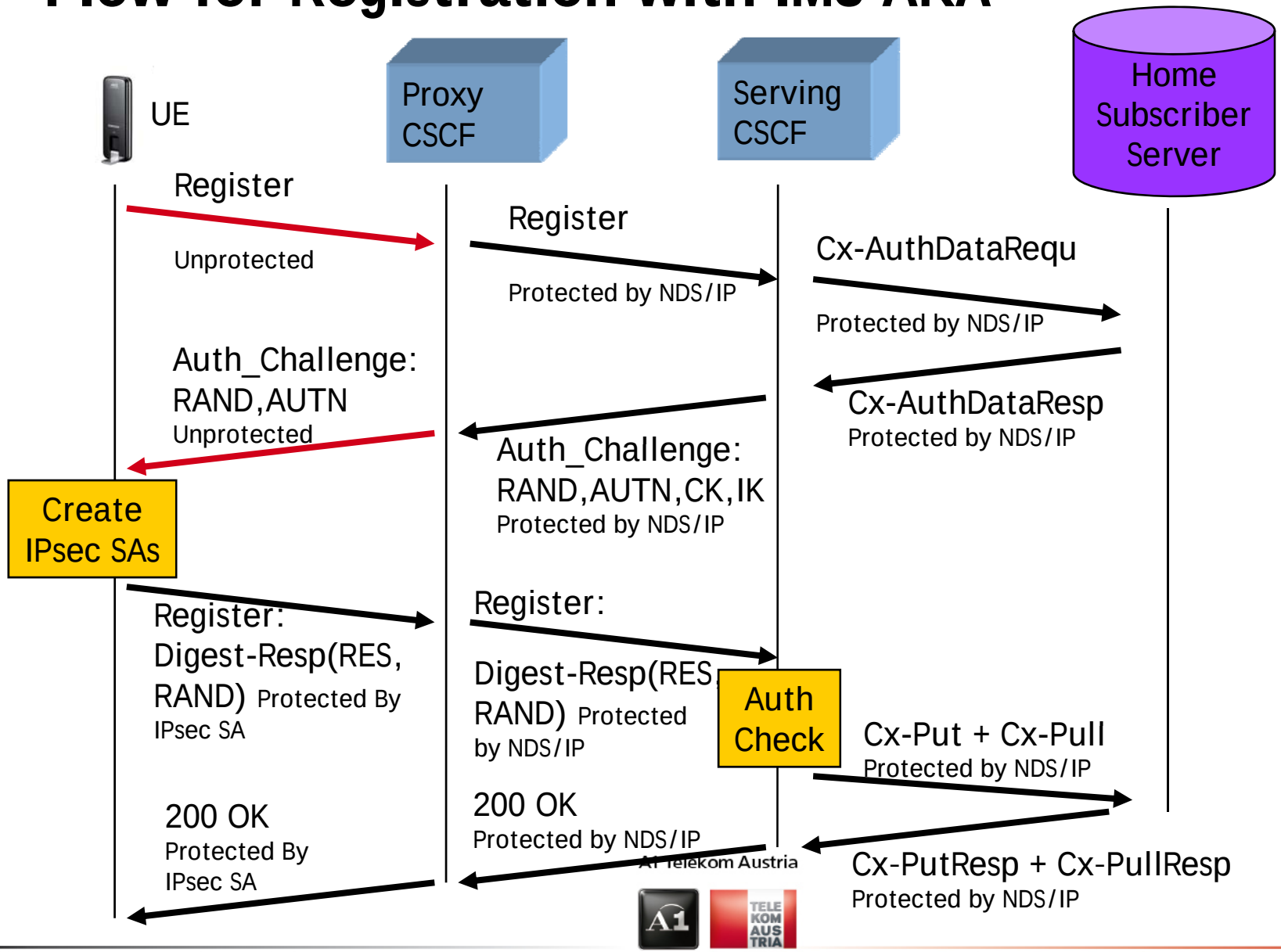
Circuit Switched Fallback (CSFB)
- this provides voice service by fallback from LTE to 3G or 2G (3GPP2-defined networks)

