SECURITY IN 5G INTER-NETWORK SIGNALLING

Stefan Schröder
Telekom Security

LIFE IS FOR SHARING.

SECURITY IN 5G INTER-NETWORK ~~SIGNALLING~~ API CALLS

Stefan Schröder
Telekom Security

LIFE IS FOR SHARING.

5G SERVICE BASED ARCHITECTURE (SBA)

01	Where we are:	Current situation
02	Where we go:	Network service bus
03	What we send:	The 5GC protocol stack
04	What we want:	SA3‘s goals for SBA
05	What we hear:	Agenda for today

01 WHERE WE ARE:
CURRENT SITUATION

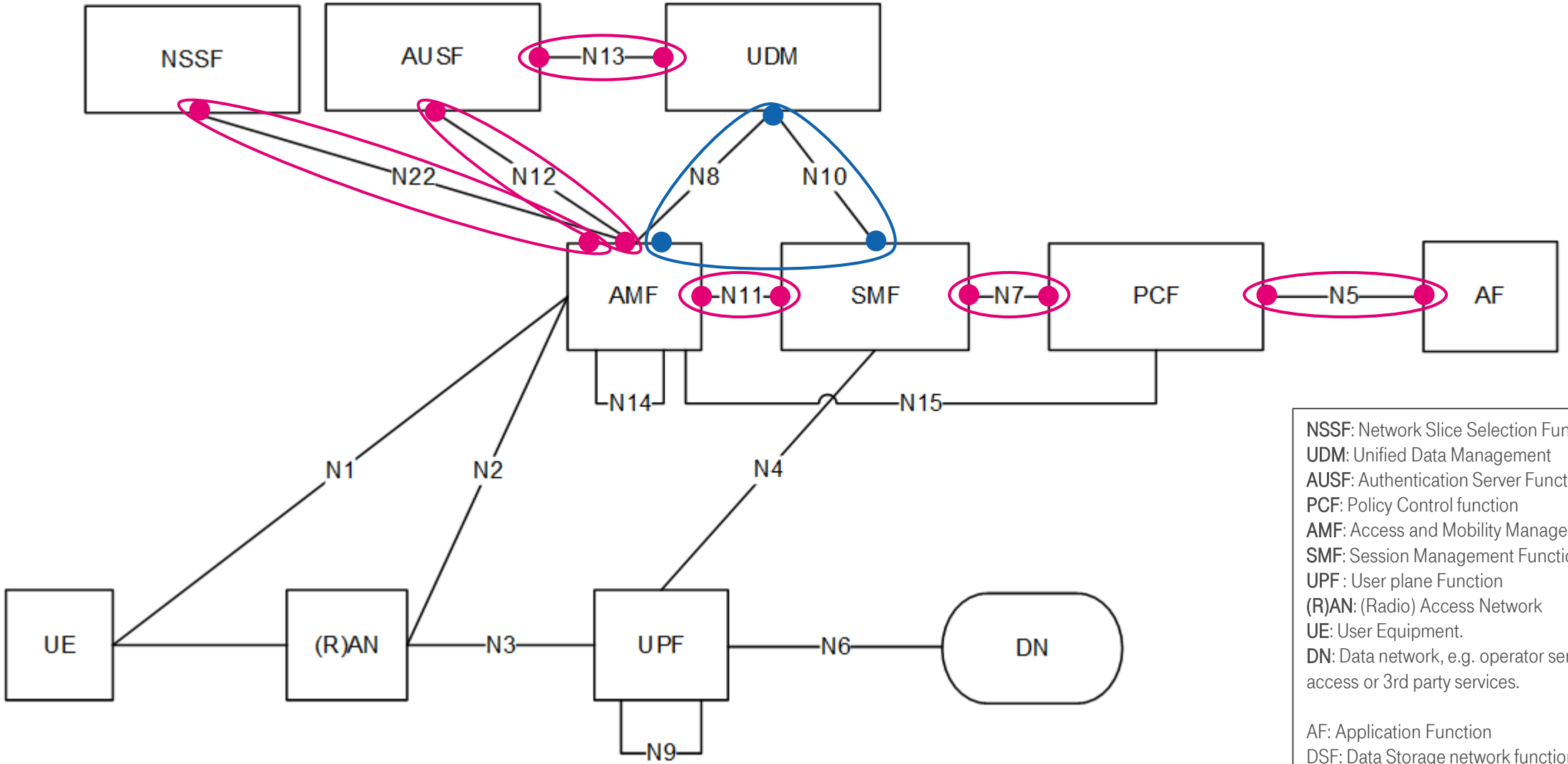
MARCH 2018: ENISA STUDY ON SIGNALLING SECURITY

Some citations from the study:

