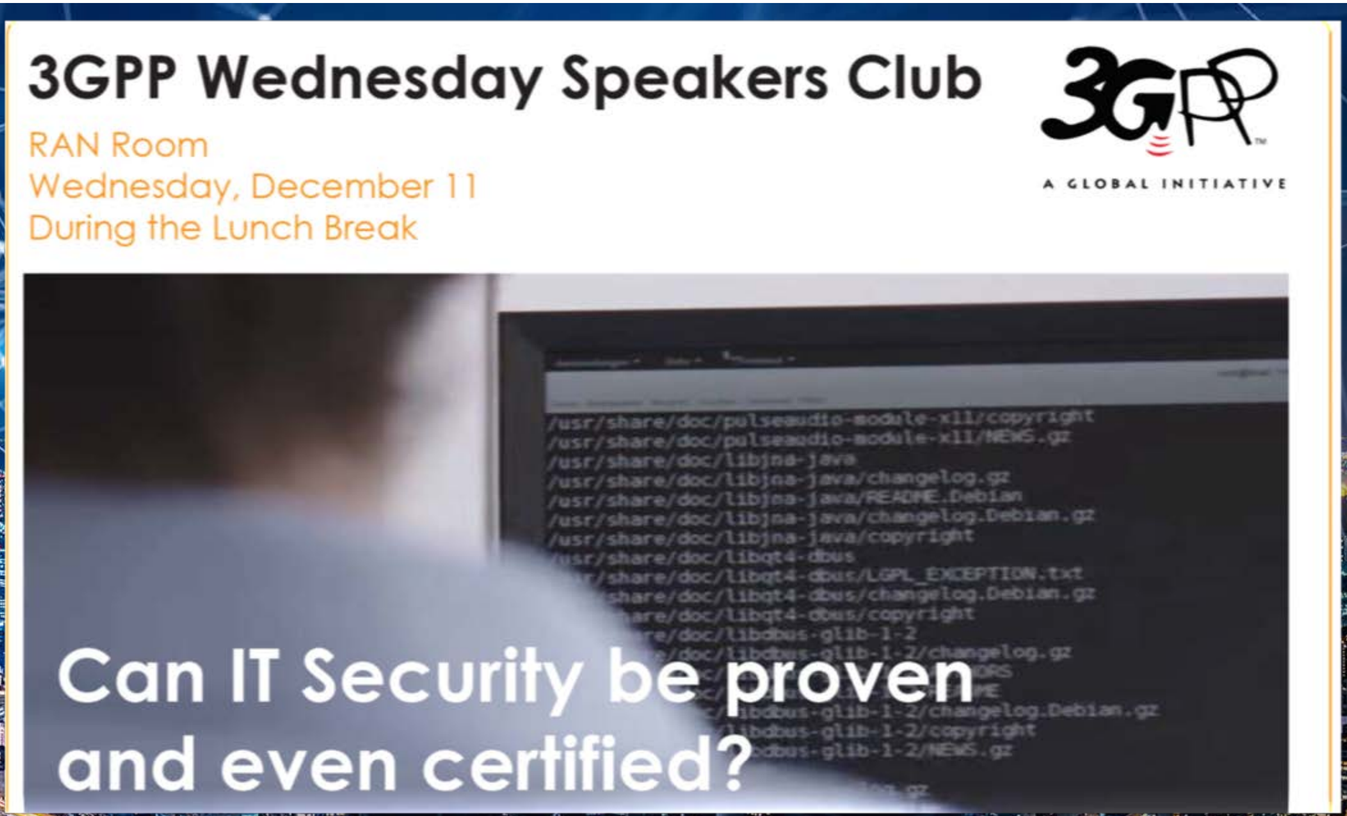


3GPP Wednesday Speakers Club

RAN Room
Wednesday, December 11
During the Lunch Break

3GPP
A GLOBAL INITIATIVE

Can IT Security be proven and even certified?

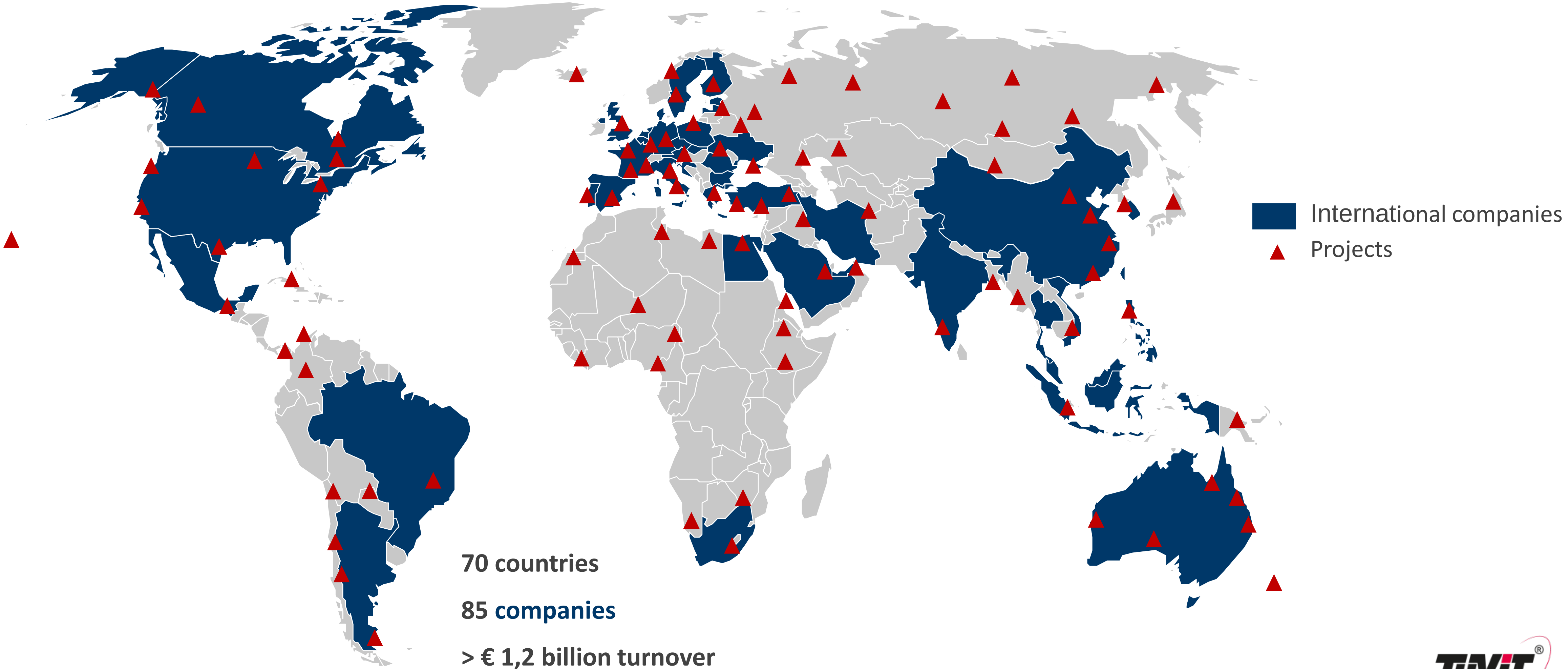
How do you check IT security?
Practice of an accredited IT Security testing laboratory

Dirk Kretzschmar
Managing Director
TÜV Informationstechnik GmbH
Member Group Executive Committee TÜV NORD Group
CEO Business Unit IT

Barcelona Sitges, December 11th, 2019

TÜViT®
TÜV NORD GROUP

THE WORLD OF TÜV NORD GROUP AT A GLANCE



70 countries

85 companies

> € 1,2 billion turnover

ONE ENTERPRISE – FOUR BRANDS

TÜV NORD GROUP

TÜV NORD

Industrial Services,
Mobility,
Training

DMT

Natural
Resources

ALTER TECHNOLOGY

Aerospace

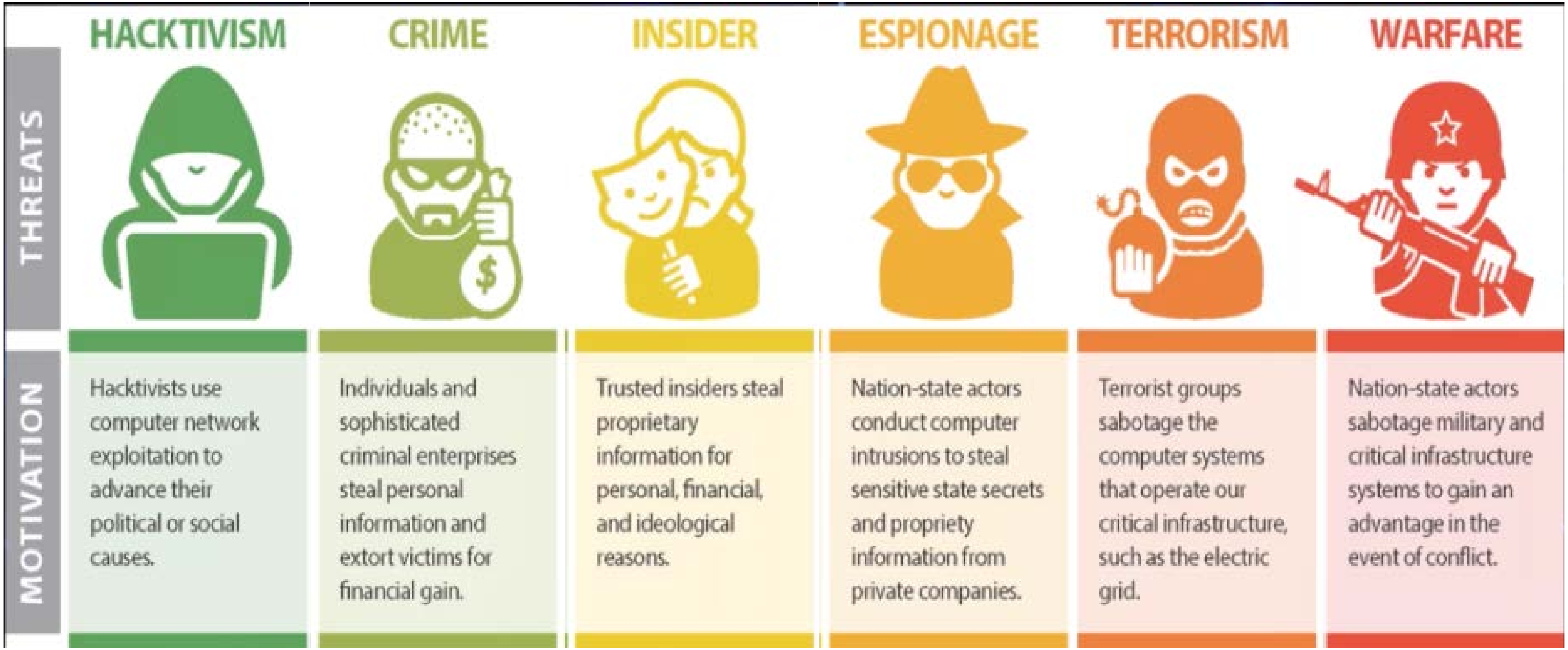
TÜViT®

ICT Security

Safety (avoid accidents)
compliance, norms, conformity to save human lives against threads by machines and environment

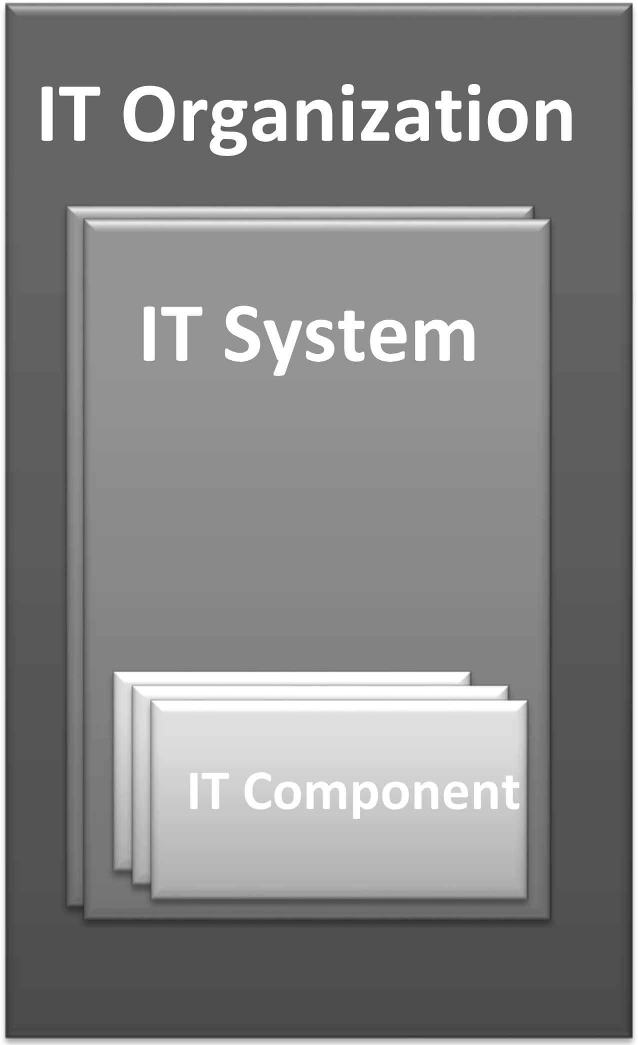
Security (criminal prevention)
Evaluate resistance of build in protection
Handle the unknown
Creative detection and use of vulnerabilities
Analysis with an attacker‘s view

THE CYBER THREAD SPECTRUM



THREATS	HACKTIVISM	CRIME	INSIDER	ESPIONAGE	TERRORISM	WARFARE
MOTIVATION	Hacktivists use computer network exploitation to advance their political or social causes.	Individuals and sophisticated criminal enterprises steal personal information and extort victims for financial gain.	Trusted insiders steal proprietary information for personal, financial, and ideological reasons.	Nation-state actors conduct computer intrusions to steal sensitive state secrets and propriety information from private companies.	Terrorist groups sabotage the computer systems that operate our critical infrastructure, such as the electric grid.	Nation-state actors sabotage military and critical infrastructure systems to gain an advantage in the event of conflict.

