5G Security
Drivers, Challenges and Opportunities

Stefan Covaci

Agentscape AG

5GinFIRE.eu

contact@5GinFIRE.eu

5GinFIRE

5GINFIRE is a three years Research and Innovation action / project under the EU program Horizon 2020 (Grant Agreement no. 732497) started on 1 January 2017.

Overview

- 5G Security Drivers
- 4G to 5G Security Evolution
- 5G security Challenges and Opportunities

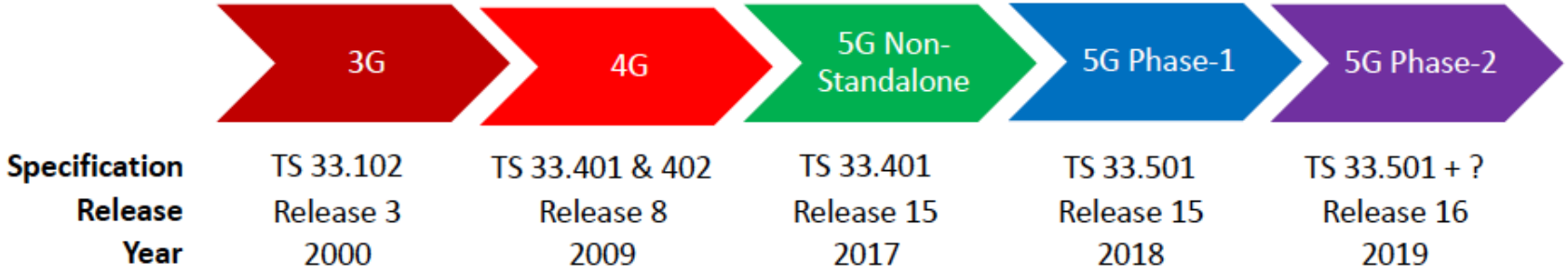
5G Security Drivers

- Pressure from Business and Regulatory stakeholders
  - Digitalisation, supply chains,
  - Liability, reputation, trust-building
- User Privacy awareness
- 5G is about (enabler of) Use Cases, supporting new type of devices and business models -> new trust model
- New service delivery model
- Attack surface grows with 5G
  - IoT devices
  - Virtualisation and cloud-delivery (SBA, network-slicing)
  - Secure software, shared resource
- Criminal activities
  - 0.8% of global GDP (ca. 600 B yearly)
  - 5G opens more „opportunities“ to criminals