- "Wild West" running on legacy infrastructure
- Consider revising the current legal landscape
- [in 5G] grace period between vulnerability discovery and real exploitation will become much shorter compared to SS7 and Diameter

Sources: Heise.de, Telecoms.com, Internetofbusiness,com

3GPP RELEASE 15 – 5G REFERENCE POINT REPRESENTATION



NSSF: Network Slice Selection Function
UDM: Unified Data Management
AUSF: Authentication Server Function
PCF: Policy Control function
AMF: Access and Mobility Management Function
SMF: Session Management Function
UPF : User plane Function
(R)AN: (Radio) Access Network
UE: User Equipment.
DN: Data network, e.g. operator services, Internet access or 3rd party services.

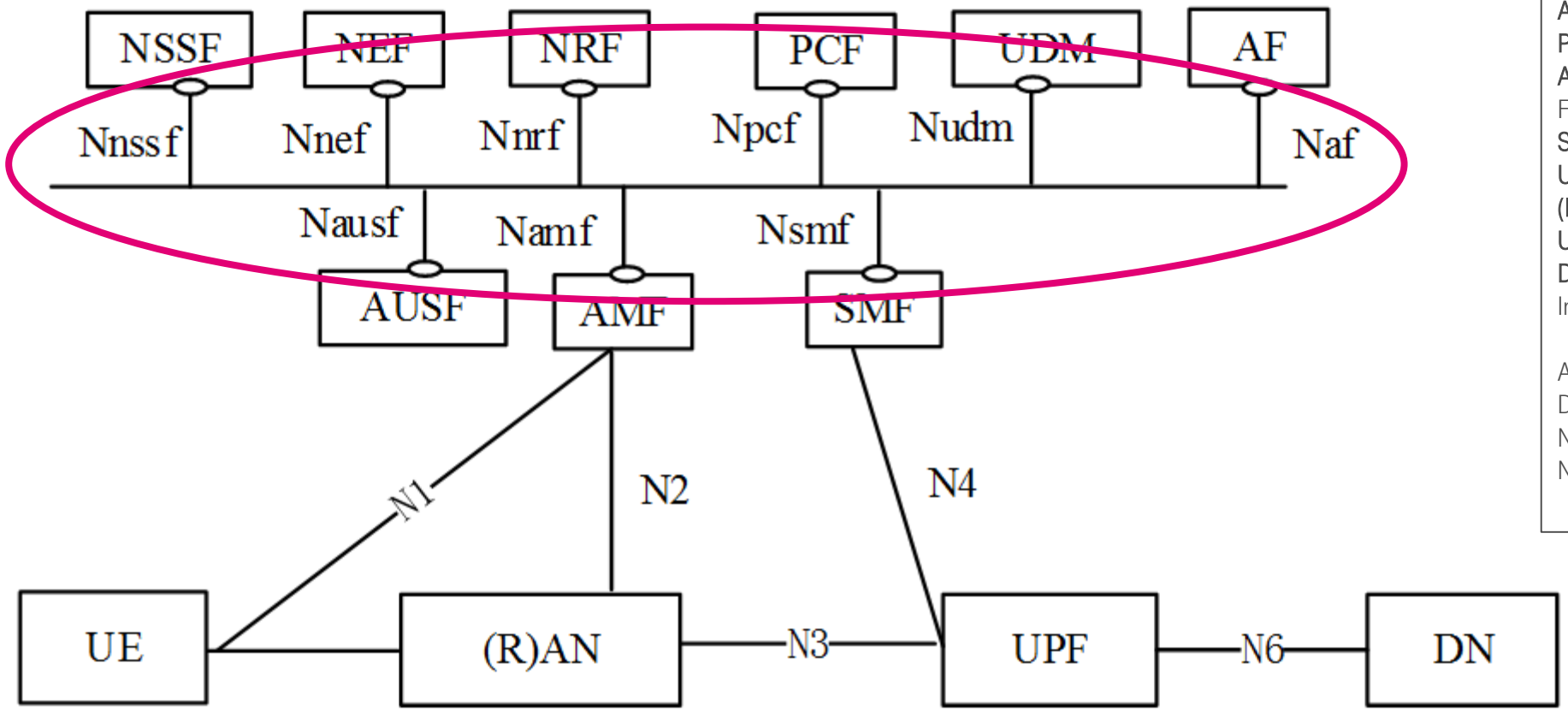
AF: Application Function
DSF: Data Storage network function.
NEF : Network Exposure Function
NRF: NF Repository Function

