Evolved Intelligence

Innovation in an interconnected world

Identifying and managing the issues around 5G interconnect security

Stephen Buck

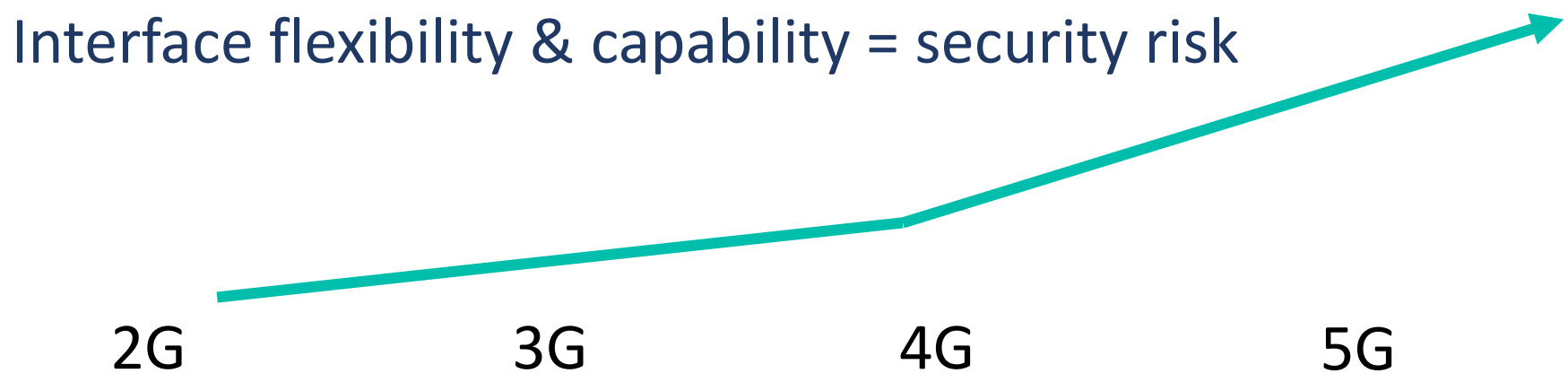
Stephen.buck@evolved.intelligence.com

Evolved Intelligence

- Leaders in 2G/3G and 4G signalling firewall
- Leaders in roaming value added services and analytics
- Supply both
  - Interconnect/IPX providers (e.g. Syniverse, Comfone etc)
  - Operators (e.g. DTAG, Orange, Vodafone etc)
- Active in GSMA