TÜVIT - SECURITY AT ALL LEVELS



- Information Security Management (ISO)
- Data Privacy (GDPR)
- Project- and Quality Management
- Process Optimization

Documentation
Organisation
Interviews

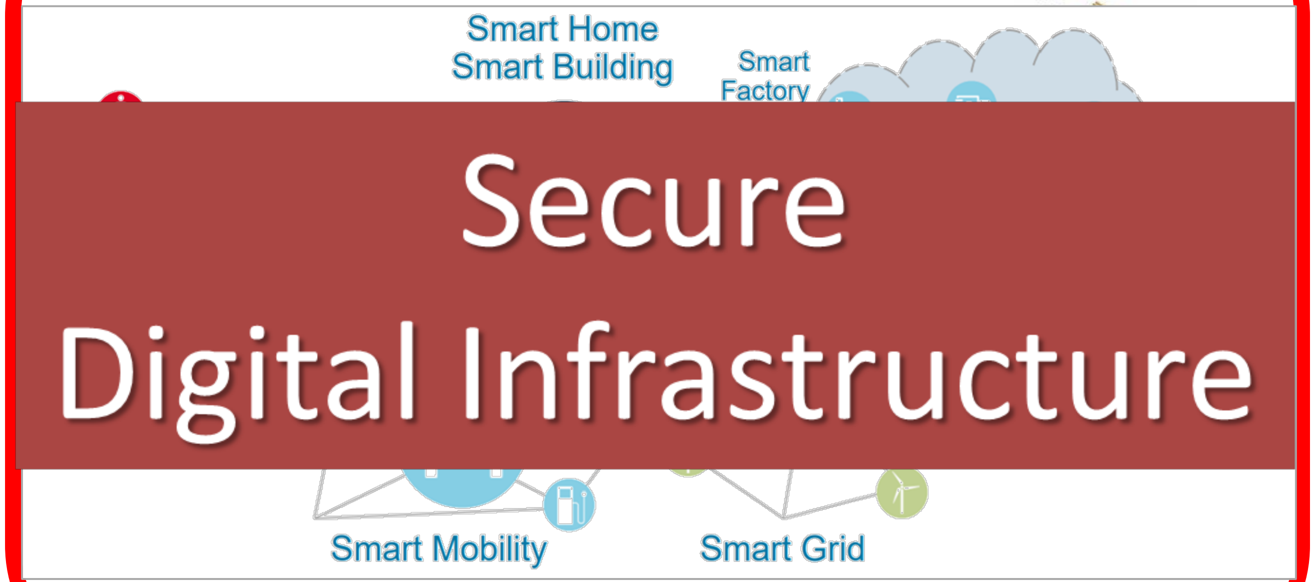
- Industrial Security (IEC)
- System- and Network Security (NIST)
- Web Application Security (OWASP)
- Mobile Security (OWASP)
- Security Concepts and Analysis
- Data Privacy (GDPR)
- Datacenter (TSI)

- Product Evaluation (Common Criteria)
- Validation Tests (FIPS140-2)
- Security Tests and Assessments (Hard-and Software)
- Source Code Analysis (SW/Embedded)
- Reviews according to Bank Specifications
- Conformity Test

Lab evaluation
On site review
Development process
Logistics
Update/Patch management

TÜVIT
BUSINESS MISSION

Cyber Security



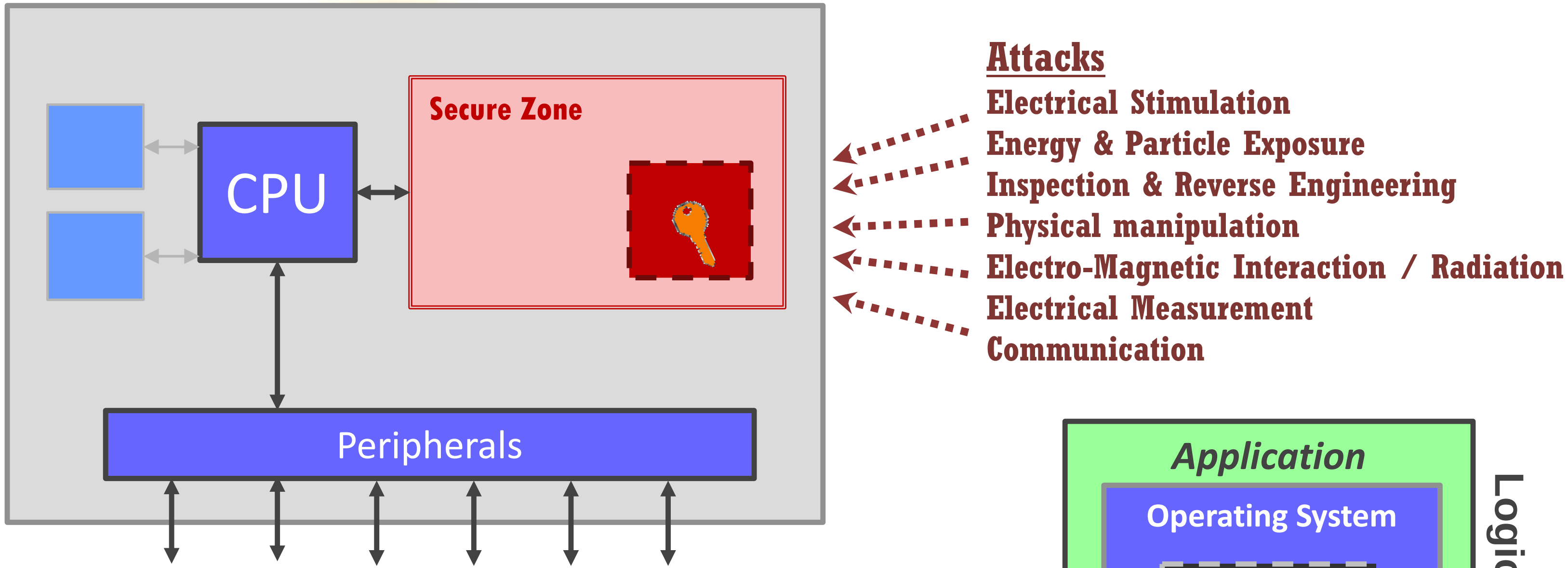
Secure
Digital Infrastructure

Cyber security is the essential prerequisite for the success of digitalization.
In order to take full advantage of the opportunities offered by digitalization, the risks associated with it must be made manageable.

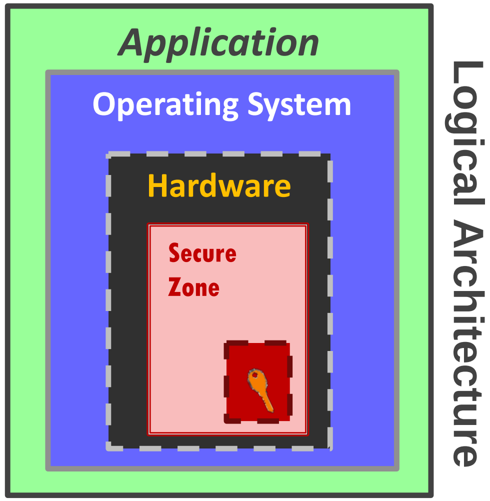
The challenge is the cyber security of the digital infrastructure and applications, both national and international, in all areas of the digitalization. By bundling IT security and ICT expertise, we lead our customers' digitalization projects to success.

SECURE ELEMENTS

Embedded



Attacks
Electrical Stimulation
Energy & Particle Exposure
Inspection & Reverse Engineering
Physical manipulation
Electro-Magnetic Interaction / Radiation
Electrical Measurement
Communication



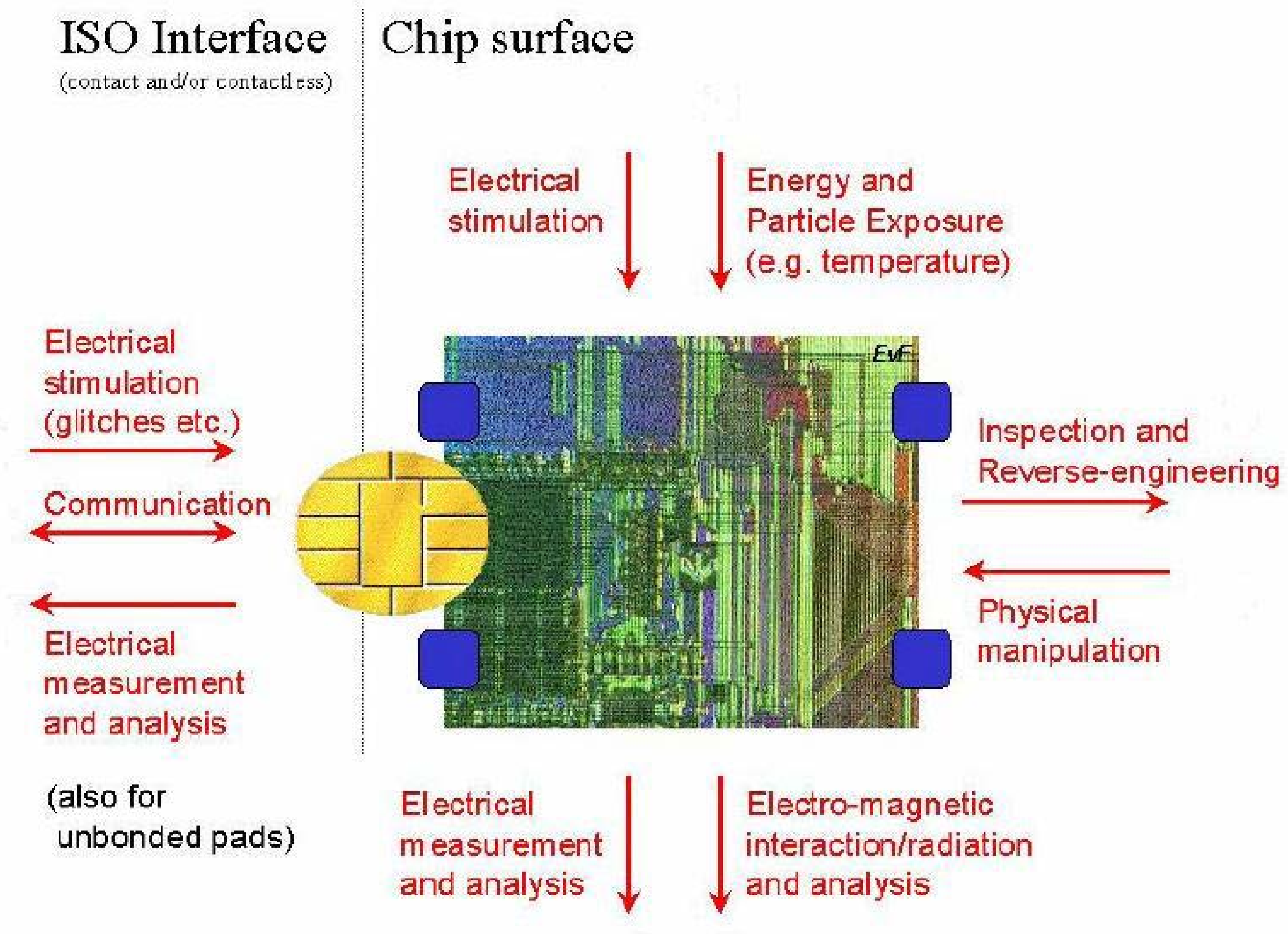
POTENTIAL ATTACK PATHES

Logical attacks

- Software attacks

Physical attacks

- Passive Side-Channel Analysis (Power analysis)
- Perturbation Attacks (Fault injection)


ISO Interface
(contact and/or contactless)
Chip surface
Electrical stimulation
Energy and Particle Exposure (e.g. temperature)
Electrical stimulation (glitches etc.)
Communication
Electrical measurement and analysis
(also for unbonded pads)
Inspection and Reverse-engineering
Physical manipulation
Electrical measurement and analysis
Electro-magnetic interaction/radiation and analysis

HARDWARE EVALUATION

- Secure storage of Information in Hardware Modules
- Fully automated test passes
- Continuously adapted test software
- Usage of KI within the analysis