MAIN IDEAS OF REFERENCE POINTS

- Point-to-point communication within the core network
- Well-defined interfaces for certain data exchanges
- Pre-5G: different signalling protocols (MAP, RADIUS, GTP-C, ...)
- Monolithic conception of network functions
- Tight coupling of network functions, statically configured security
- Fine-grained network segmentation possible

02 WHERE WE GO:
NETWORK SERVICE BUS

3GPP RELEASE 15 – SERVICE-BASED REPRESENTATION



NSSF: Network Slice Selection Function
UDM: Unified Data Management
AUSF: Authentication Server Function
PCF: Policy Control function
AMF: Access and Mobility Management Function
SMF: Session Management Function
UPF : User plane Function
(R)AN: (Radio) Access Network
UE: User Equipment.
DN: Data network, e.g. operator services, Internet access or 3rd party services.

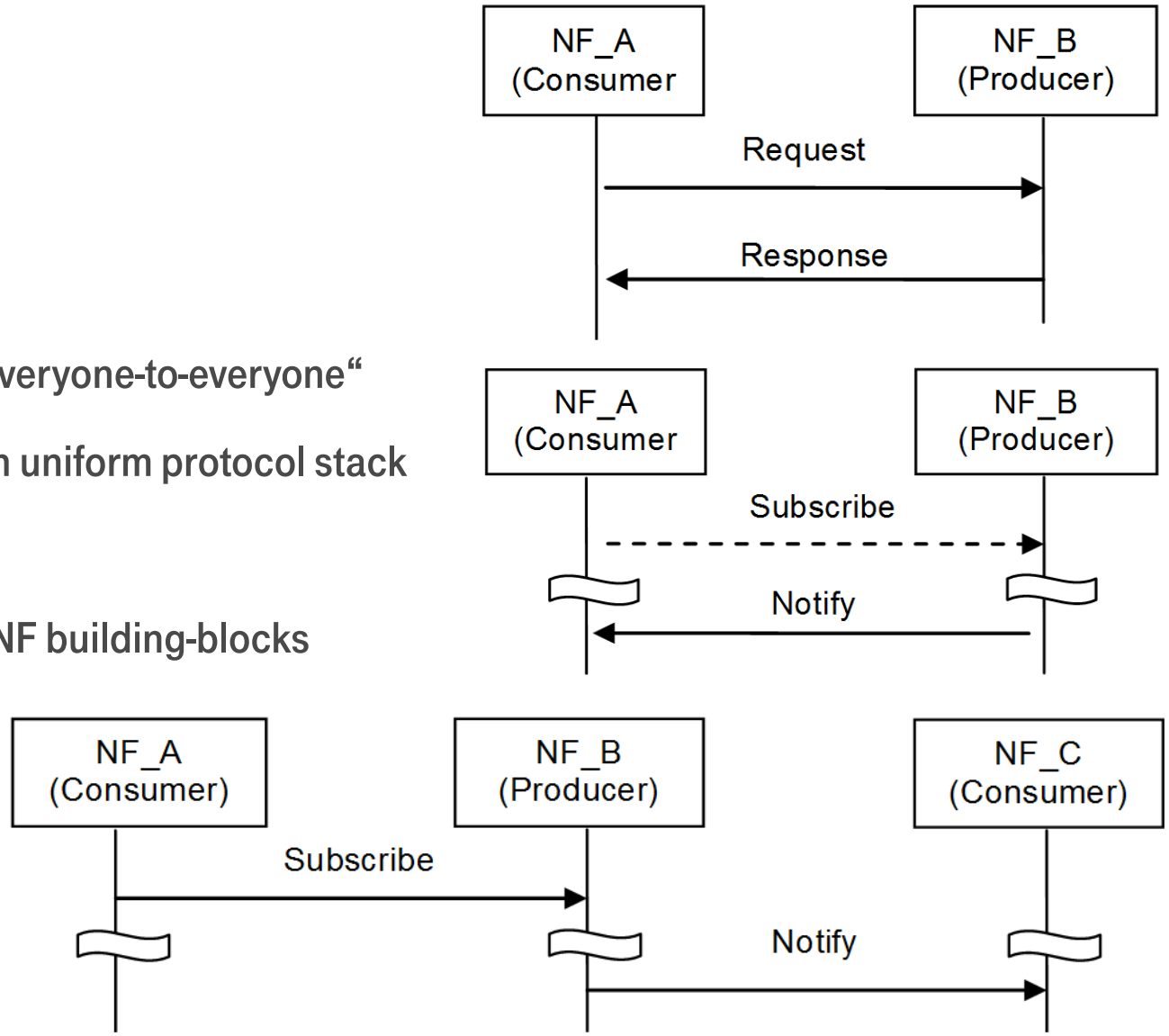
AF: Application Function
DSF: Data Storage network function.
NEF : Network Exposure Function
NRF: NF Repository Function