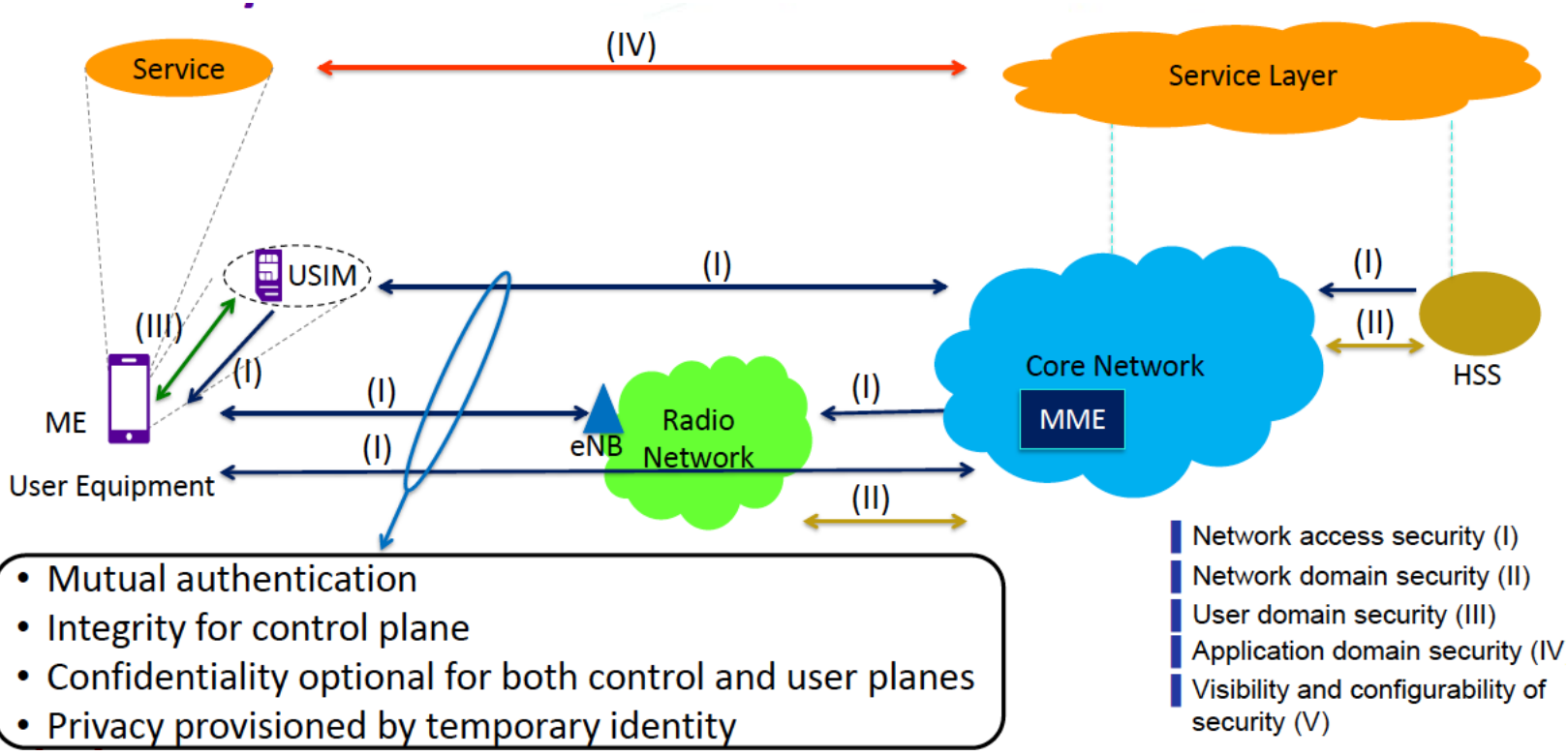
Need for measurable security and compliance, privacy safeguarding

4G to 5G Evolution

- 3GPP SA3 is the working group that develops mobile communications security specifications