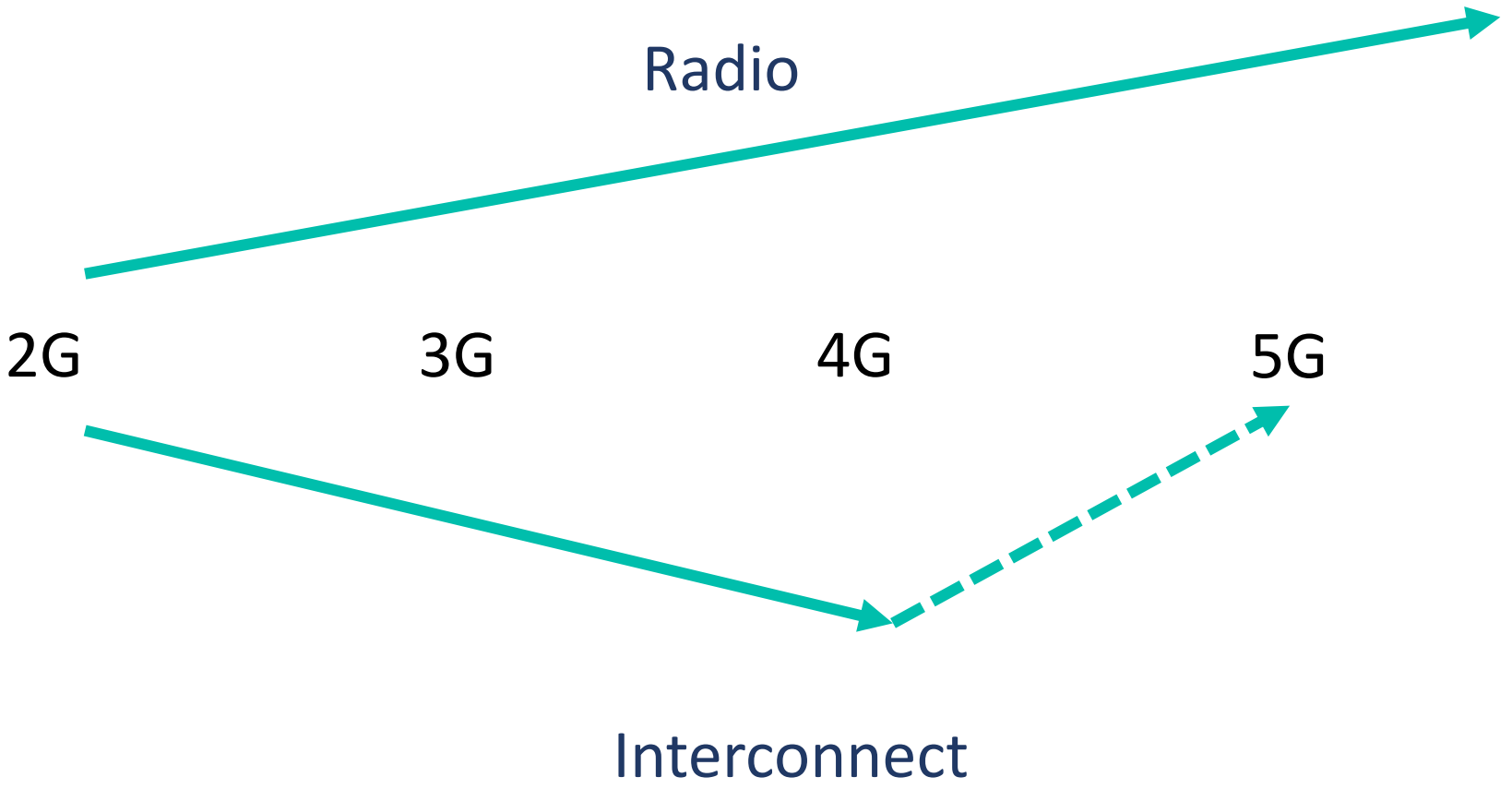
Security threats

Evolved Intelligence



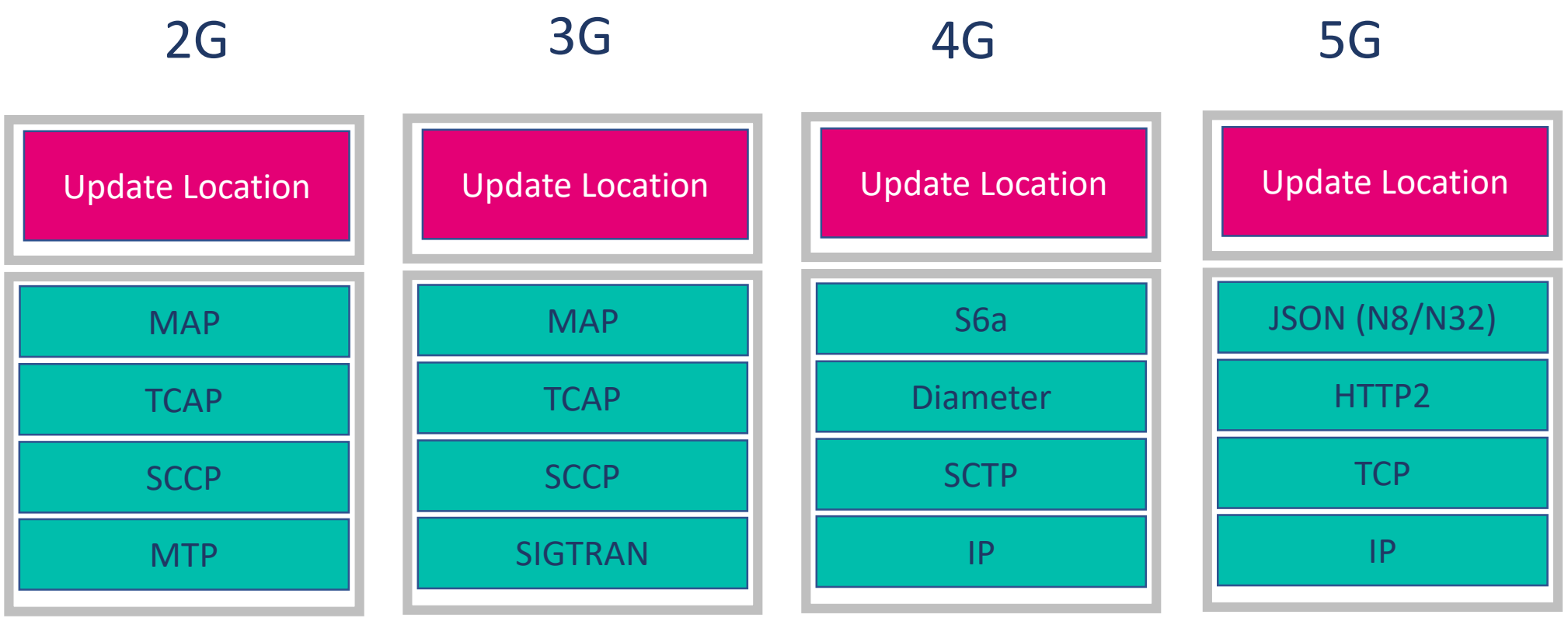
- 5G service based architecture and exposed web services
- Necessary for new business models
- Opens up new risks

