MOBILEUM

5G SEPP

Contents

- 5G overview
- Mobileum integrated firewall / SEPP

5G signalling (API) – protocol stack

JSON	Serialisation data format for 3gpp information elements De-facto standard for web services Straightforward to specify. Widely available tooling.
HTTP/2	Binary framing Multiplexing requests Header compression
TCP	De-facto standard for web services More widespread than SCTP Redundancy and load balancing via “cloud magic”

Protocol evolution

2G	3G	4G	5G
Update Location	Update Location	Update Location	Update Location
MAP	MAP	S6a	JSON (N8/N32)
TCAP	TCAP	Diameter	HTTP2
SCCP	SCCP	SCTP	TCP
MTP	SIGTRAN	IP	IP

Parameters	Mostly fixed	Mostly fixed	Flexible AVPs	Free text
E2E security	Not used	Not used	Not used	Being defined
Session	TCAP dialogue	TCAP dialogue	Diameter Req/Resp (id)	Http Req/resp (id)
E2E routing	Global title	Global title	Host/realm route record	Host

5G interconnect security requirements

- Encryption of sensitive parameters not needed by IPX
  - E.g. SUPI/IMSI, keys, (location)
- Protection against replay attacks
- Integrity of message
- Authentication of sender
- For IPX (i.e. outsource routing, billing, services)
- Ability to modify parameters (as allowed by operators)
- Log of IPX making changes
- Integrity of message

Authentication

Who is the real sender?

Integrity

Was the message /parameter modified?

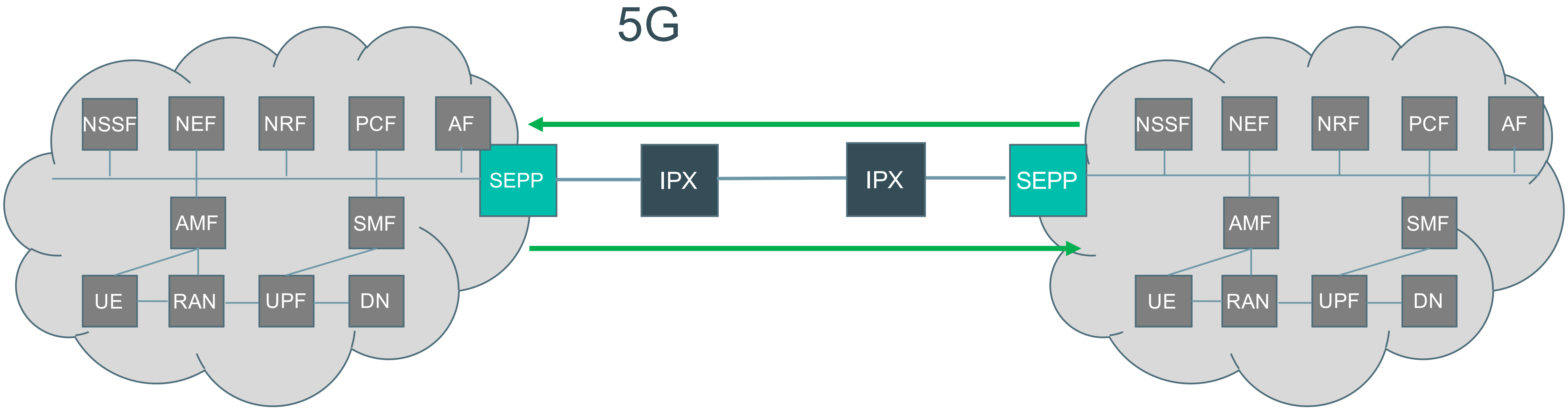
Replay protection

Can a message be recorded and replayed

Confidentiality

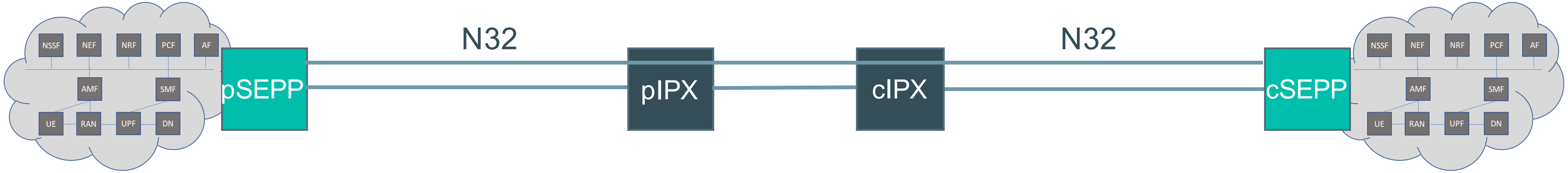
Can the message /parameter be read

Routing evolution and risks



- Defence – protection not implication
  - End to End encryption and authentication
- IPX needs to inspect and modify messages
  - Provide commercial benefit particularly to smaller operators
  - Roaming hub – i.e. Merge small operator to “look” the same
  - Roaming services – e.g. VHE, Sponsored roaming