4G Security Architecture

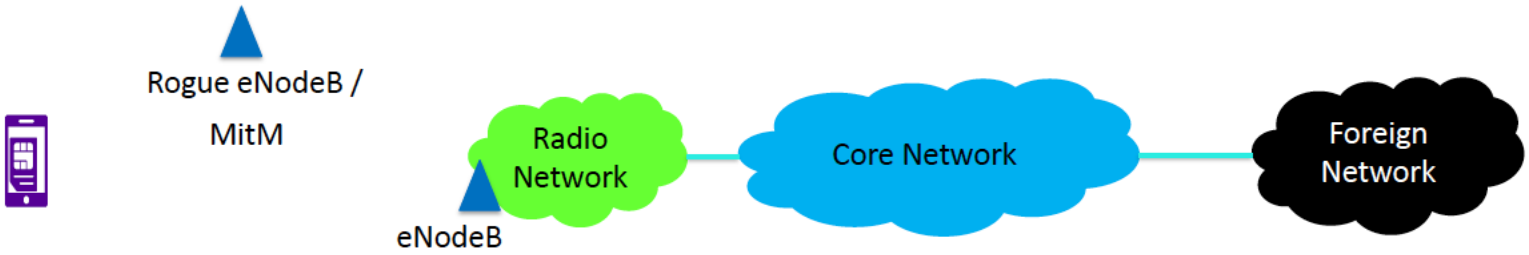


Evolution of 4G Security

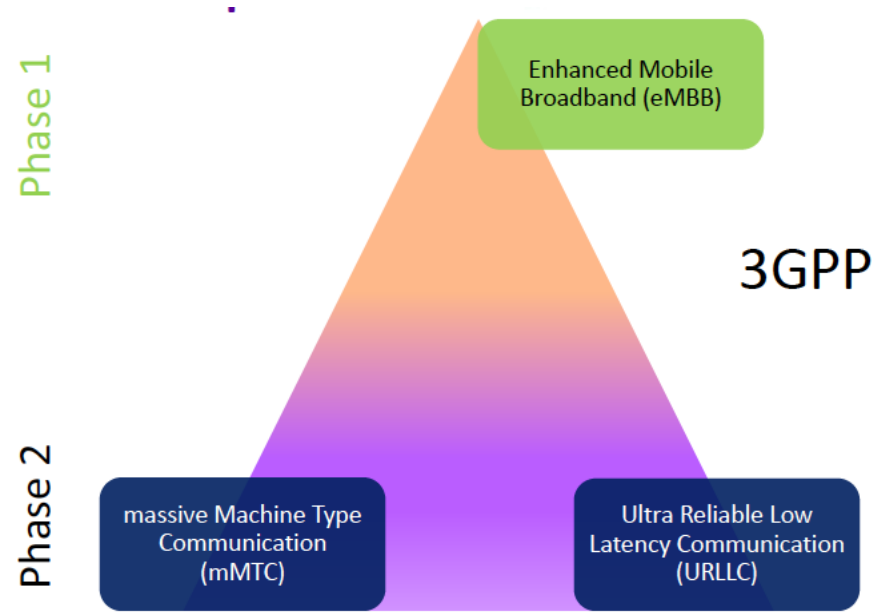
Potential Threats of 4G

- IMSI in clear
- Temporary identity not changed
- No UP integrity protection
- Bid-down to GSM