Subscriber Authentication in IMS

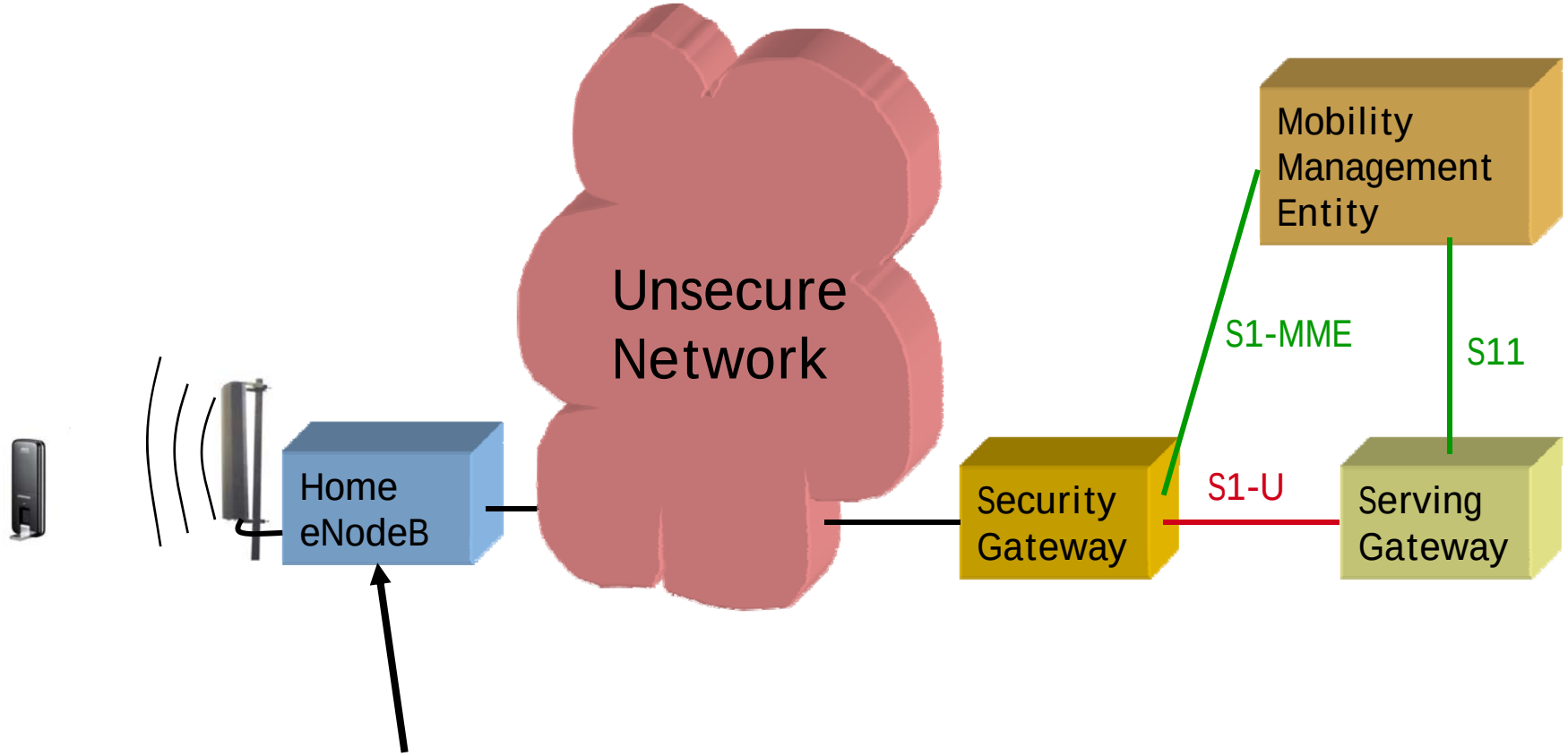
SIP-layer Authentication
Access-Network bundled Authentication
Trusted Node Authentication

A1 Telekom Austria

Flow for Registration with IMS AKA



Security for Home Base Station Deployment

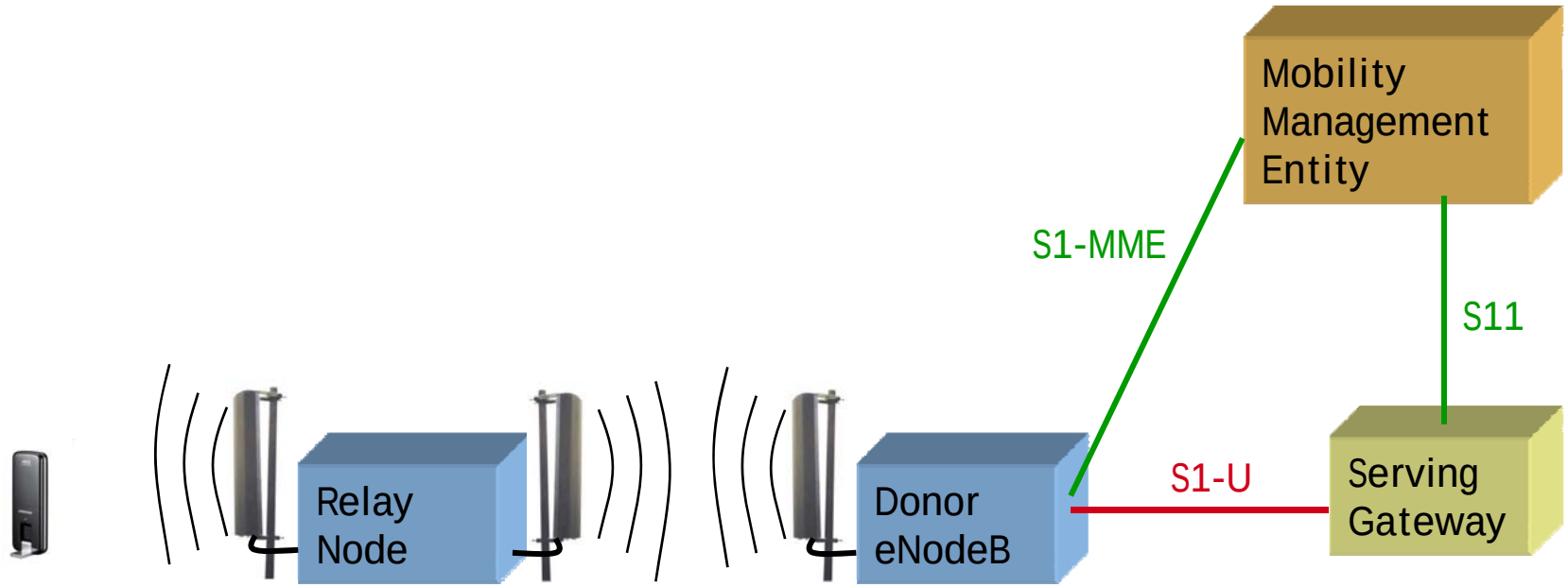


A1 Telekom Austria

User plane

Contrrol plane

Security for Relay Node Architecture



Still under study to prevent possible threats

A1 Telekom Austria

User plane

Contrrol plane

Speaker

Dipl.-Ing. Herbert Koblmiller
Mobile Network Planning
Optimisation & Network Performance

A1 Telekom Austria AG
Obere Donaustraße 29 1020 Wien

herbert.koblmiller@a1telekom.at