APPLIED CRITERIA

Common Criteria

Bundesamt
für Sicherheit in der
Informationstechnik

ilac-MRA

International Accreditation Japan
IAJapan
ASNITE 0019 T

EMVCo

MasterCard
Worldwide

VISA

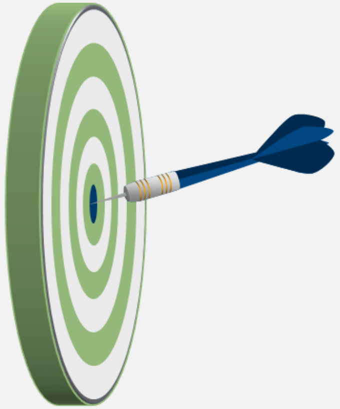
AMERICAN EXPRESS

UnionPay
银联

DISCOVER

JCB

AIM

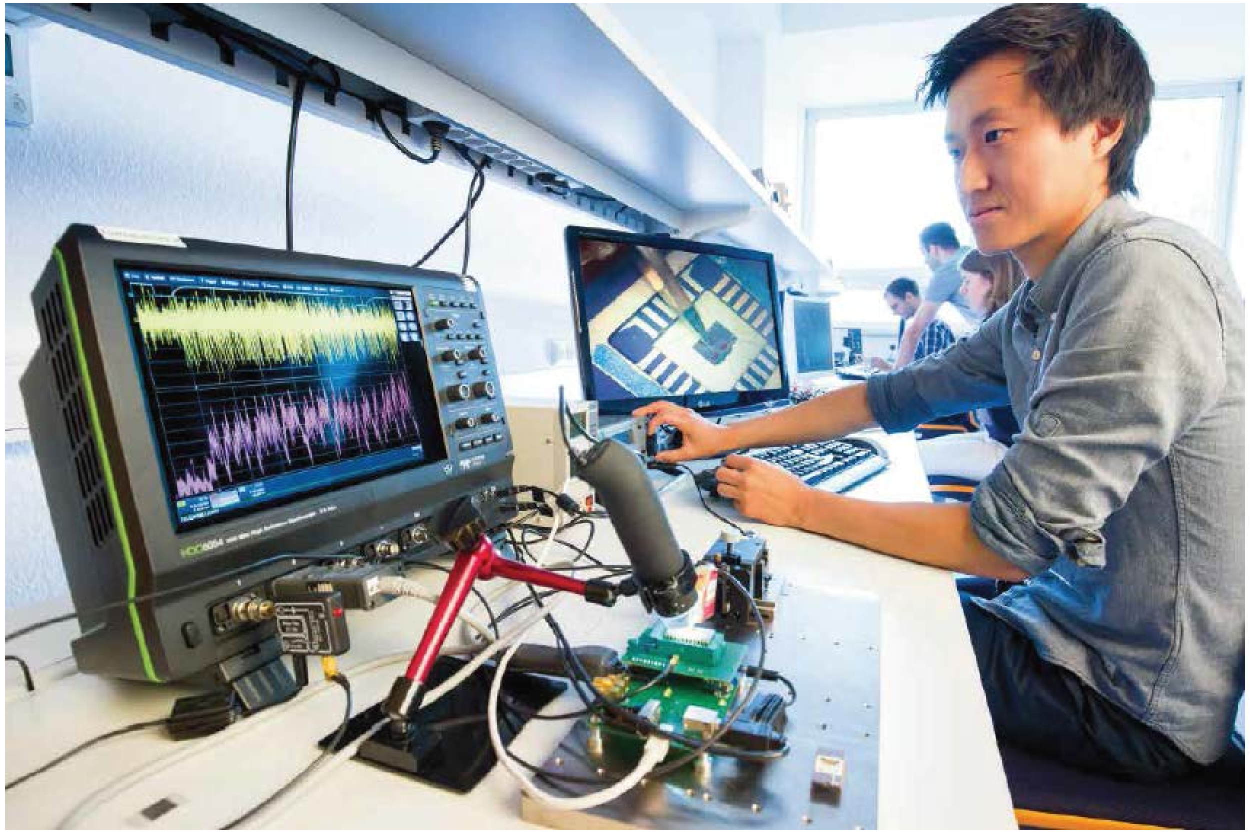


Protection of stored/processed secure data against manipulation and monitoring

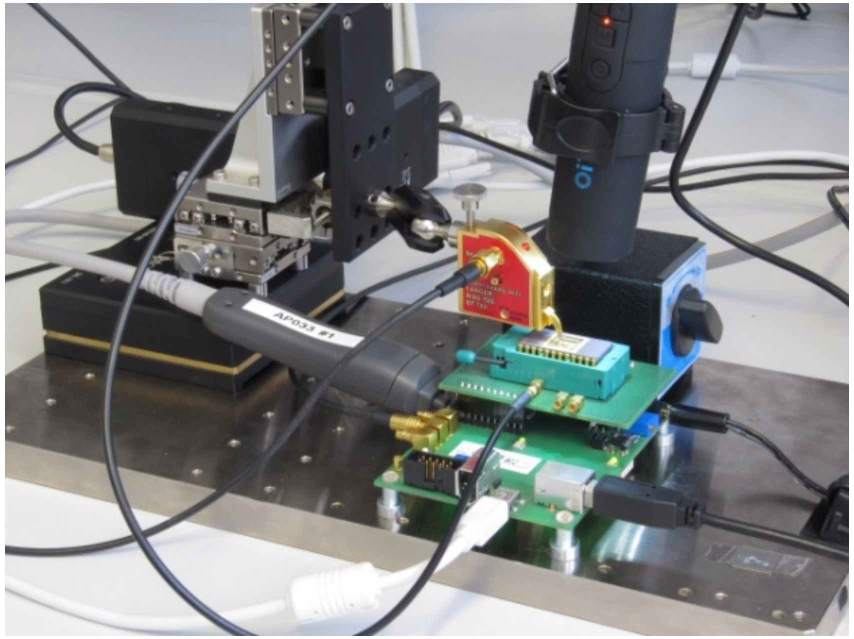
APPROACH

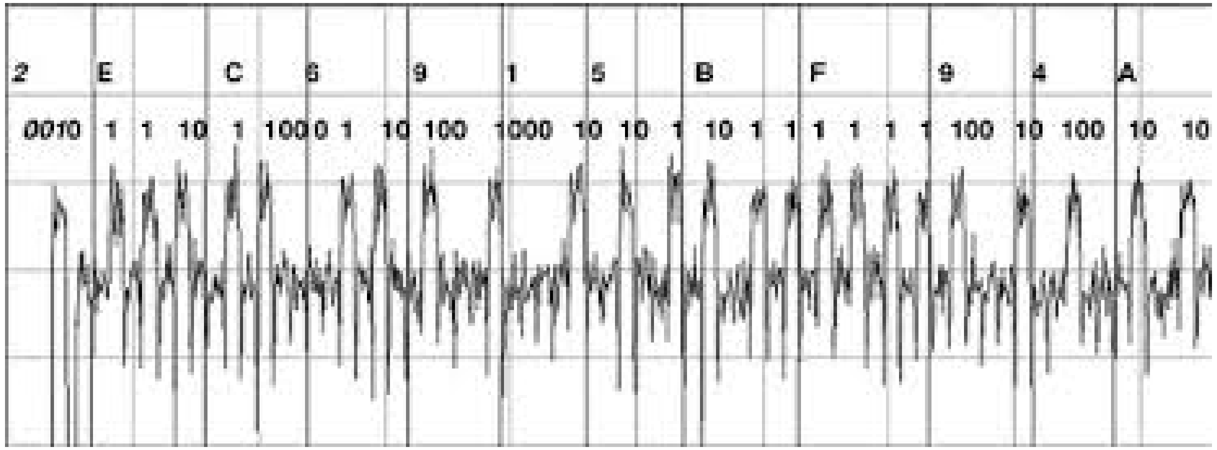
- **Vulnerability analysis** of the implemented security mechanisms (Protection against attackers with „high attack potential“, i.e. with high effort (time, cost, equipment)
- **Audit** of the development and production environment (entire life cycle)
- Execution of **penetration tests** in the HW laboratory of the evaluation lab

TÜVIT HARDWARE-LAB LOCATION ESSEN (GERMANY)



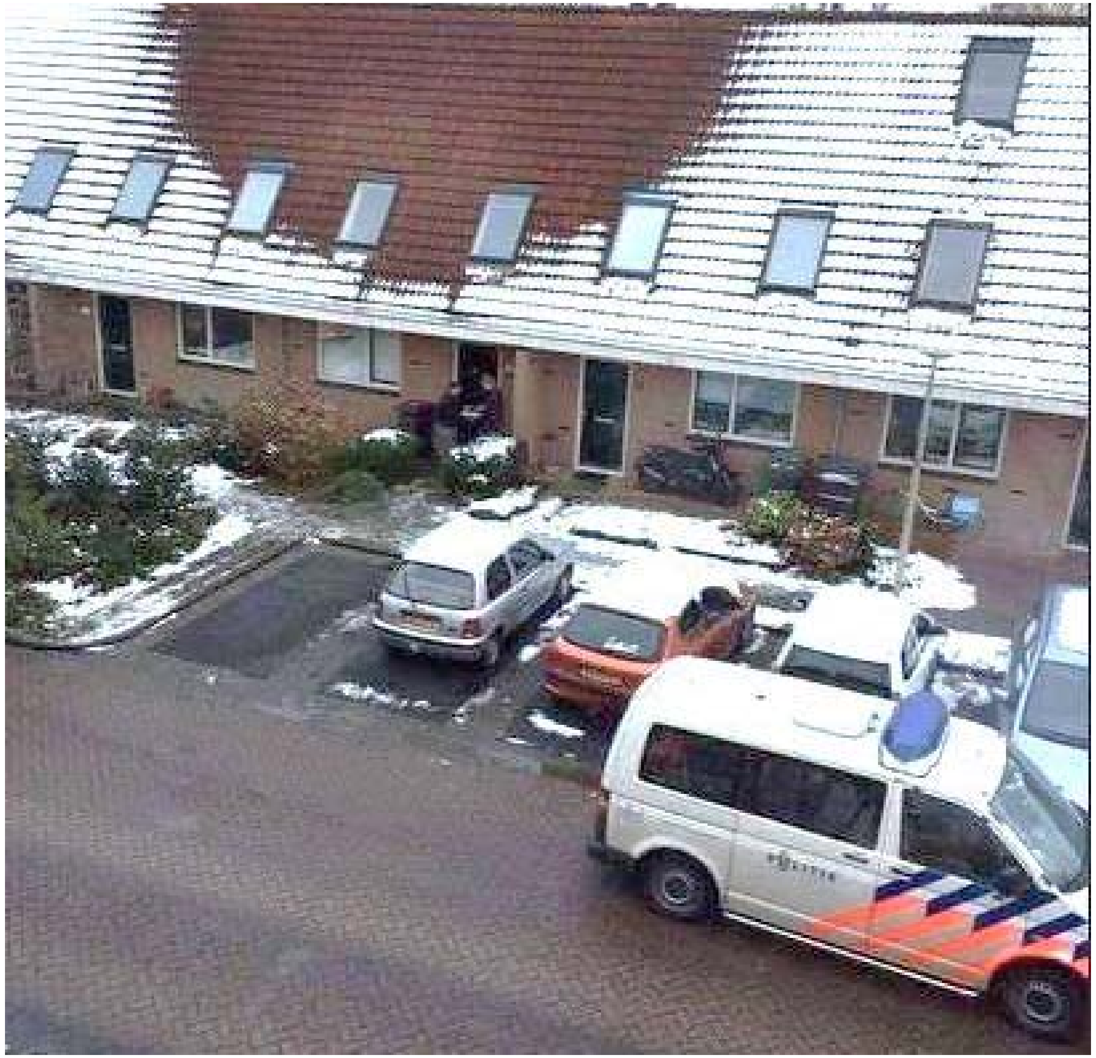
SIDE CHANNEL:
MONITORING COMPUTED DATA



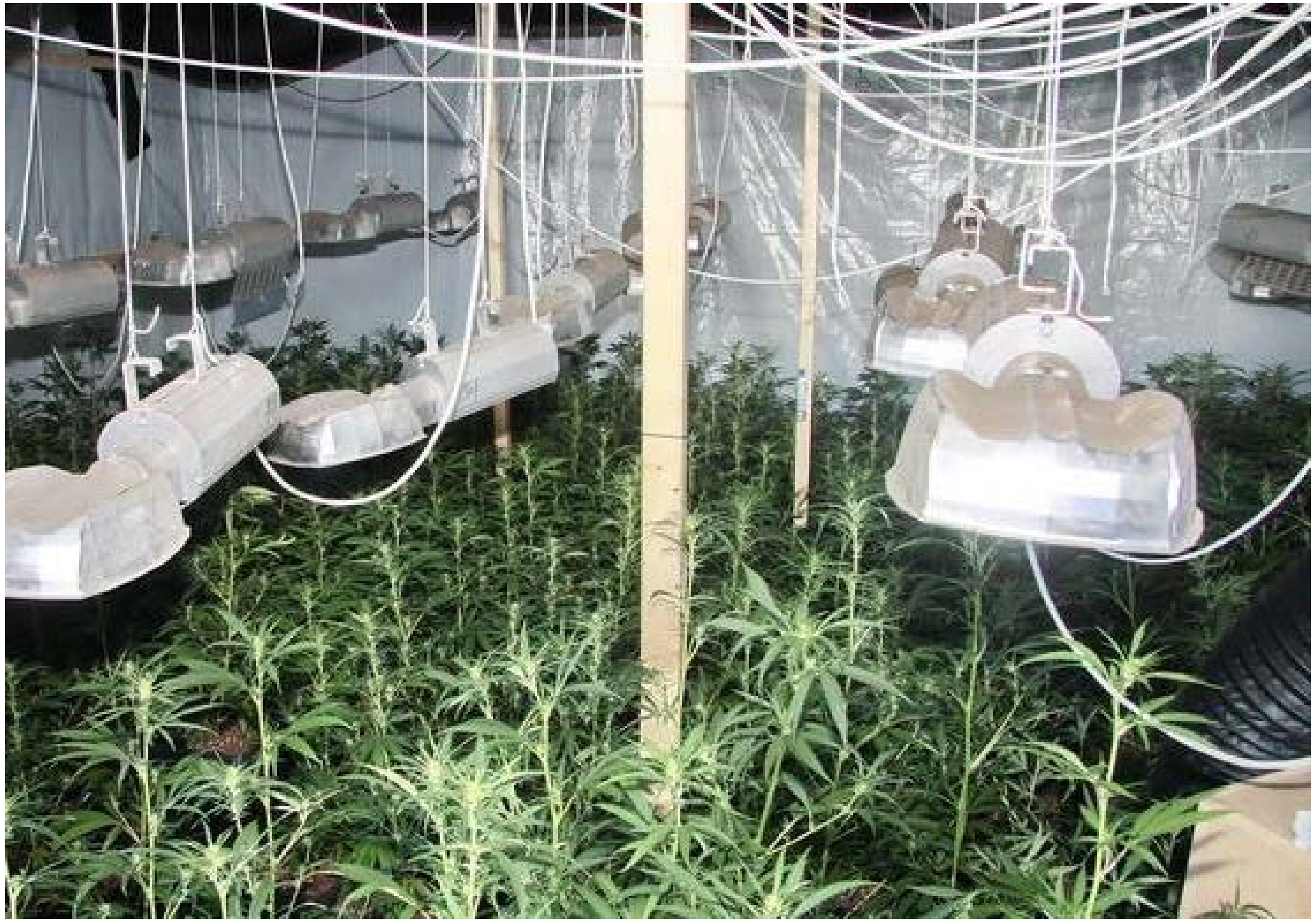


Example of a side channel attack

Outside view



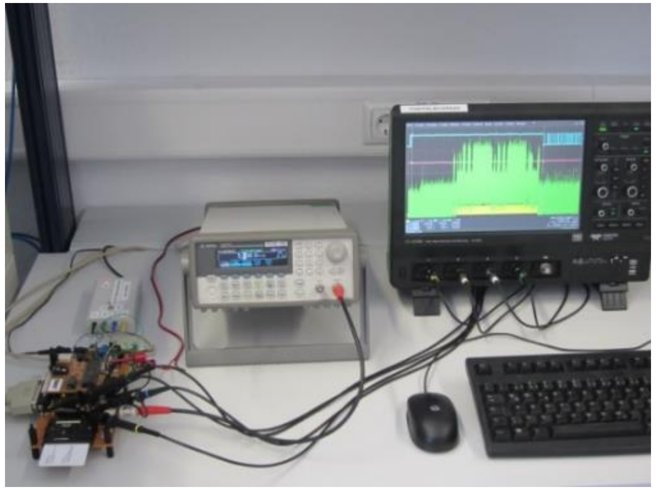
Inside view



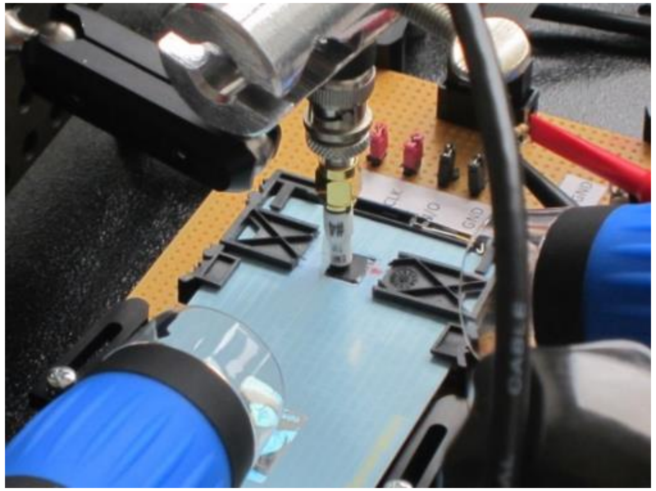
FAULT ATTACKS – ALTERNATIVE FAULT SOURCES

Manipulation of:

- Program flow (e.g. skip commands)
- Computed data (e.g. result of calculation)
- Memory content (e.g. stored value)