Interconnect threats due to SS7 & Diameter

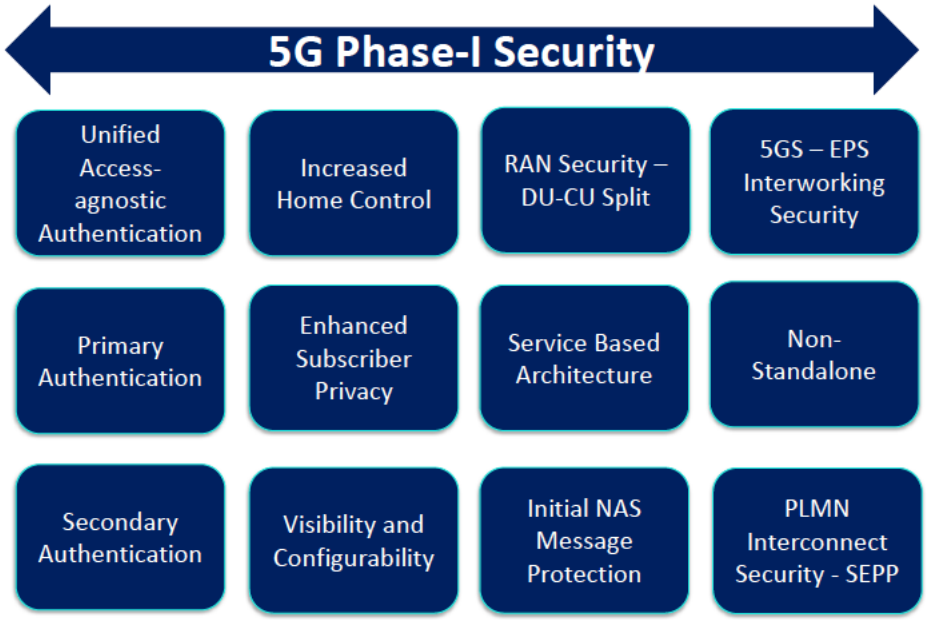


3GPP 5G Specification Phases

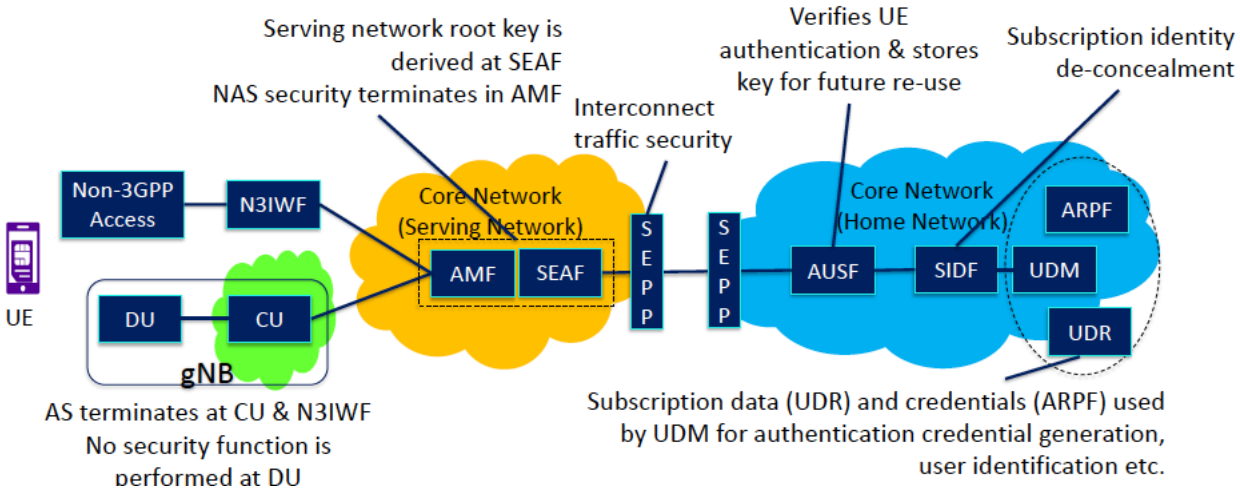


3GPP phase based 5G specification

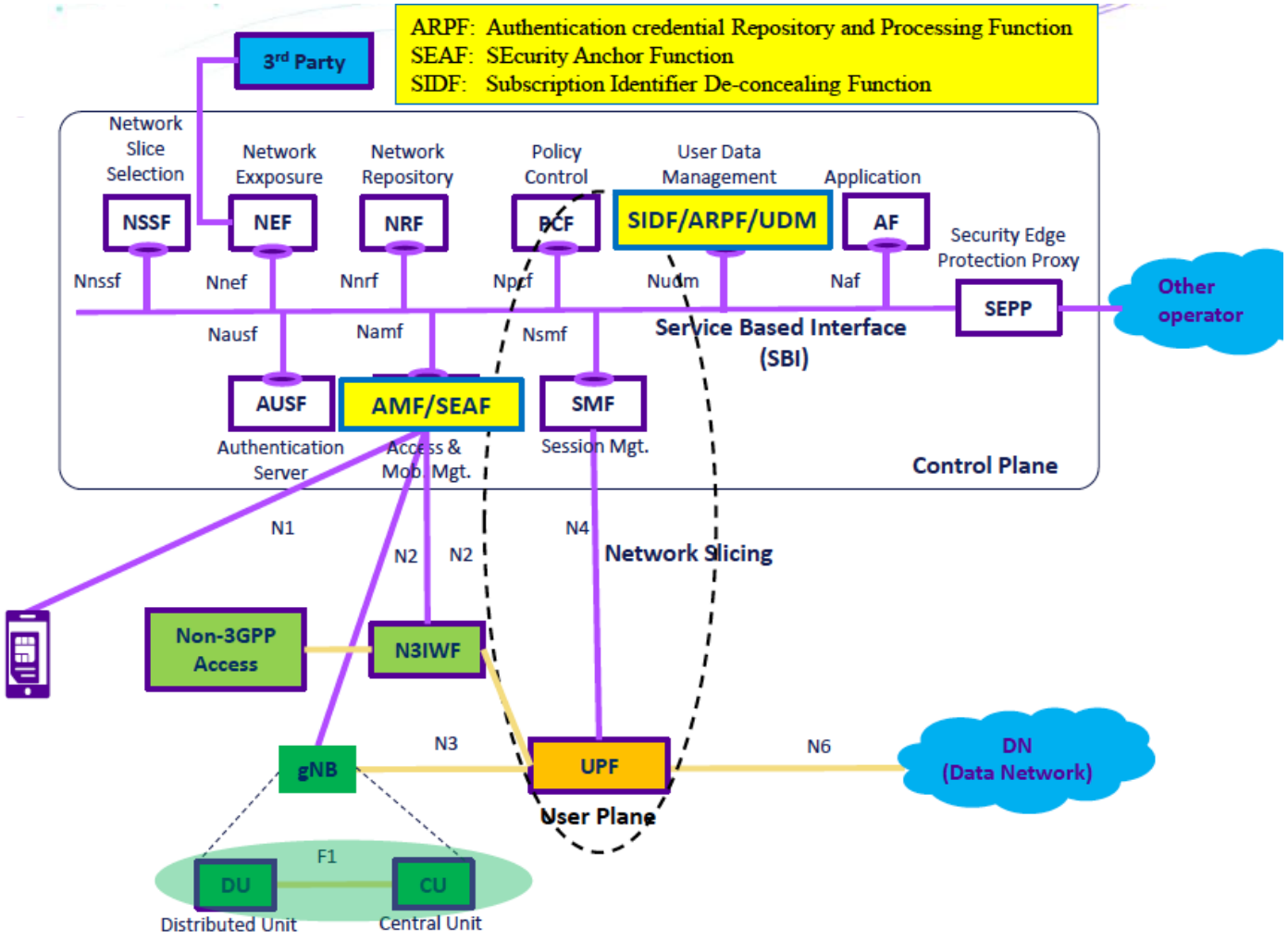
5G Phase 1 Security - Overview



5G Security Functions

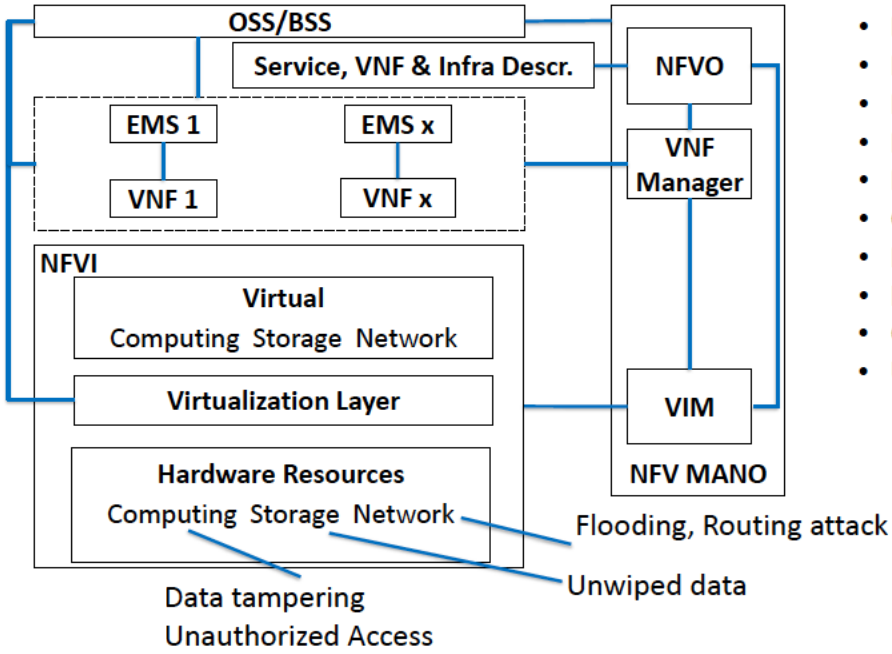


SBA and Network Slicing bring cloud and NFV to the mobile network service



Virtualisation Security

Threats



- Data manipulation
- Privilege misuse
- Package modification
- Rogue VNF
- Malicious code or tenant
- Configuration modification
- Resource allocation issues
- Image tampering
- Catalogue information exploit
- Uploading malicious images