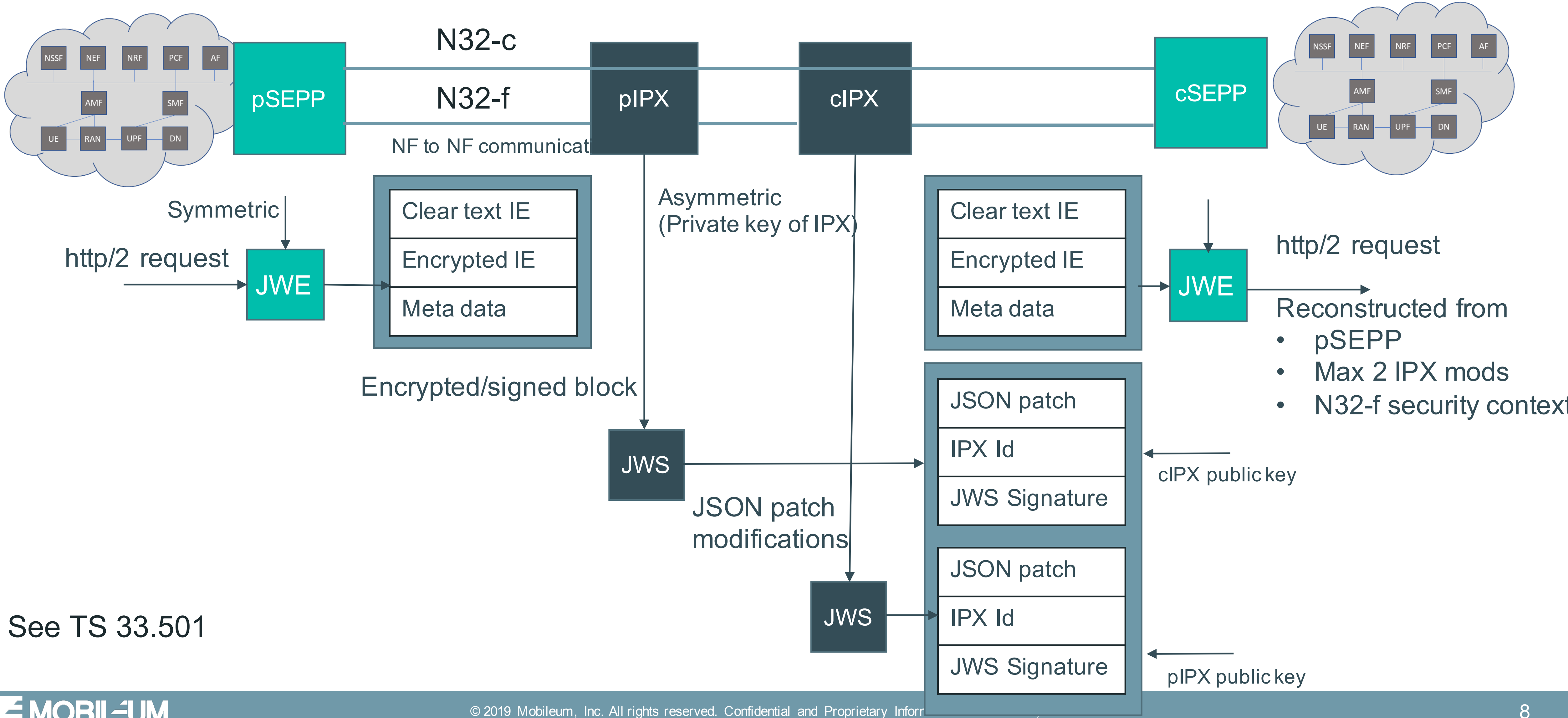
5G interconnect security overview



SEPP – Provides encryption, integrity and authentication

- SEPPs authenticated using TLS (N32-c)
  - Negotiate cipher suites for messages over interconnect
  - Exchange protection policies per NE roaming partner – what is encrypted
    - E.g. SUPI, location, keys, authorisation tokens
  - Policies on what can be modified per IPX and per roaming partner
- SEPPs encrypt and sign all messages over N32-f using JOSE (JSON web signing encryption)
  - Using JWE – JSON web encryption & signature (with symmetric key from TLS key export)
- IPX modify, append and sign changes
  - Using JWS JSON web signature (IPX private key from client PLMN)

5G interconnect security overview (N32)