Security trends



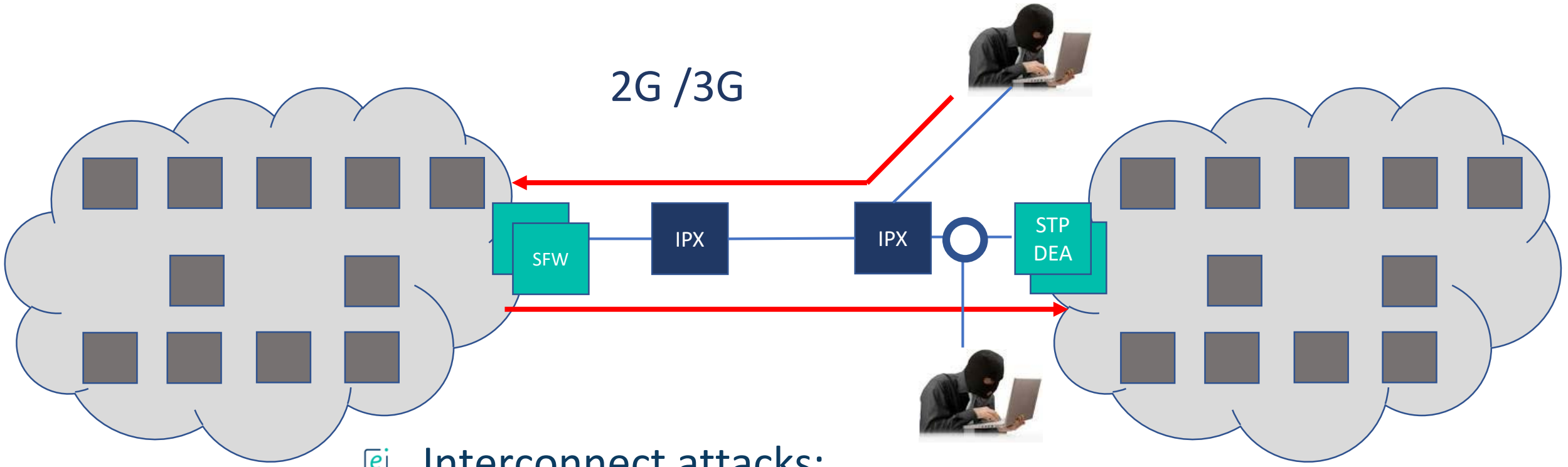
Protocol evolution

Evolved Intelligence



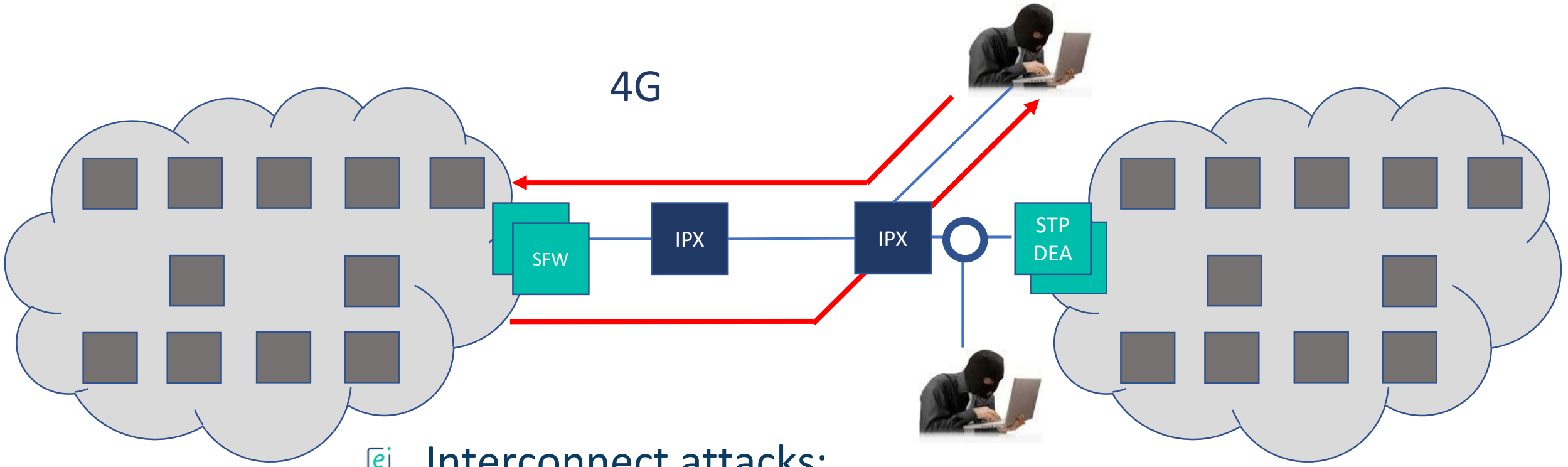
Parameters	Mostly fixed	Mostly fixed	Flexible AVPs	Free text
E2E security	Not used	Not used	Not used	Being defined
Session	TCAP dialogue	TCAP dialogue	Diameter Req/Resp (id)	Http Req/resp (id)
E2E routing	Global title	Global title	Host/realm route record	Host