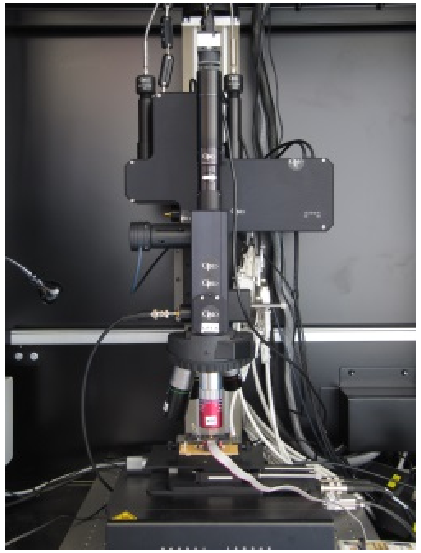
Voltage Glitches

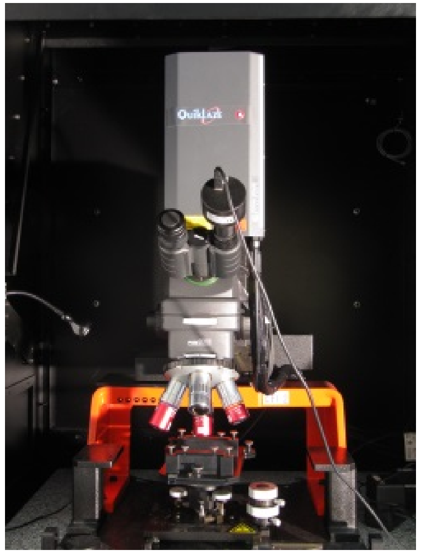


EM pulses

Temperature

PERTURBATION ATTACKS
FAULT ATTACK: LASER

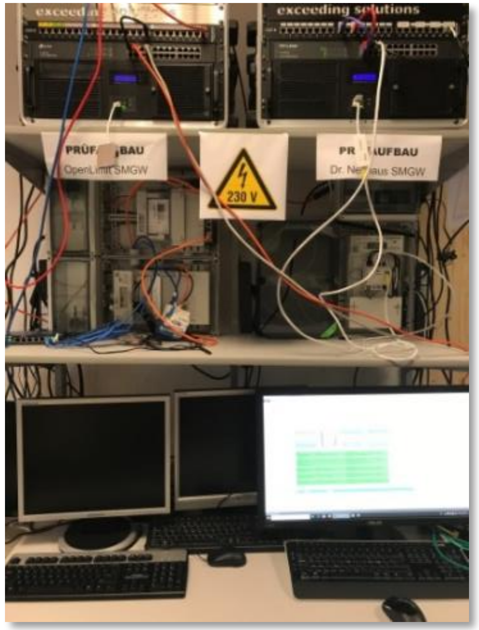


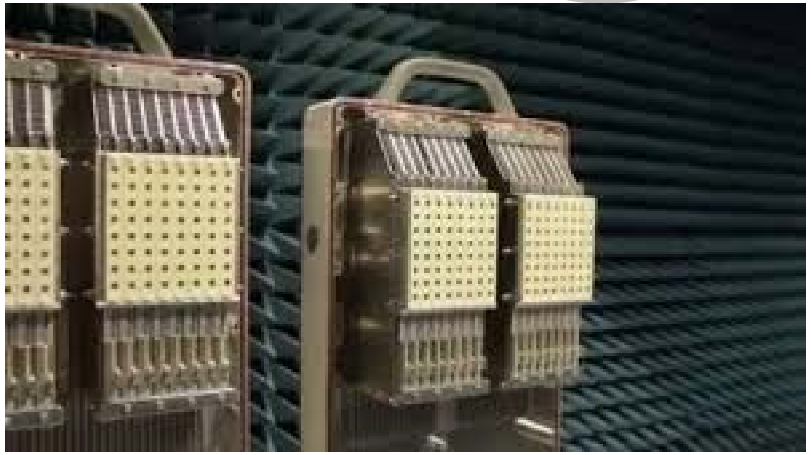


- Laser setup
  - Diode pumped double laser / Nd:YAG laser / diode laser
  - Delay generator
  - Digital oscilloscope
  - Control PC
  - Interface device (e. g. card terminal)

SOFTWARE EVALUATION

- **Source Code Review**
- **Fully automated test environment** for the evaluation of **protocols and crypto algorithms**
- Utilization of **virtual test environments** for software product evaluation
- Use of state-of-the-art **3rd party analysis** and **test tools** (e.g. Smart Meter Gateway Test Suite)
- Continuous investment and development of test environments to be able to test the **latest technologies**

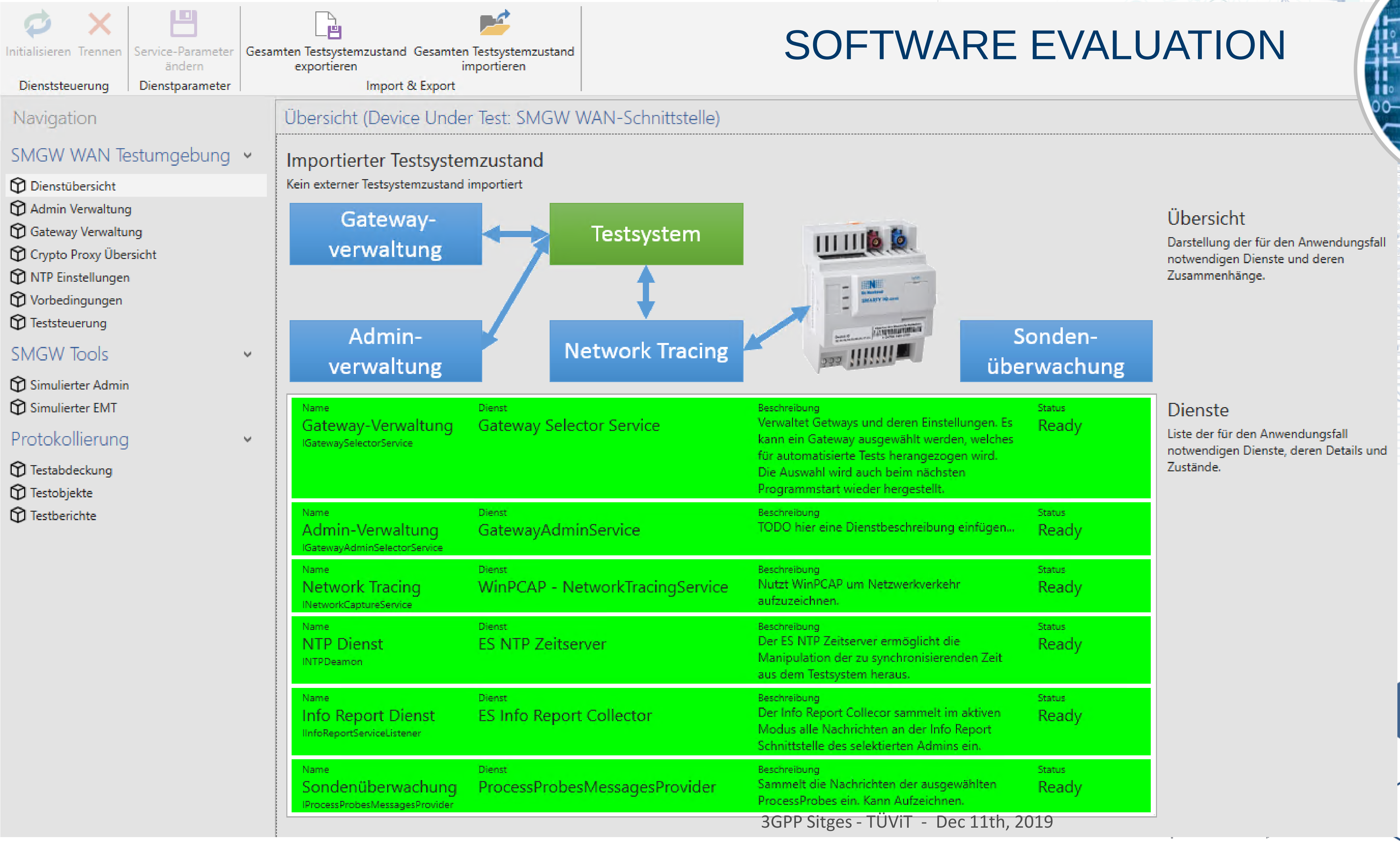




```
ient = new bl.deskt
ionClient.Insert();
ationClient.LastRequest = DateTi
ationClient.RequestCount = Notifi
icationClient.Update();
onClient.Deny == false)
quest Notificatio
.ClientId
```

Building trust in IT security products – complete test concepts for software and hardware

SOFTWARE EVALUATION



Übersicht (Device Under Test: SMGW WAN-Schnittstelle)

Importierter Testsystemzustand

Kein externer Testsystemzustand importiert

Name	Dienst	Beschreibung	Status
Gateway-Verwaltung IGatewaySelectorService	Gateway Selector Service	Verwaltet Getways und deren Einstellungen. Es kann ein Gateway ausgewählt werden, welches für automatisierte Tests herangezogen wird. Die Auswahl wird auch beim nächsten Programmstart wieder hergestellt.	Ready
Admin-Verwaltung IGatewayAdminSelectorService	GatewayAdminService	TODO hier eine Dienstbeschreibung einfügen...	Ready
Network Tracing INetworkCaptureService	WinPCAP - NetworkTracingService	Nutzt WinPCAP um Netzwerkverkehr aufzuzeichnen.	Ready
NTP Dienst INTPDeamon	ES NTP Zeitserver	Der ES NTP Zeitserver ermöglicht die Manipulation der zu synchronisierenden Zeit aus dem Testsystem heraus.	Ready
Info Report Dienst IInfoReportServiceListener	ES Info Report Collector	Der Info Report Collecor sammelt im aktiven Modus alle Nachrichten an der Info Report Schnittstelle des selektierten Admins ein.	Ready
Sondenüberwachung IProcessProbesMessagesProvider	ProcessProbesMessagesProvider	Sammelt die Nachrichten der ausgewählten ProcessProbes ein. Kann Aufzeichnen.	Ready

Übersicht

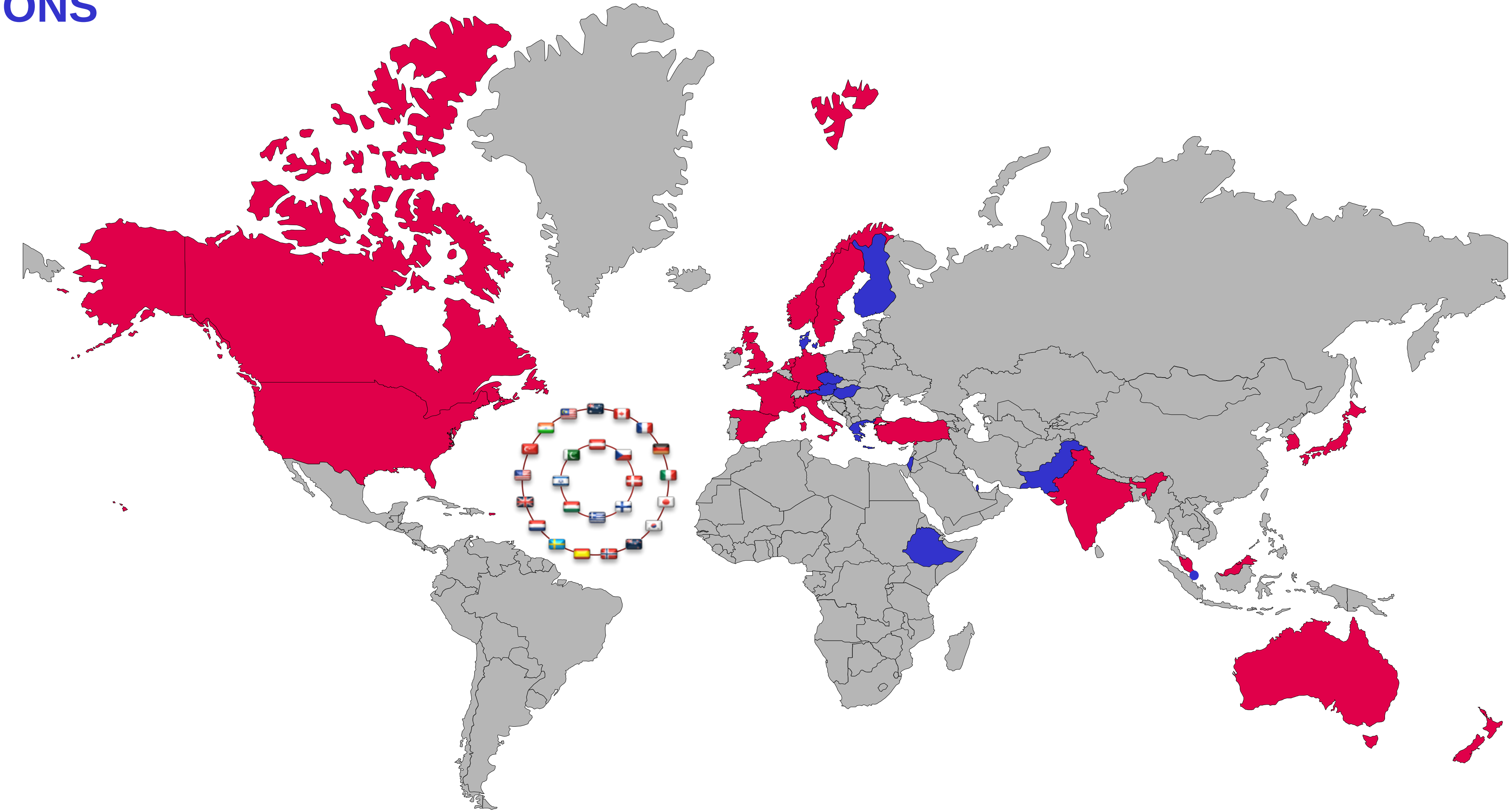
Darstellung der für den Anwendungsfall notwendigen Dienste und deren Zusammenhänge.

Dienste

Liste der für den Anwendungsfall notwendigen Dienste, deren Details und Zustände.

COMMON CRITERIA – CCRA

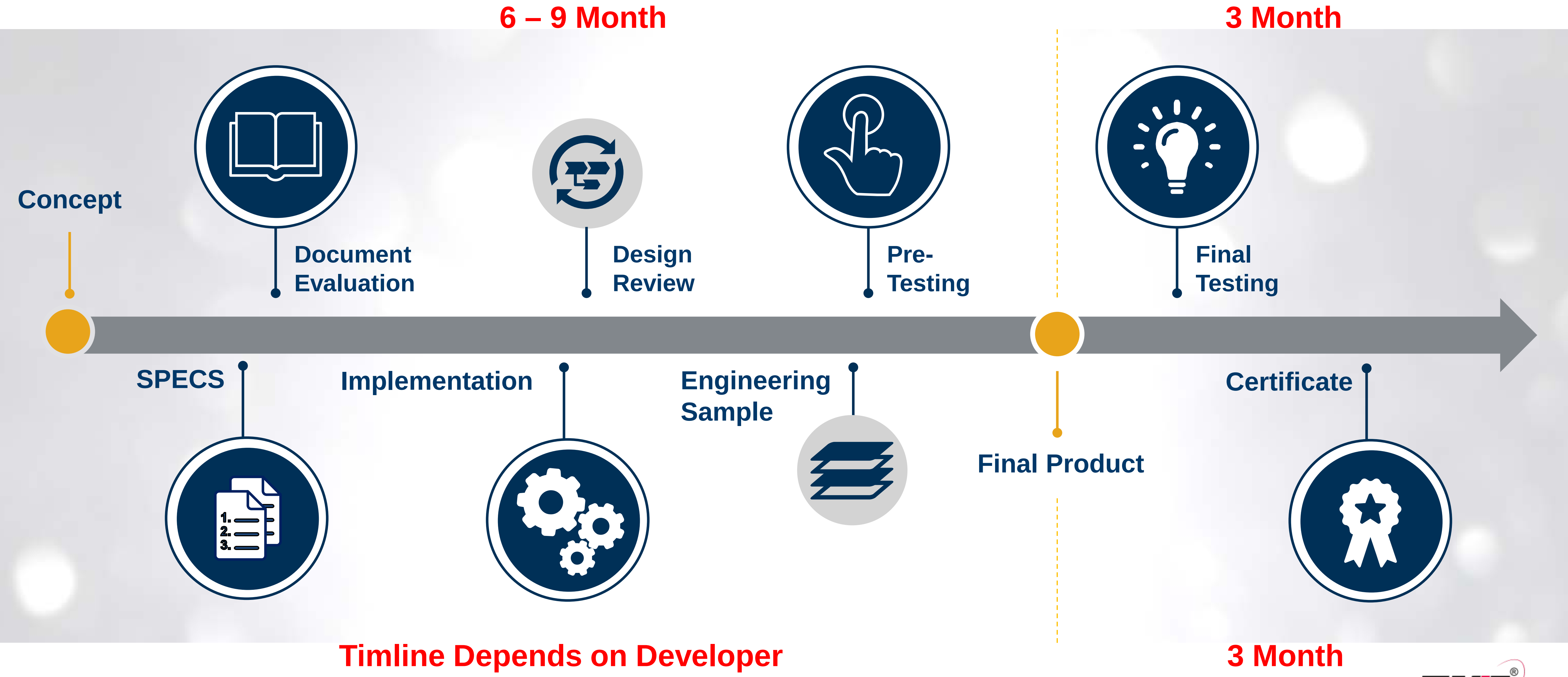
CERTIFICATE ISSUING AND CONSUMING NATIONS - CERTIFICATE CONSUMING NATIONS



IMPORTANCE OF COMMON CRITERIA

APPLICATION SECTOR	PRODUCT/ COMPONENT	MANDATORY/ CC ASSURANCE LEVEL
eHealth and Telematic Infrastructure	eHealth Smart Cards eHealth Terminals Connectors (to eHealth backbone)	EAL4 EAL2 EAL4
Smart Energy	Smart Meter Gateways	EAL4
Electronic Signature	Signature Smart Cards Signature Terminals Signature SW Time Stamp Servers Certificate Servers	EAL4 EAL4 EAL4 EAL4 EAL4
Cloud Computing	Cloud Server	EAL2
eID	Electronic Passports National ID Cards	EAL4 EAL4
Governmental/ Military Use	Secret HW, SW and Crypto Components	EAL 2 to EAL6
		VOLUNTARY/ MARKET DRIVEN
Information Technology	Trusted Platform Modules (TPM) Firewalls Databases Biometric Systems And many more	EAL3 EAL 2 to EAL4 EAL 2 to EAL4 EAL 2 to EAL4