Reconstructed from

- pSEPP
- Max 2 IPX mods
- N32-f security context

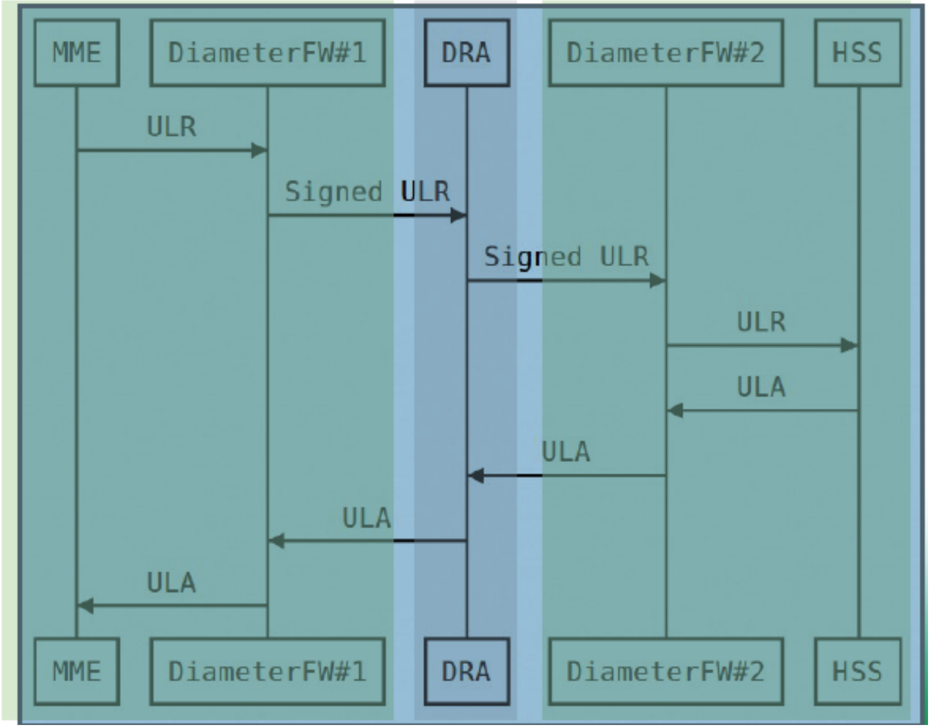
See TS 33.501

5G Summary

- SEPP secures 5G interconnect – encryption, integrity and authentication of signalling
- Improves security of interconnect versus 2G/3G and 4G
- Additional to firewall and potentially combined
- Enables IPX business model, but allows operators to control what is modified

4G retrofit - DESS

- DESS Diameter end to end security (i.e. encryption/authentication on Diameter)
- Add for SMS interface initially
- New AVPs
  - Signing realm
  - Signature
  - Encrypted container
- Discussion still on encryption / discovery

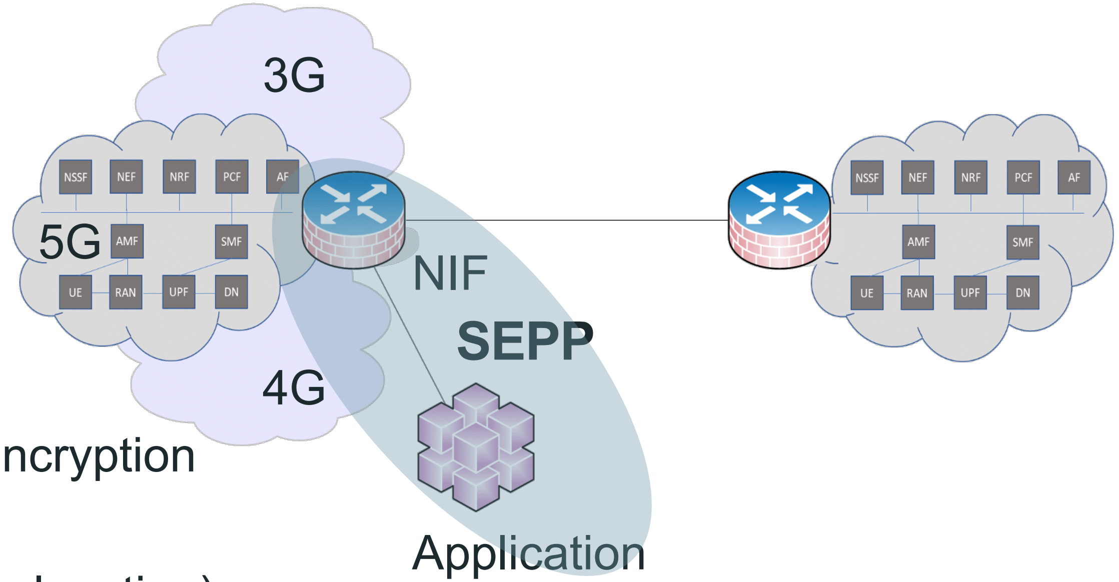


Contents

- 5G overview
- Mobileum integrated firewall / SEPP

Mobileum SEPP

- SEPP
  - As per 23.501
  - N32c and N32f
  - Authentication, Encryption and key exchange
- Combined SEPP and 3G/4G/5G firewall
  - 5G firewall – i.e. rules AND SEPP authentication/encryption
  - Consistency and state/location checks
  - Cross protocol correlation (e.g. service information, location)
- Support for DESS (once defined)
  - i.e. Encryption and authentication on 4G (diameter) signalling
- Available 2020
- Common architecture with 2G/3G/4G (i.e. NIF / application / data analytics



MOBILEUM

THANK YOU