Routing evolution and risks



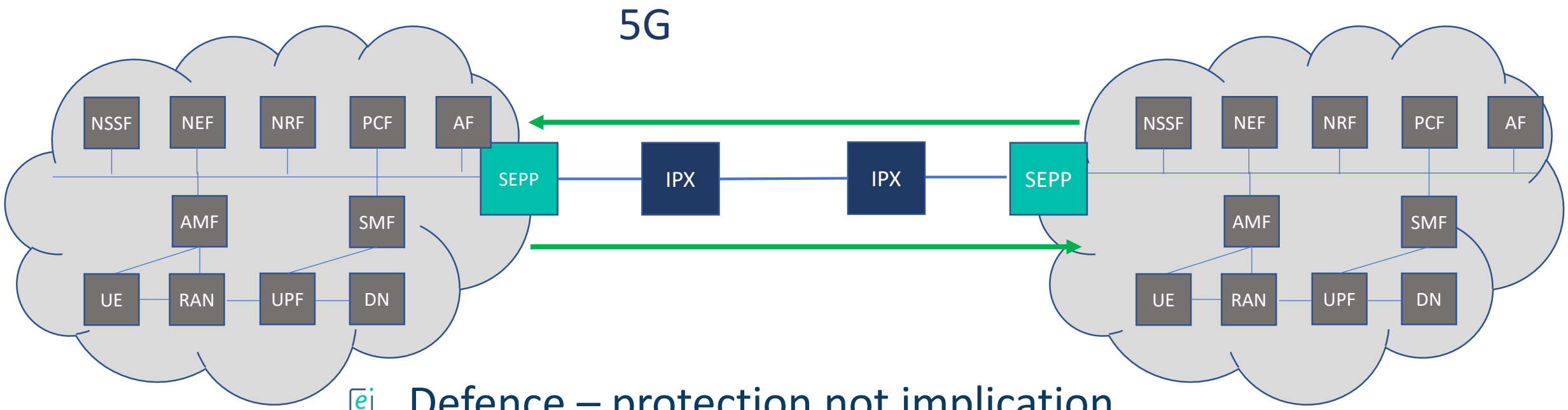
- Interconnect attacks:
  - Insert messages – intercept, track, deny service
    - E.g. Fake Location update, Fake reset
  - Snoop – monitor subscriber information
- Defence
  - Firewall – interprets what is valid message (e.g. consistency, location, velocity etc)

Routing evolution and risks



- Interconnect attacks:
  - Insert messages – intercept, track, deny service
    - E.g. Fake Location update, Fake reset
  - Snoop – monitor subscriber information
- Defence
  - Firewall – interprets what is valid message. Harder to spot spoof.