EVALUATION TIMELINE



6 – 9 Month

3 Month

Concept

Document Evaluation

Design Review

Pre-Testing

Final Testing

SPECS

Implementation

Engineering Sample

Final Product

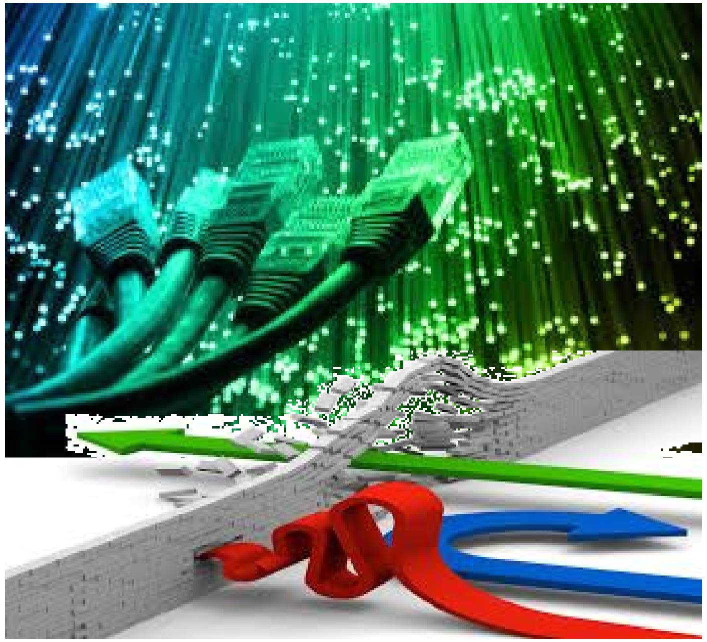
Certificate

Timline Depends on Developer

3 Month

IT SECURITY FOR SYSTEMS:

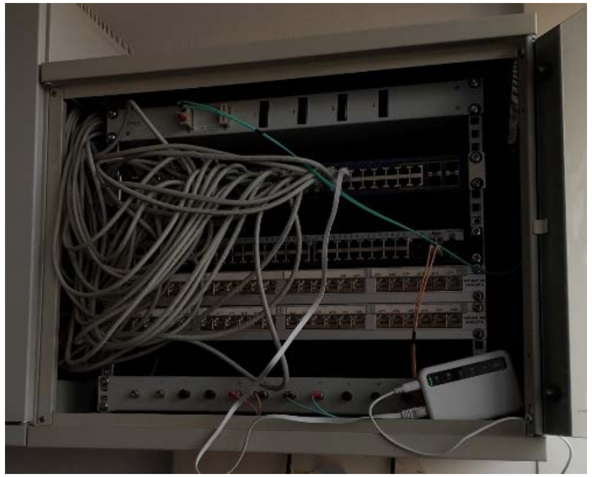
Network Analysis



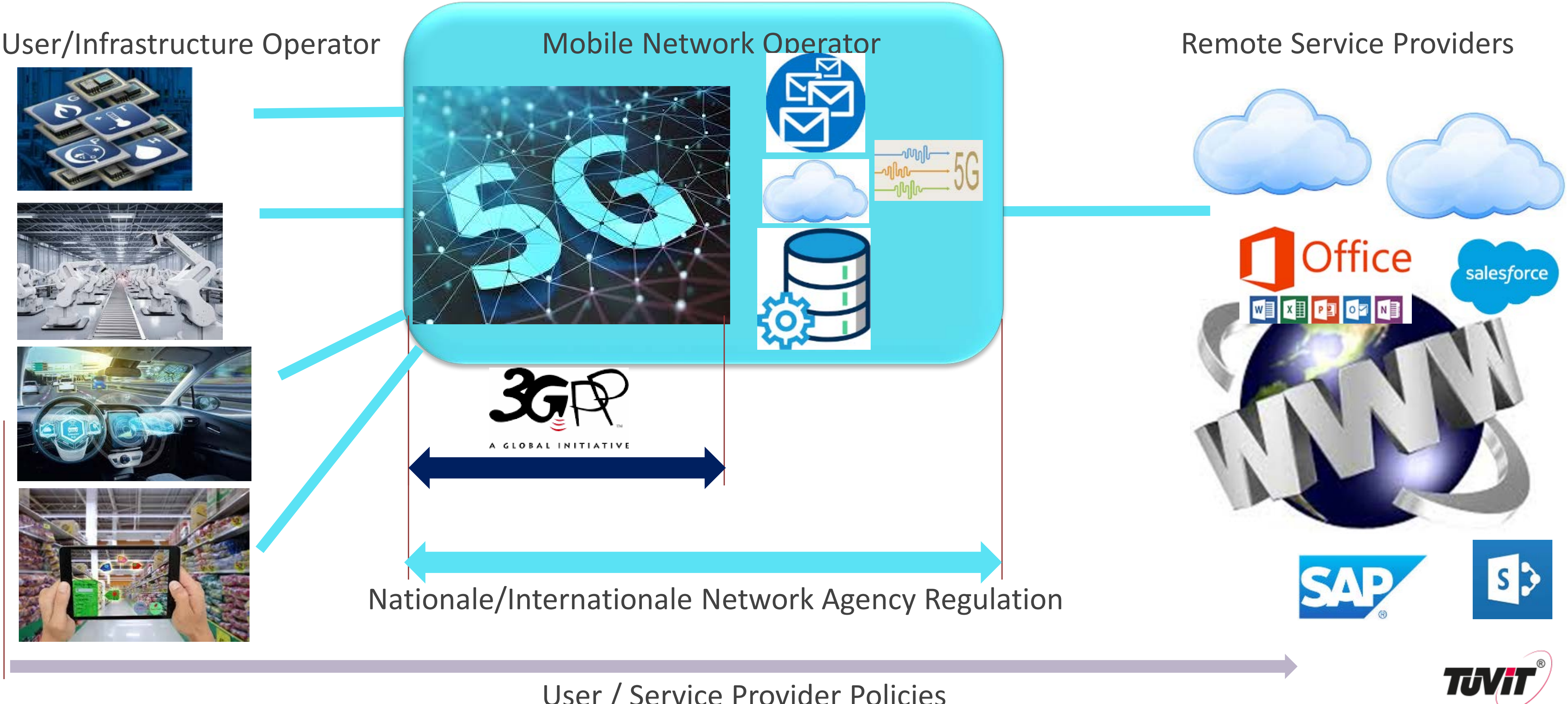
Social Engineering

Bypass Test / internal threads

PERIMETER SECURITY & APT



5G MODELL MNO



User/Infrastructure Operator

Mobile Network Operator

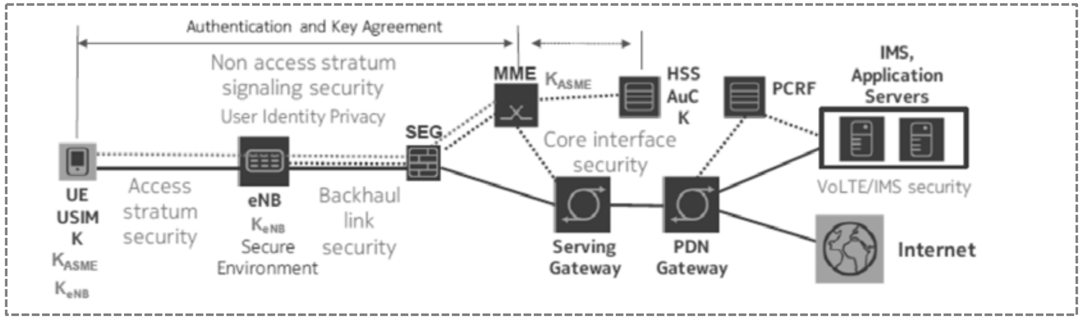
Remote Service Providers

Nationale/Internationale Network Agency Regulation

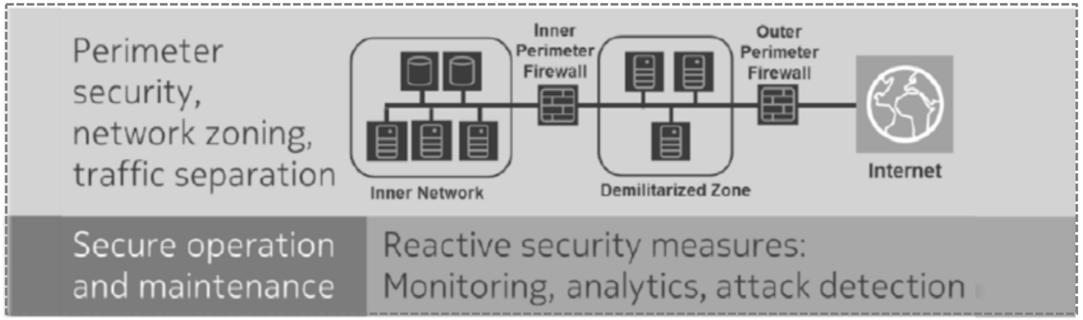
User / Service Provider Policies

Layers of mobile network security as of today (example 4G/LTE)

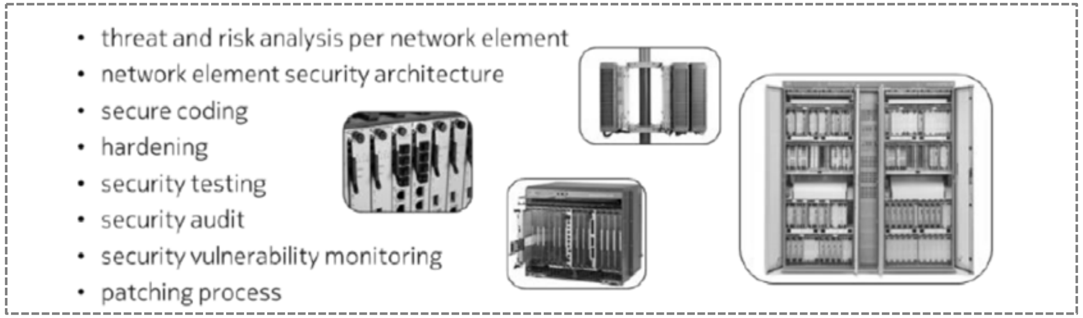
3GPP-specified security architecture



Network security not specified by 3GPP



Network element security measures



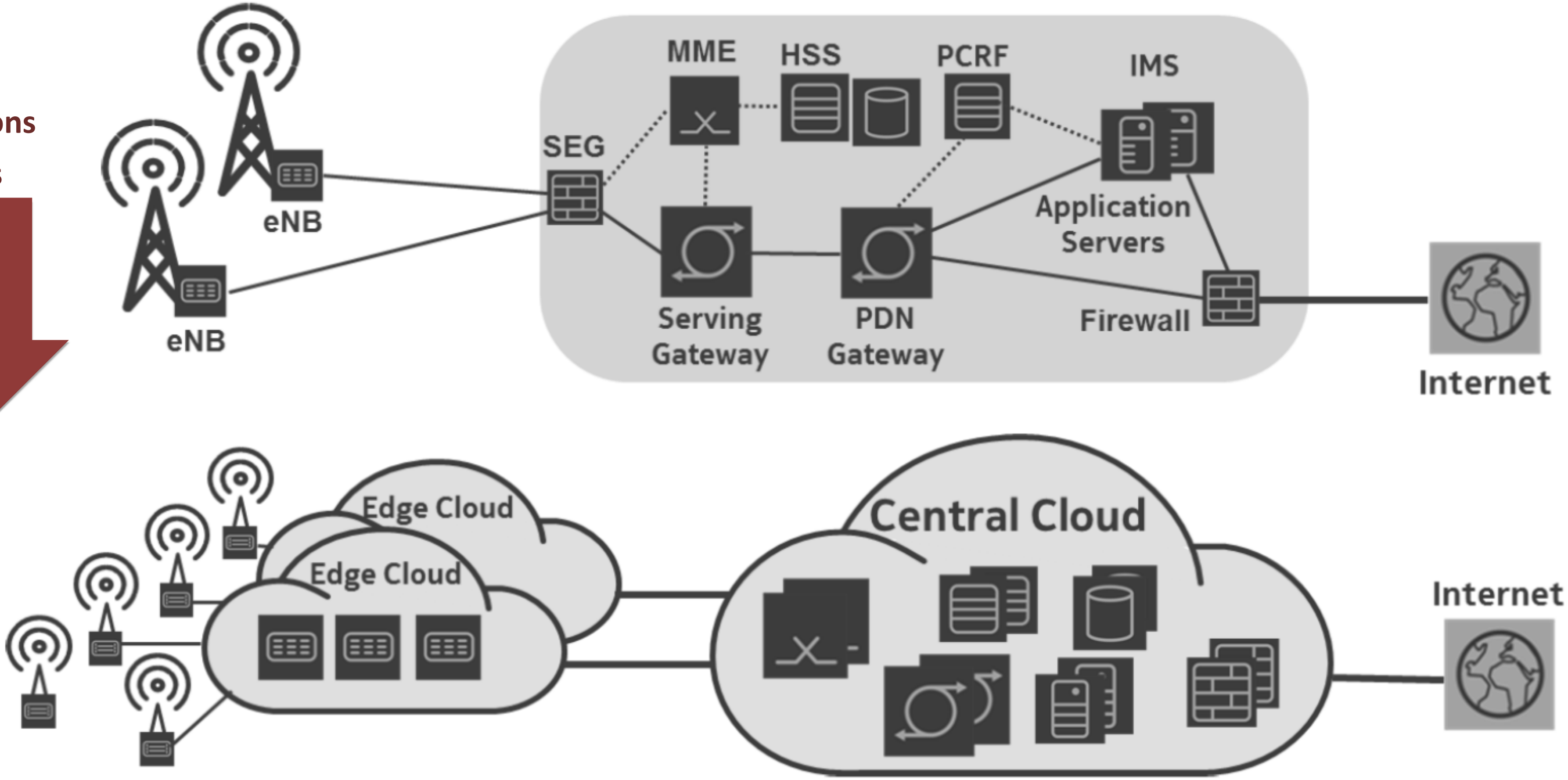
- threat and risk analysis per network element
- network element security architecture
- secure coding
- hardening
- security testing
- security audit
- security vulnerability monitoring
- patching process