SBA: Service Based Architecture

SBI: Service Based Interfaces

MAIN IDEAS OF SBA

- Replace signalling messages by API calls
- Core network = logically-uniform service bus
- No longer point-to-point communication, but „everyone-to-everyone“
- Well-defined interfaces for available services on uniform protocol stack
- Network Functions in the cloud
- Consumer/Producer model: easily deployable NF building-blocks
- Basic NF service interactions:
  - Request/Response
  - Subscribe/Notify (Me)
  - Subscribe/Notify (Someone else)



03 WHAT WE SEND:
THE 5GC PROTOCOL STACK

THE 5GC PROTOCOL STACK

ACCORDING TO 3GPP TS 29.50X

TCP	▪ De-facto industry standard for HTTP web services ▪ More widespread than SCTP ▪ Redundancy and load balancing via “cloudification magic”
HTTP/2	▪ Binary framing ▪ Multiplexing of requests over the same connection ▪ Header compression
JSON	▪ Serialization data format for the 3GPP 5GC protocol information elements (IE) ▪ De-facto industry standard for web services ▪ Simple, straightforward specification, immense tooling

RELATED CONCEPTS

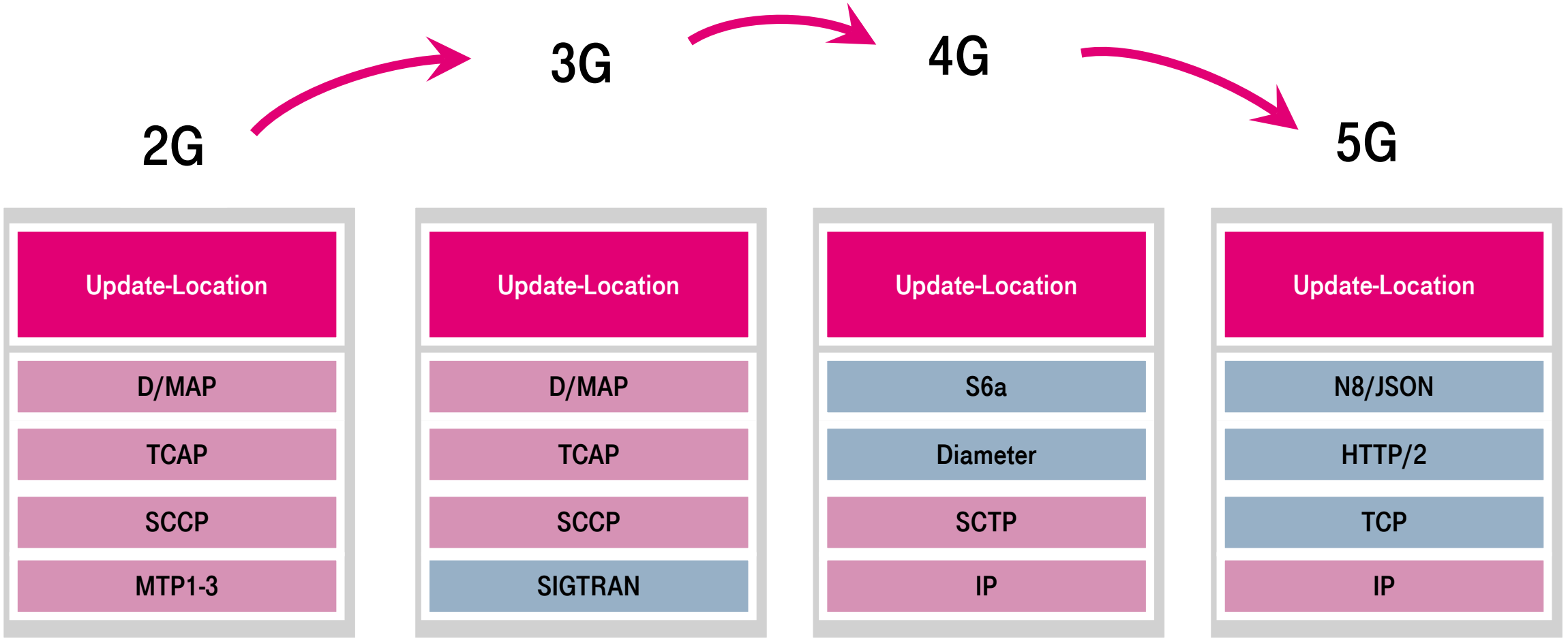
ADOPTED BY 3GPP ARCHITECTURE AND CORE NETWORK GROUPS

RESTful services	▪ Client/Server communication ▪ URL-addressable resources ▪ Uniform HTTP-interface ▪ Statelessness + Cacheable responses (?)
OpenAPI specification (aka Swagger)	▪ RESTful API description language ▪ Open source collaborative project by the Linux Foundation ▪ JSON object, represented either in JSON or YAML format
Two HTTP client-server pairs	▪ Necessary in Subscribe/Notify scenarios ▪ Subscriber to inform Notifier about receiving endpoint

REST: Representational State Transfer

PROTOCOL EVOLUTION

EXAMPLE: UPDATE LOCATION REQUEST



04 WHAT WE WANT:
SA3 GOALS FOR SBA

SECURITY GOAL #1 FOR RELEASE 15

Message origin authentication

"Who is the real sender?"

Message protection (integrity /confidentiality)

"Was the message modified/read?"