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

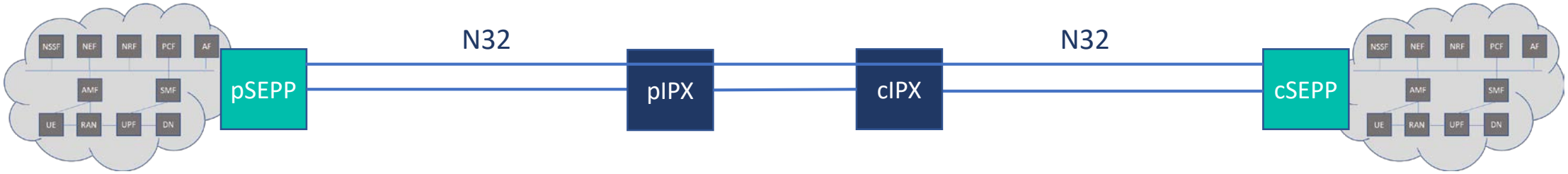
5G interconnect security requirements

- 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

5G interconnect security overview

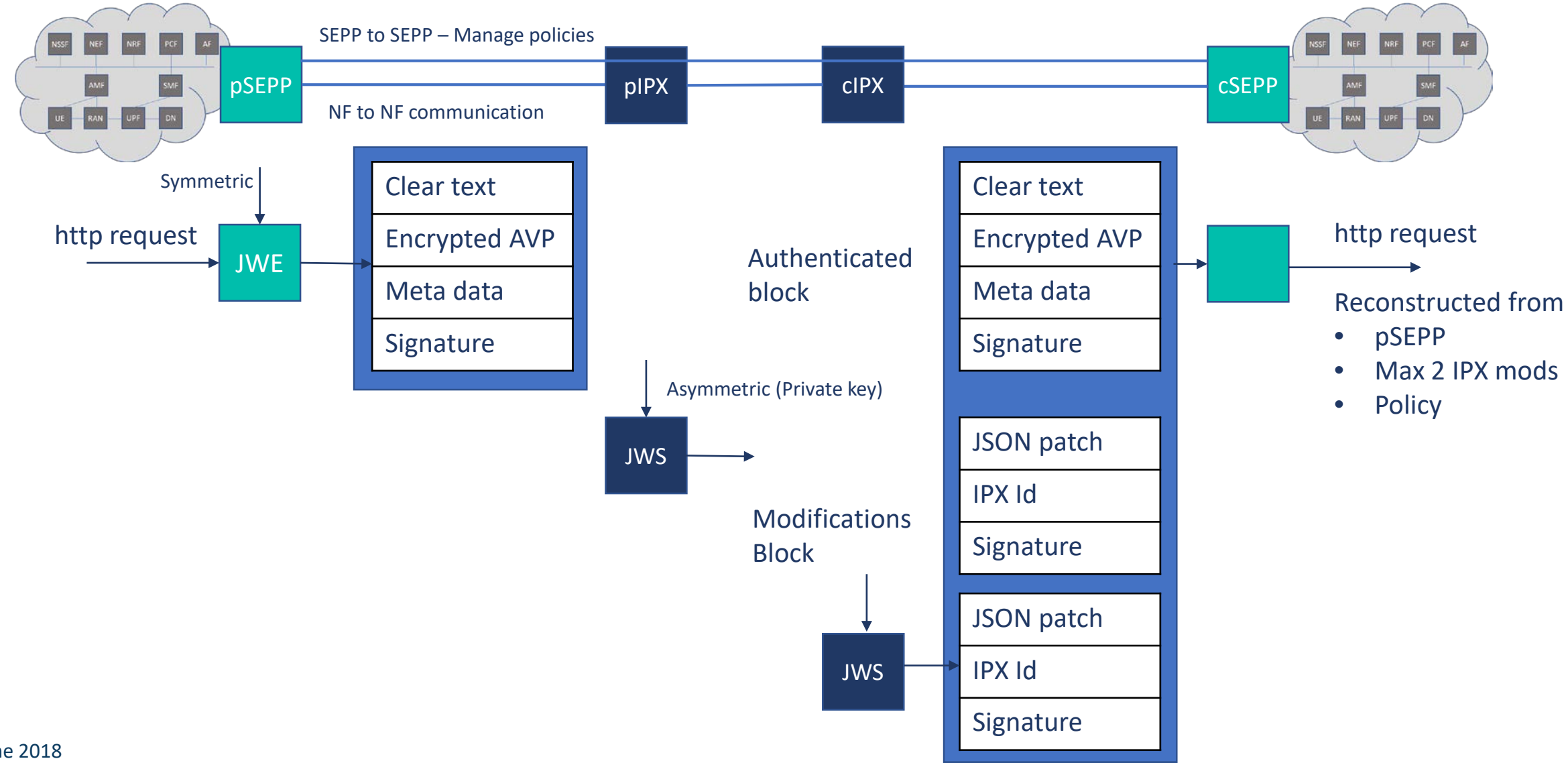


- SEPP – Provides encryption, integrity and authentication

- SEPPs authenticated using TLS
  - Negotiate cipher suites for messages over interconnect (N32)
  - Exchange protection policies per NE and roaming partner – what can be modified
- SEPPs encrypt and sign all messages over N32 using JOSE (JSON web signing encryption)
  - Using JWE – JSON web encryption & signature (with symmetric key from TLS key exchange)
- IPX modify, append and sign changes
  - Using JWS JSON web signature (IPX private key from client PLMN)

5G interconnect security overview

Evolved Intelligence



Summary

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