Source: Nokia

From LTE zu 5G

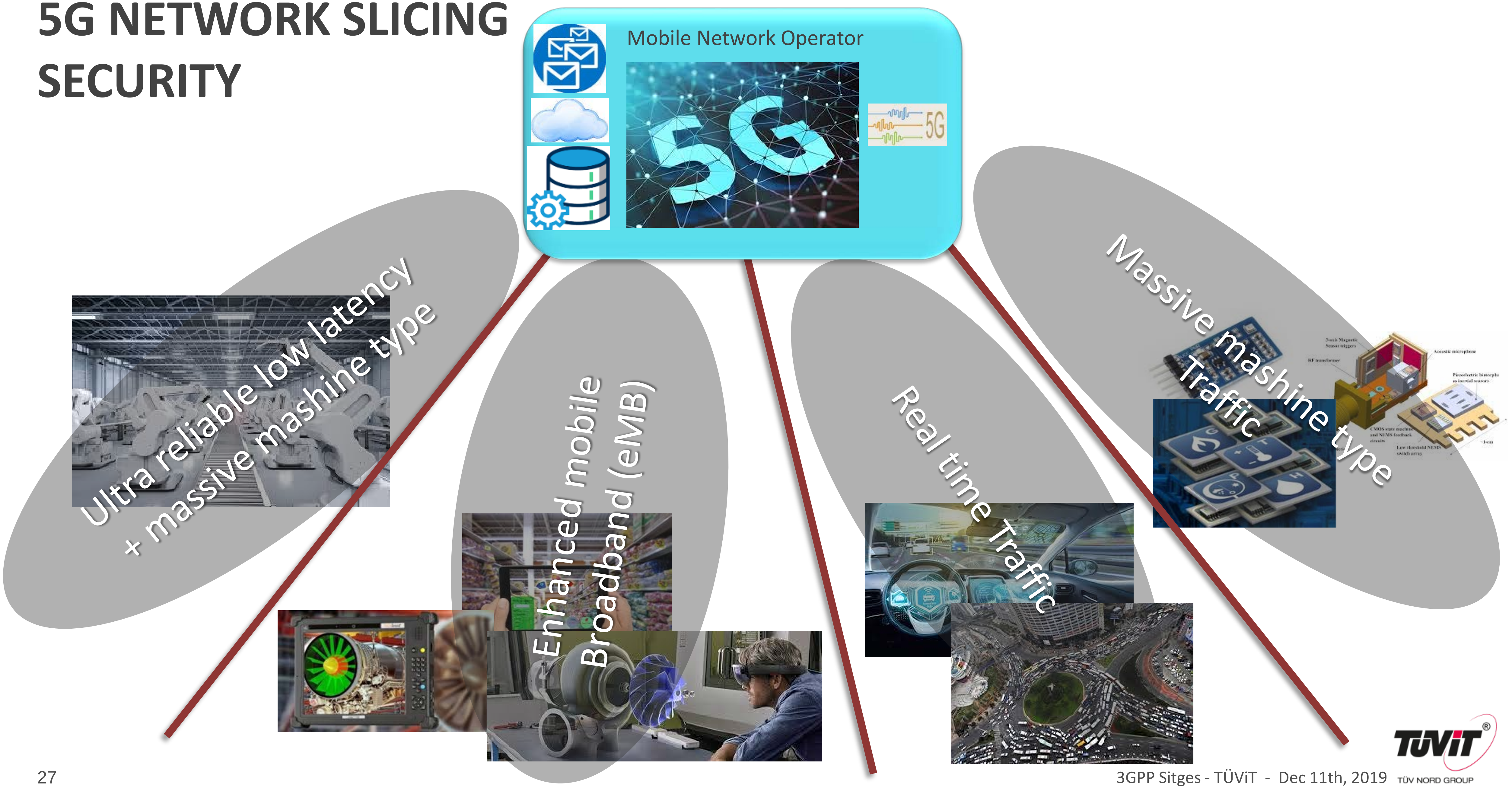
LTE fix funtions in components

5G virtual functions, software defined networking



Source: Nokia

5G NETWORK SLICING SECURITY



Mobile Network Operator

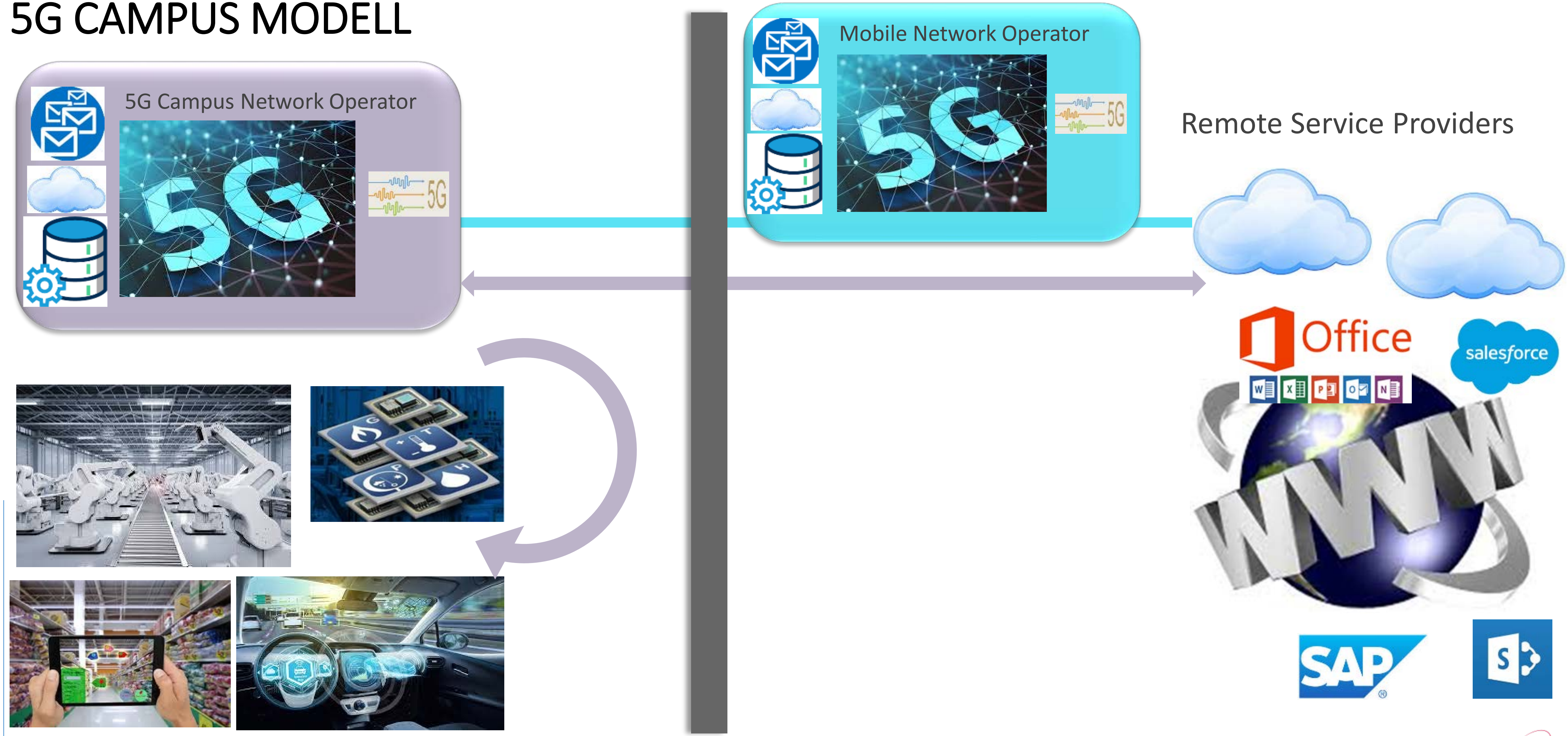
Ultra reliable low latency + massive mashine type

Enhanced mobile Broadband (eMB)