Standardize all of these aspects in 5G

Cross-layer anti-spoofing enforcement

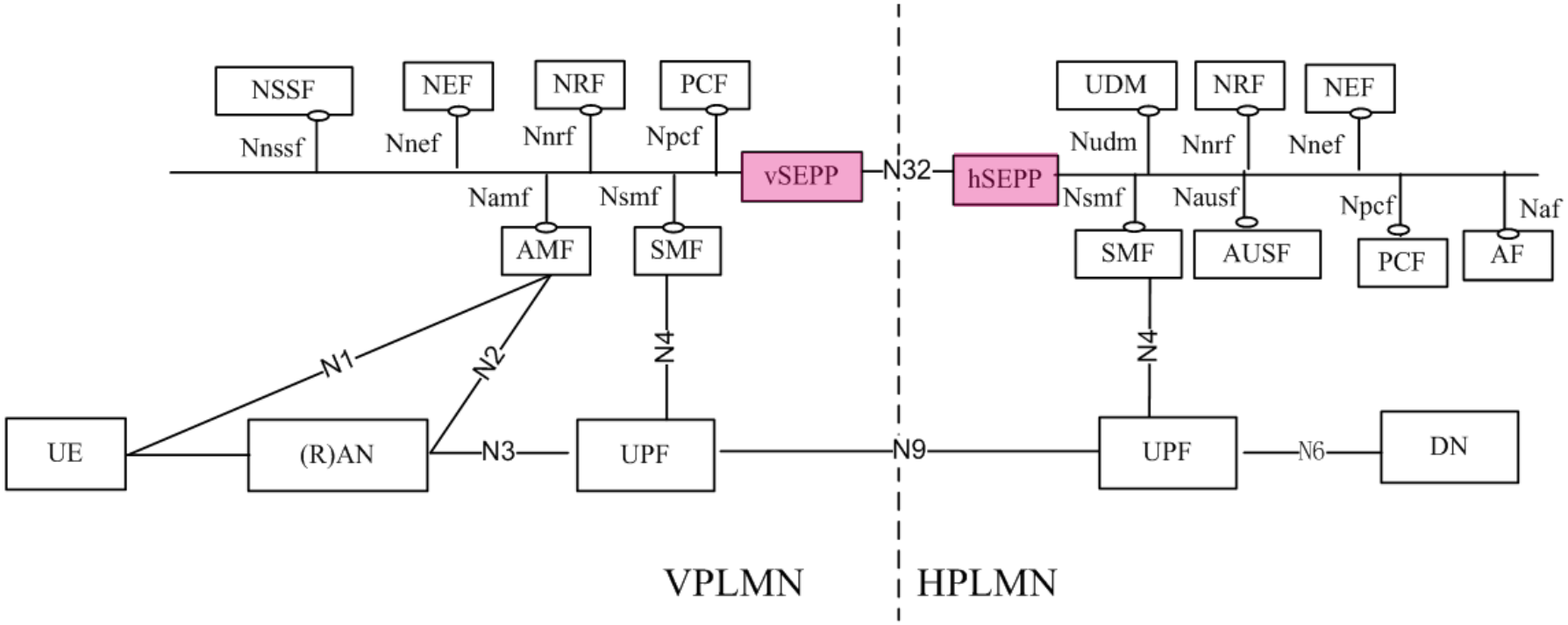
"Do identities used on different protocol layers all belong to the same sender?"

Message content authorization

"Is the consumer legitimized to request or be subscribed to a specific service?"

SECURITY GOAL #3 FOR 3GPP RELEASE 15

A 5G signalling edge proxy is required to protect traffic crossing a security domain boundary, and thus needs to be included in the architecture.



SEPP: Security Edge Protection Proxy

05 WHAT WE‘LL HEAR:
AGENDA FOR TODAY

AGENDA PART 1

09:00	**Session 2: Security in 5G Inter-Network Signalling** **Session Chair: Stefan Schroeder, T-Systems** 09:00 Presentation on SBA: introduction of the topic and current status in SA3 Stefan Schroeder, T-Systems 09:20 5G Inter-PLMN security: The trade-off between security and the existing IPX business model Ewout Pronk, KPN on behalf of GSMA Diameter End to End Security Subgroup 09:40 Secure Interworking between networks in 5G Service Based Architecture Silke Holtmanns, Nokia Bell Labs
10:00	**Coffee Break**

AGENDA PART 2

10:30	**Session 2: Security in 5G Inter-Network Signalling (continuation)** **Session Chair: Stefan Schroeder, T-Systems** 10:30 Security Best Practises using RESTful APIs Sven Walther, CA Technologies 10:50 Identifying and Managing the Issues around 5G Interconnect Security Stephen Buck, Evolved Intelligence 11:10 Zero Trust Security Posture in 5G Architecture Galina Pildush, Palo Alto Networks 11:30 Questions & Answers with all Session 2 Speakers and the Audience led by Stefan Schroeder, T-Systems
12:00	**Workshop Wrap up: 5G Phase 1 Conclusions and Outlook Towards Phase 2** Stefan Schroeder, T-Systems – Bengt Sahlin, Ericsson
12:30	**Close of the event - Lunch Break**