Mitigation

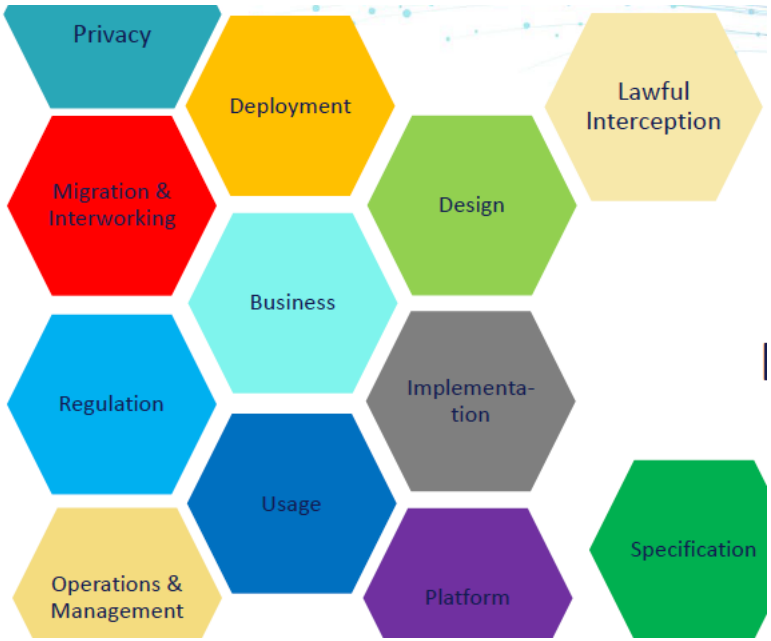
- Secure boot and chain of trust
- Remote attestation
- Secure crash
- Security assurance, signing and verification of image
- VNF isolation
- Tenant and administrator isolation

5G Security Next Steps

- Phase 2
  - Long-term key update
  - 256 bits keys usage
  - Security Assurance
  - Network Slicing Security
  - Location services Security
  - Security for URLLC
  - Security for Vertical & LAN Services

Holistic Security

- Security by Design
- Zero Trust



Opportunities - Targets

- Service Providers (Mobile NS-Operators, IT, Digitalisation – IoT, verticals)
  - Understand own connectivity and security requirements
  - Map the requirements to 5G and virtualisation (delivery model)
  - Develop appropriate security management and increase degree of automation
- Vendors
  - Implement as cloud-native
  - Security assurance tests as specified by 3GPP
  - Adapt to customer network architecture and changes

Opportunities

- Security Assurance as a Service
  - **Objective**: provide a customer-tailored security solution for the customer enterprise application- and network-services
    - Implement the customer-defined security policies
    - Provide security visibility and integrate with the customer Security Operations Center
    - Provide regulatory compliance and Lawful Interception
    - Integrate / Interoperate with the enterprise application- and network-Service Providers

  No specific security knowledge required from the app and connectivity DevOps

Opportunities

- Security Assurance as a Service
  - **Challanges**:
    - IAM :
      - Interoperability / federation with CSP-domains (mediated by local Orchestrators) and legacy on-premise,
      - flexible authentication and authorization by means of dynamic configuration of IAM- components triggered by the customer security policy
      - Key Management and secure store
      - Traffic visibility / duplication: middlebox security protocols

agentscape
Xtreme Personalisation

5GINFIRE

Thank You!

5GinFIRE.eu

contact@5GinFIRE.eu

5GinFIRE

5GINFIRE is a three years Research and Innovation action / project under the EU program Horizon 2020 (Grant Agreement no. 732497) started on 1 January 2017.