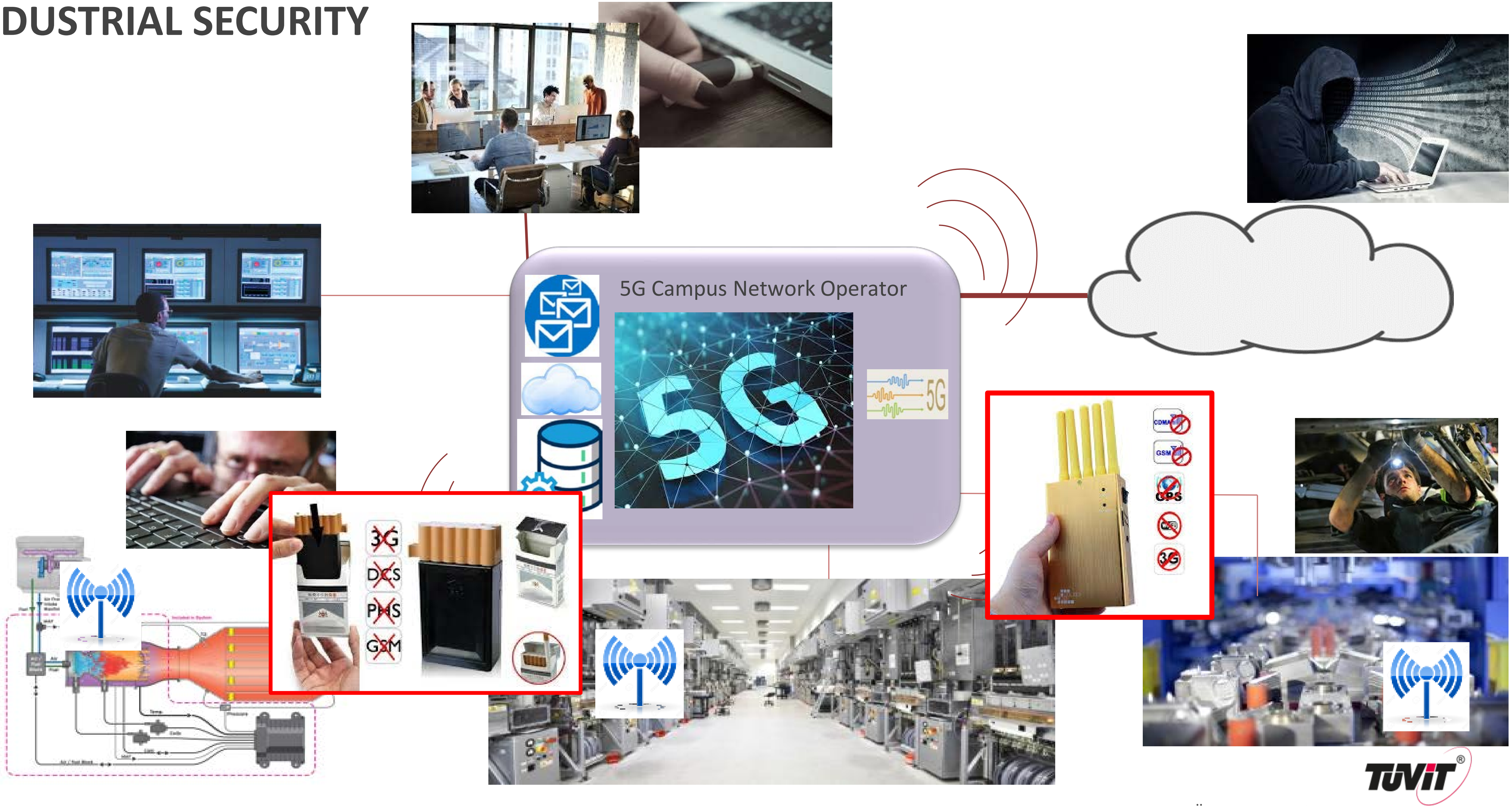
Real time Traffic

Massive mashine type Traffic

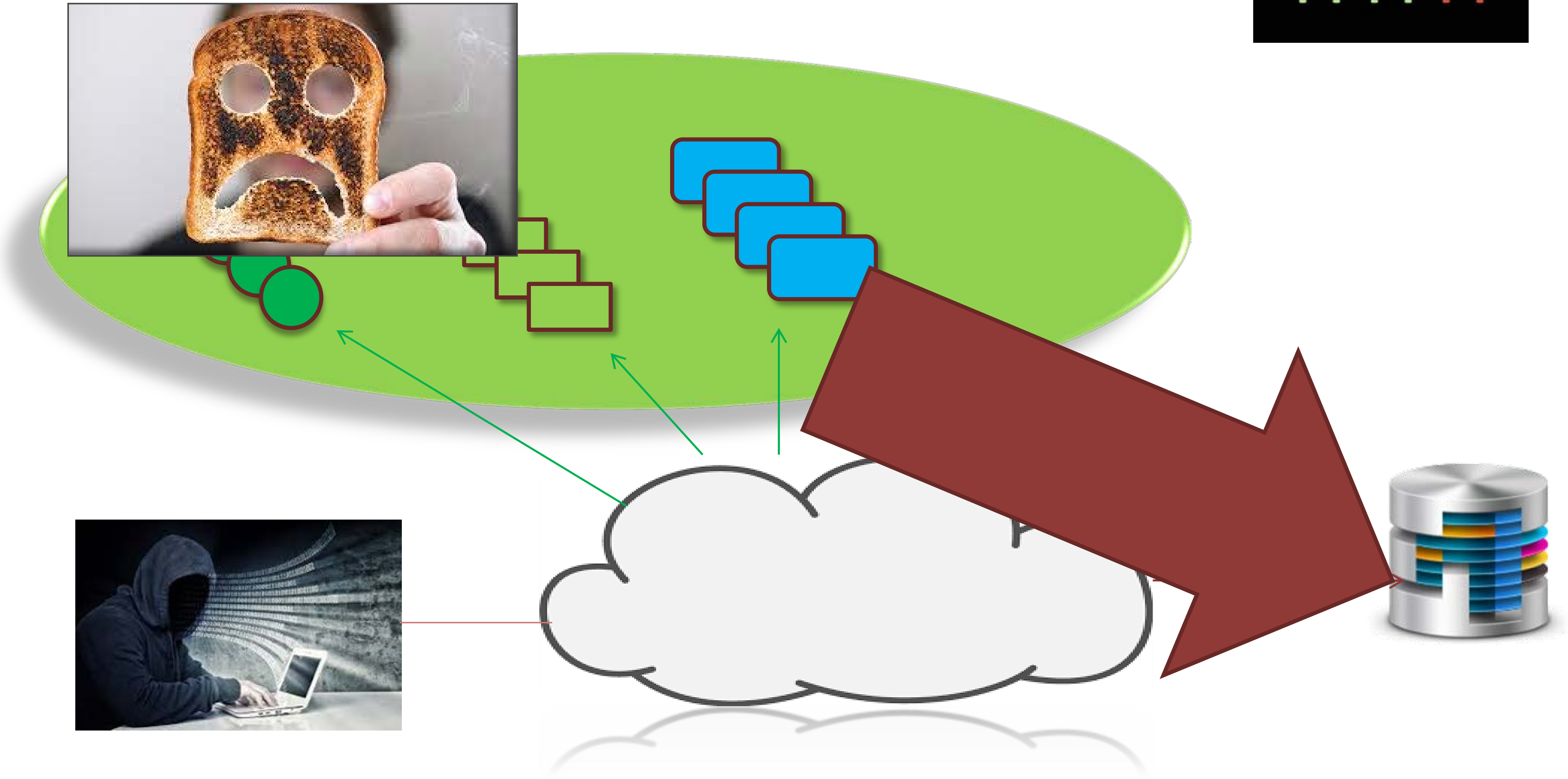
5G CAMPUS MODELL



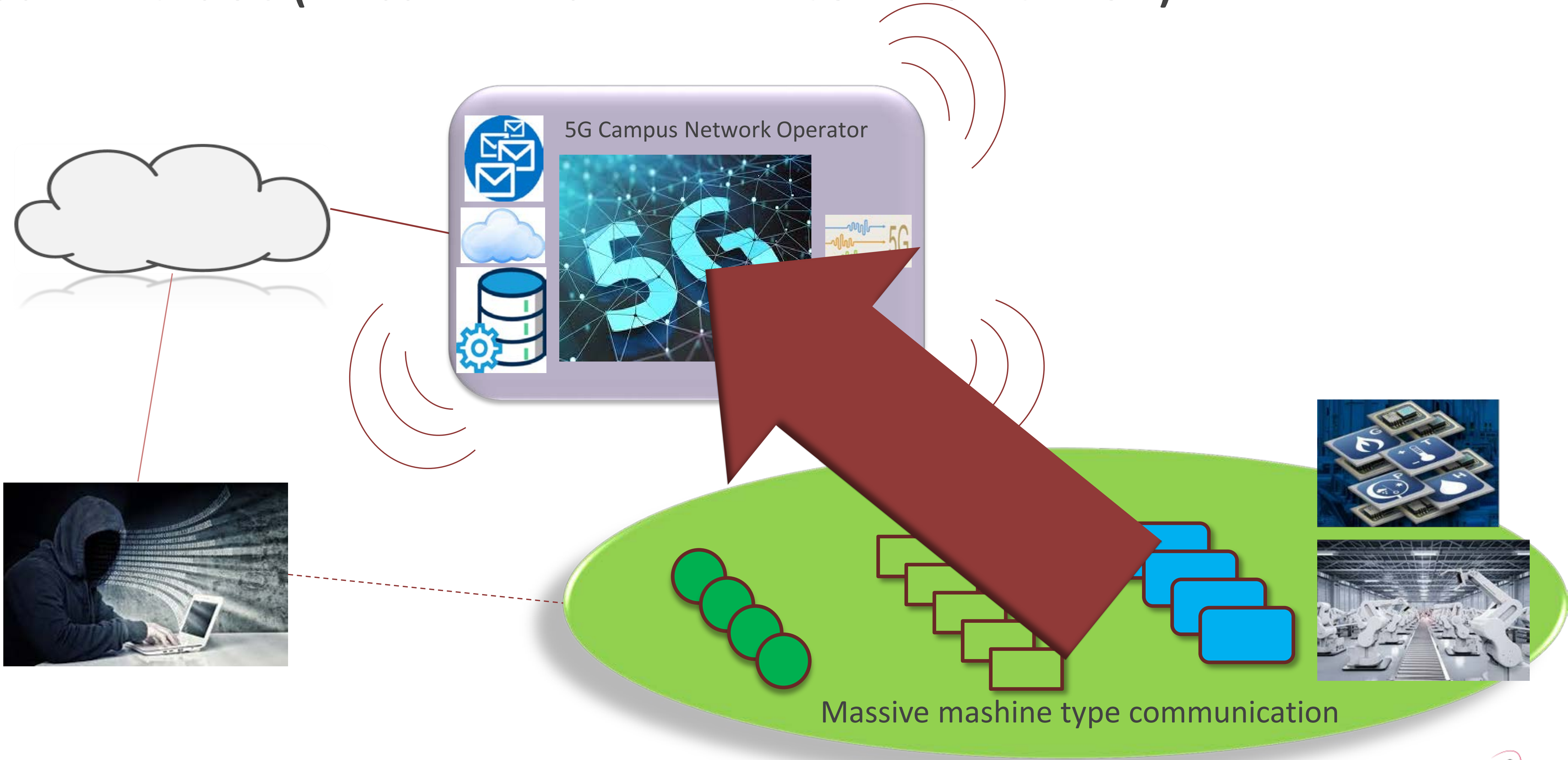
INDUSTRIAL SECURITY



„ATTACK OF THE SMART TOASTERS“



DDOS ATTACKS 5G (MASSIVE MASHINE TYPE COMMUNICATION)



5G Campus Network Operator

Massive mashine type communication

5G IS AN EVOLUTION OF THE 4G MOBILE COMMUNICATION SYSTEMS

5G security architecture is designed to integrate 4G equivalent security

security threats recognized in existing mobile network systems were attacks on

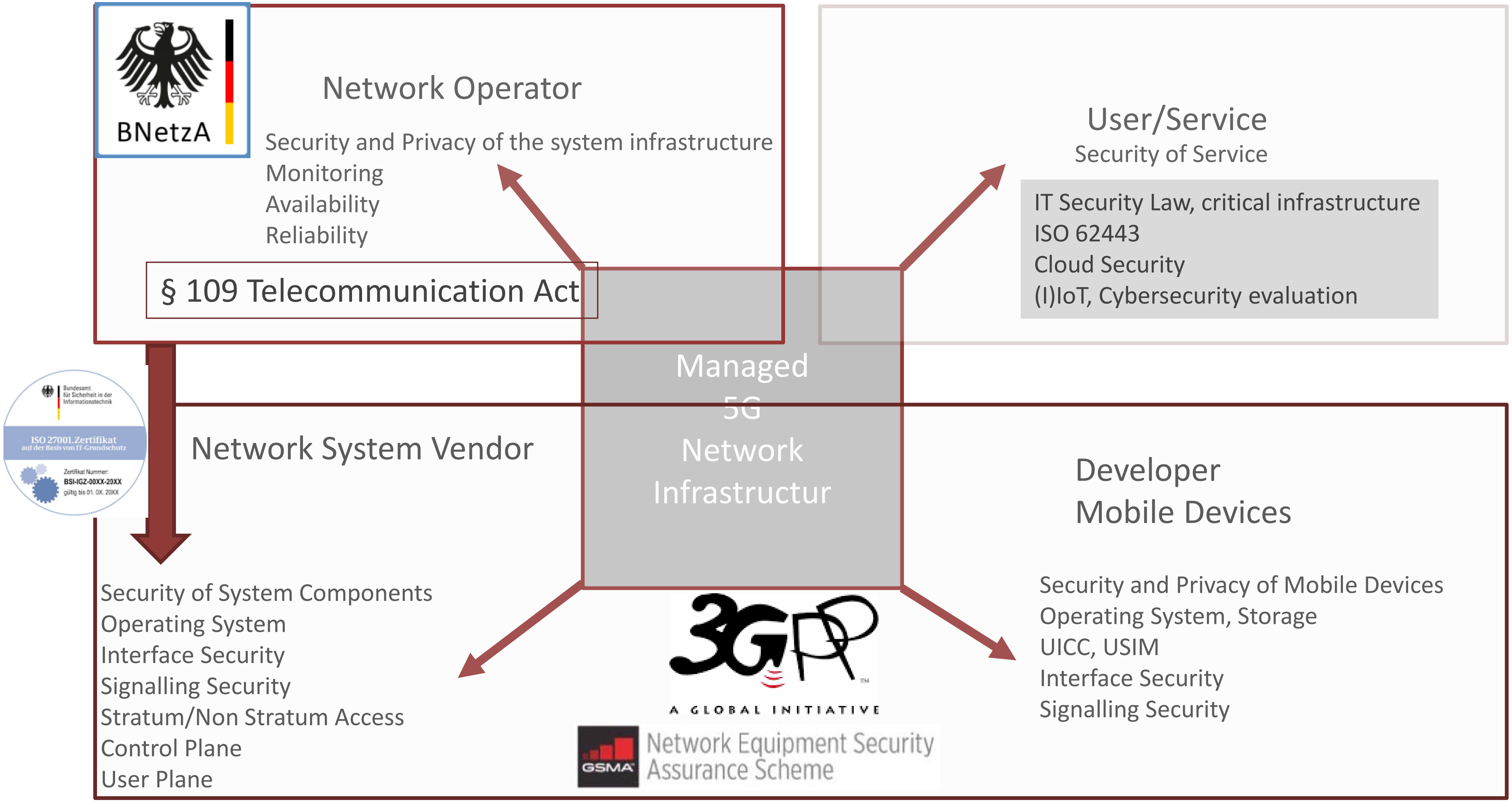
- **radio interfaces**
- **signaling plane**
- **user plane**
- **masquerading**
- **privacy**
- **replay**
- **bidding down**
- **man-in-the-middle**
- **inter-operator security**

5G should lead to further security enhancements

LTE-5G

Transition Assessment

GERMANY: COMPLEX 5G SECURITY TARGETS ECOSYSTEM


BNetzA
Bundesamt für Sicherheit in der Informationstechnik
ISO 27001-Zertifikat auf der Basis von IT-Grundschutz
Zertifikat Nummer: BSI-IGZ-00XX-20XX
gültig bis 01. 0X. 20XX
3GPP
A GLOBAL INITIATIVE
GSMA

Network Operator

Security and Privacy of the system infrastructure
Monitoring
Availability
Reliability

§ 109 Telecommunication Act

User/Service
Security of Service

IT Security Law, critical infrastructure
ISO 62443
Cloud Security
(I)IoT, Cybersecurity evaluation

Managed
5G
Network
Infrastructur

Network System Vendor

Security of System Components
Operating System
Interface Security
Signalling Security
Stratum/Non Stratum Access
Control Plane
User Plane

Network Equipment Security Assurance Scheme

Developer
Mobile Devices

Security and Privacy of Mobile Devices
Operating System, Storage
UICC, USIM
Interface Security
Signalling Security

NETWORK EQUIPMENT SECURITY ASSURANCE SCHEME (NESAS)

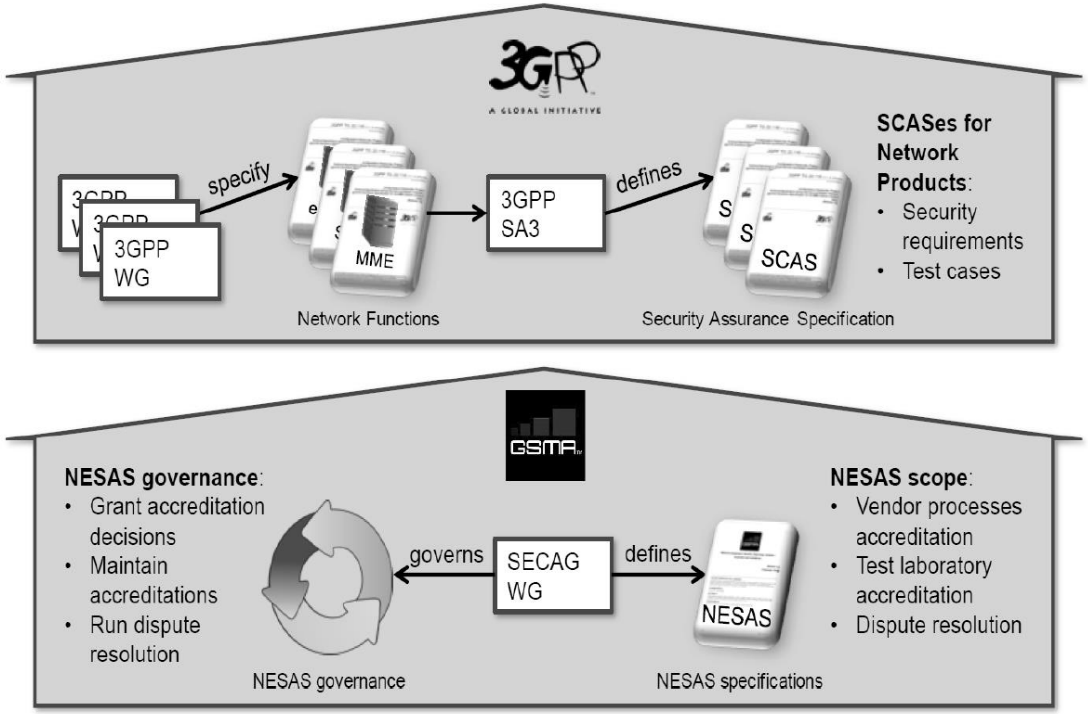
- NESAS is a voluntary scheme defined by 3GPP and GSMA for the mobile industry
- It provides a security baseline to evidence that network equipment satisfies a list of security requirements and has been developed according to standard guidelines
- NESAS consists of
  - (a) Audit and Accreditation of the security related development and product lifecycle processes of a vendor
  - (b) Security evaluation of network equipment by a competent test laboratory with defined and standardized security tests, which allows security levels to be objectively measured and visualized
    If these tests are performed by a recognized and competent test laboratory, a high quality and consistency of testing can be assured
- NESAS is currently running in pilot mode. On successful completion of the pilot the first official NESAS Release will be announced
- TUViT is currently in its application process to become a recognized competent test laboratory.

PROPOSAL OF APPROPRIATE STANDARDISATION BODIES AND AN INITIAL CERTIFICATION SCHEME

3GPP & GSMA as established 5G standardisation bodies have developed security tests for network components and NESAS as an security assurance scheme.

- Security testing is specified in Security Assurance Specifications (SCAS) by 3GPP based on the security functional requirements of the telecommunication components.

- GSMA defines and maintains the NESAS security and assurance scheme:
  - accreditation of the vendor development and product lifecycle processes,
  - NESAS Security Test Laboratory accreditation,
  - security evaluation of network equipment.



MME: Mobility Management Entity *(example for 5G specs)*
SA3: Security Working Group of 3GPP
SECAG: Security Assurance Group of GSMA

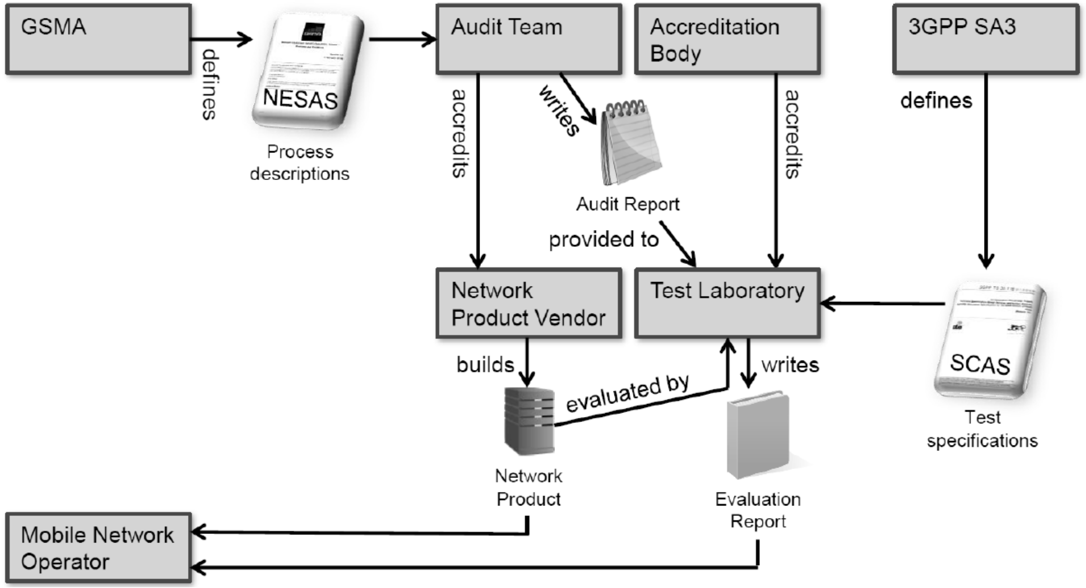
FURTHER DEVELOPMENT POTENTIAL OF NESAS

Pros:

- available and ready to use,
- known and accepted by manufacturers and operators,
- European standard via ETSI/3GPP agreement,
- under governance of the GSMA via the operators and therefore under influence of RSBs.

Cons:

- insufficient product security evaluation – *to be enhanced*,
- lack of control by regulatory and supervisory bodies
  - application of scheme is voluntary – *to be made mandatory*,
  - insufficient supervision of test labs and auditors – *to be qualified by RSBs*,
  - missing peer reviews to ensure comparability – *scheme to be completed*.



OUTLOOK

- Common Criteria (CC) is a governmental scheme and a natural candidate for being adopted by ENISA on European level as a Cybersecurity Certification Scheme under CSA
- NESAS by GSMA may be another Certification Scheme Proposal under CSA
- CC Assurance Level
  - high: certification by a public body, e.g. German BSI (federal office of IT security)
  - Substantial: certification by a private {or public} body, e.g. GSMA
  - (basic: vendor declaration or private body)

Elements of the 5G Security Architecture (3GPP)

Authentication/authorization, key agreement

- Security negotiation, key hierarchy
- Enhanced control plane robustness
- Enhanced subscription privacy

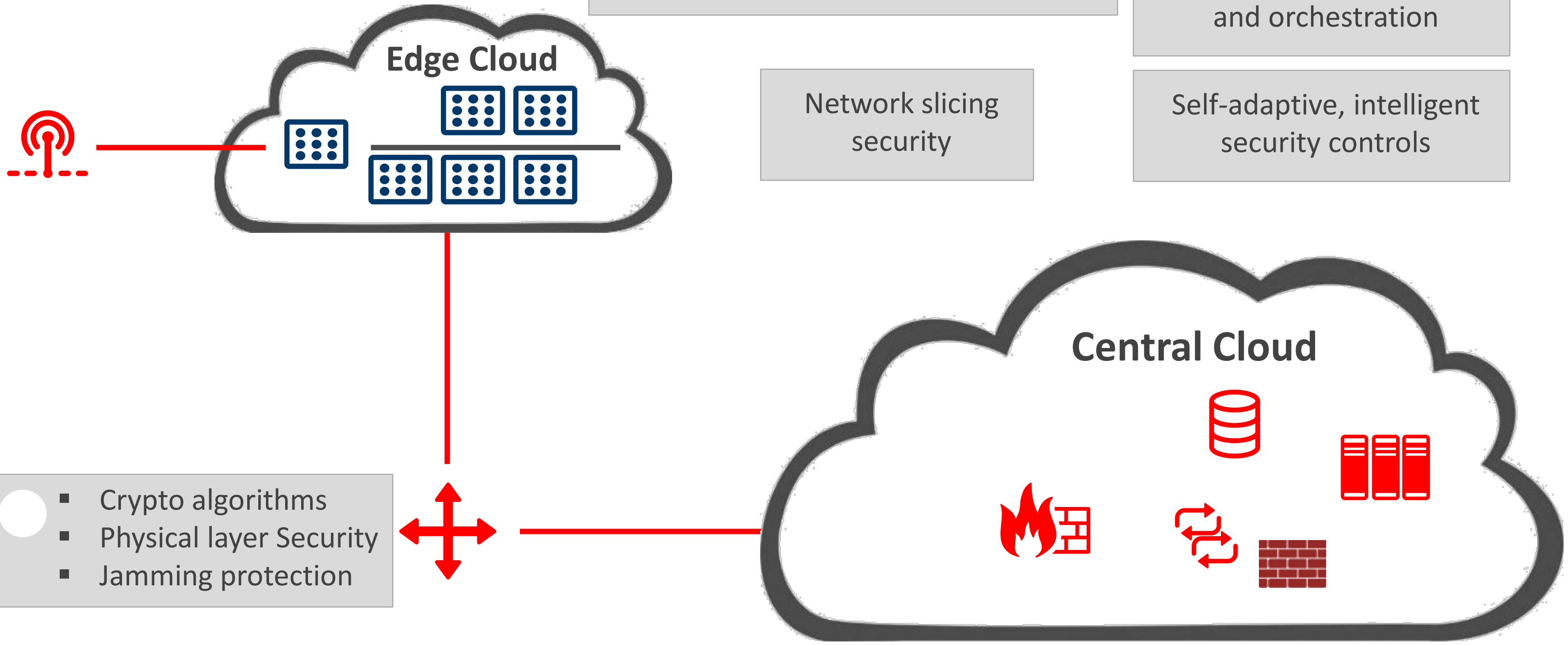
NFV (network function virtualization)
SDN (software defined network)
security

Security assurance for
NFV environments

Security management
and orchestration

Network slicing
security

Self-adaptive, intelligent
security controls



- Subscriber/device
- identifiers/credentials
- Secure Hardware

- Crypto algorithms
- Physical layer Security
- Jamming protection

PURE RISK BASED TRUST MODEL OF 3GPP

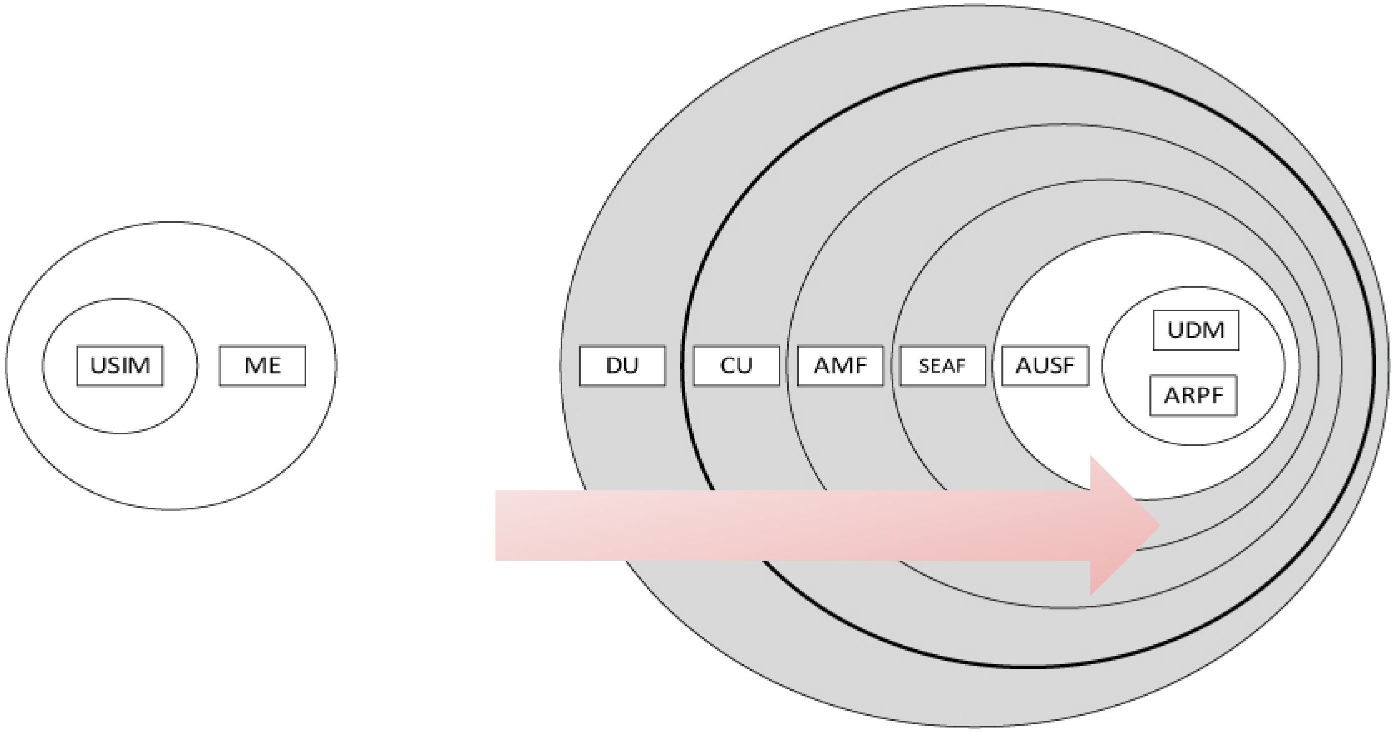


Figure 1 Trust model of non-roaming scenario

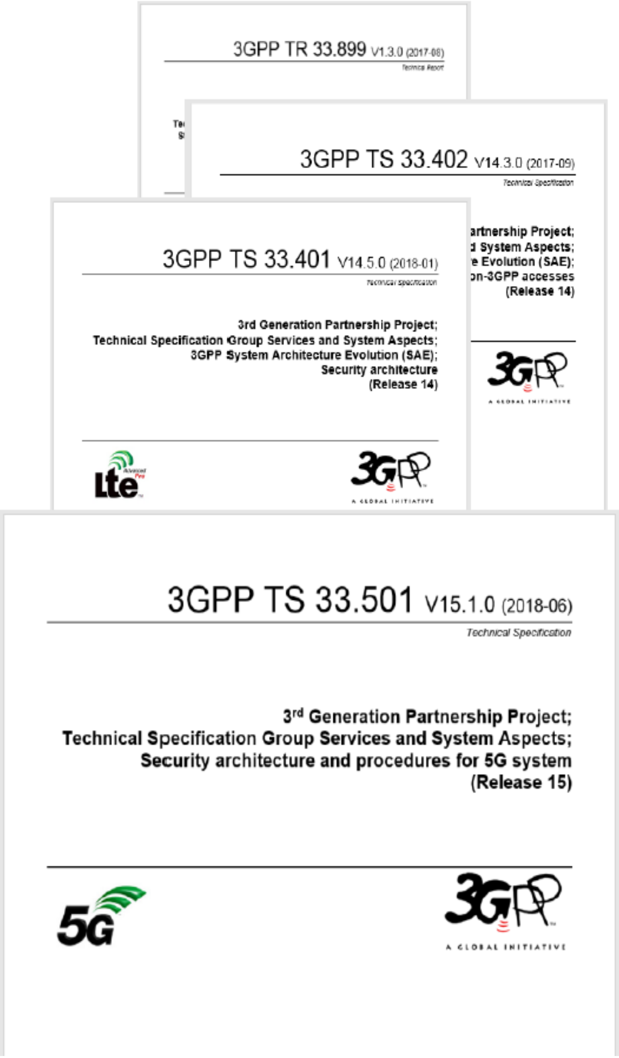
OVERVIEW 3GPP 5G SECURITY STANDARDIZATION

3GPP Technical Specification 33.501, Release 15
„Security Architecture and Procedures for 5G System“

new

New 5G security features at a glance:

- New access-agnostic authentication framework with improved home network control in roaming scenarios
- Enhanced subscription privacy
- User plane integrity protection
- EAP-based „secondary authentication“
- Security for service-based interfaces
- Enhancements for interconnection security



3GPP TR 33.899 V1.3.0 (2017-08)

Technical Report

3GPP TS 33.402 V14.3.0 (2017-09)

Technical Specification

artnership Project;
d System Aspects;
e Evolution (SAE);
on-3GPP accesses
(Release 14)

3GPP TS 33.401 V14.5.0 (2018-01)

Technical Specification

3rd Generation Partnership Project;
Technical Specification Group Services and System Aspects;
3GPP System Architecture Evolution (SAE);
Security architecture
(Release 14)

3GPP TS 33.501 V15.1.0 (2018-06)

Technical Specification

3rd Generation Partnership Project;
Technical Specification Group Services and System Aspects;
Security architecture and procedures for 5G system
(Release 15)

3GPP 5G SECURITY

- Primary authentication
- Secondary authentication
- Inter-Operator Security
- Privacy
- Service based architecture (SBA)
- Central Unit – Distributed Unit
- Key hierarchy
- Mobility

NUMBER OF KEY ELEMENTS IDENTIFIED BY EU MEMBER STATES

CATEGORIES OF ELEMENTS AND FUNCTIONS		EXAMPLES OF KEY ELEMENTS
Core network functions	**CRITICAL**	User Equipment Authentication, roaming and Session Management Functions
		User Equipment data transport functions
		Access policy management
		Registration and authorization of network services
		Storage of end-user and network data
		Link with third-party mobile networks
		Exposure of core network functions to external applications
		Attribution of end-user devices to network slices

NUMBER OF KEY ELEMENTS IDENTIFIED BY EU MEMBER STATES

CATEGORIES OF ELEMENTS AND FUNCTIONS		EXAMPLES OF KEY ELEMENTS
NFV management and network orchestration (MANO)	**CRITICAL**	
Management systems and supporting services (other than MANO)	**MODERATE/HIGH**	Security management systems
		Billing and other support systems such as network performance
Radio Access network	**HIGH**	Base stations

NUMBER OF KEY ELEMENTS IDENTIFIED BY EU MEMBER STATES

CATEGORIES OF ELEMENTS AND FUNCTIONS		EXAMPLES OF KEY ELEMENTS
Transport and transmission functions	**MODERATE/HIGH**	Low-level network equipment (routers, switches, etc)
		Filtering equipment (firewalls, IPS...)
Internetwork exchanges	**MODERATE/HIGH**	IP networks external to MNO premises Network services provided by third parties

OUR SERVICES – IT SECURITY

Critical infrastructure

Common Criteria

IT-Grundschutz

ISO 27001

Web Application Security

DataPrivacy

IT Security

Cyber Security

Security Lab

Smart Grid

Biometrics

Data Center Security

Penetration Testing

ISO 22301

Network Security

FIPS-140-2

Security4Safety

Mobile Security

Automotive Security