



## 5G campus networks – building blocks for digital sovereignty and crisis prevention

- Initial situation
- Focus topics
- Transformation

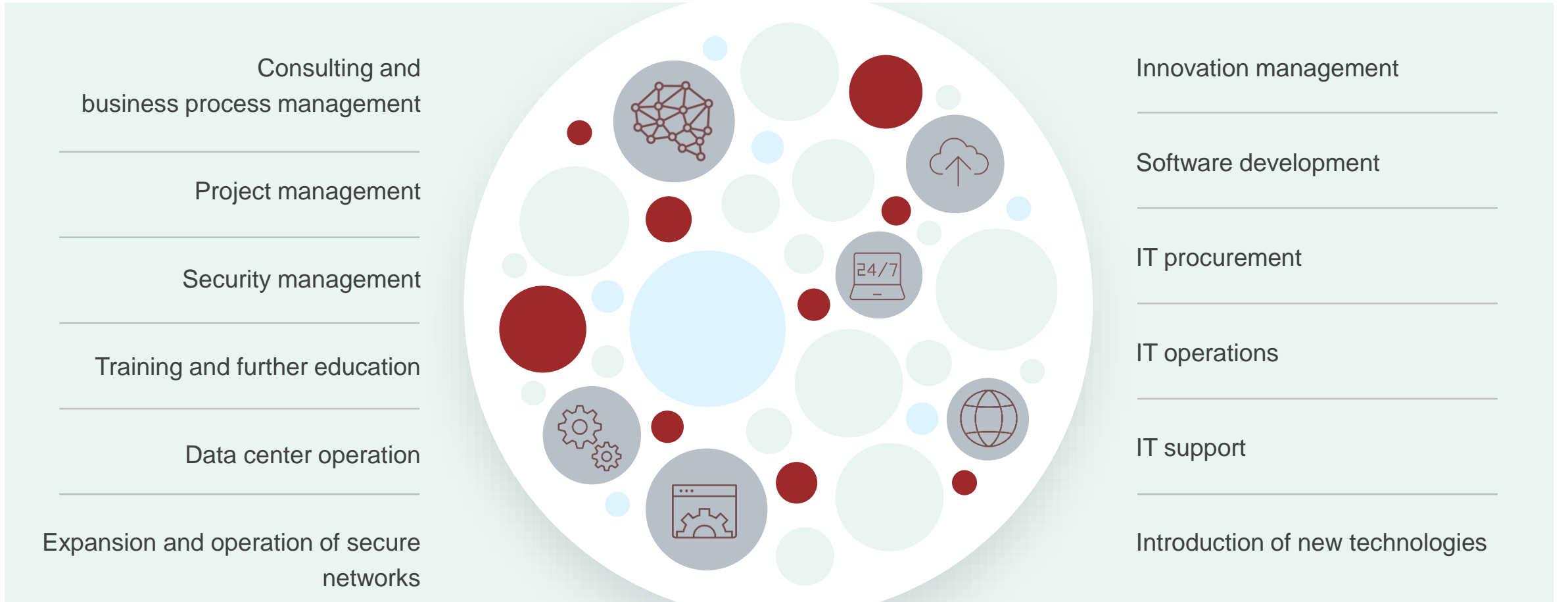
Peter Oelrichs, Dataport, 16.04.2024

# Dataport: IT service provider for federal states and municipalities

- The only federal state-crossing, public IT service provider in Germany
- The Dataport network comprises six federal states (SH, FHH, HB, ST, NI, MV) and the IT-Verbund Schleswig-Holstein
- Organizational form: Institution under public law



# Our mission: Partner for all digitization projects



# 5G campus networks – Building blocks for digital sovereignty and crisis prevention

Initial situation (1/2):

- Rapidly advancing digitalization -> increasing tactical requirements
- Applications invariably via the public mobile networks
- Network resilience is not designed for the increased requirements of BOS
  - Commercial mobile networks not subject to hardening
- Availability of a self-controlled, dedicated BDBOS network from mid-2030 at the earliest



# 5G campus networks – Building blocks for digital sovereignty and crisis prevention

Initial situation (2/2):

- private 5G-networks can be set up specifically according to the
  - digital sovereignty
  - services of general interest
  - crisis resiliencedesigned and operated under its own control.
- Black case as a specific threat situation
- Growing influence of 5G Release 3GPP standard with new features (MCX) on end devices/services



# 5G campus networks – Building blocks for digital sovereignty and crisis prevention

Focus topics:

## 1. Multi Operation Core Network (MOCN)

Integration RAN of a public 5G mobile network into a hardened p5G network

## 2. Mission Critical Services (MCX services)

New 5G Release 3GPP: push-to-talk, QoS, MCData, MCVideo, MCVoice

## 3. Centralized Unified Endpoint Management (UEM) system

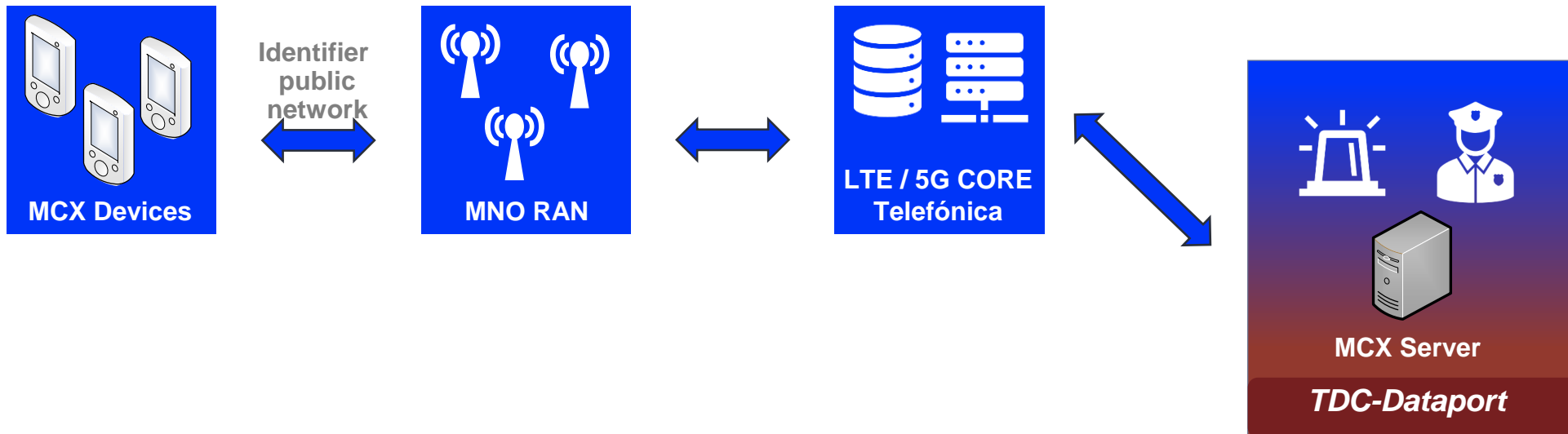
Administration of end devices and services in the changed network using a central UEM system

– Technical, legal, regulatory, organizational and procedural aspects as well as IT security must be taken into account.

# 5G campus networks – Building blocks for digital sovereignty and crisis prevention

## Multi Operation Core Network (MOCN)

### 1. Current standard operation "broadband" in the public mobile network

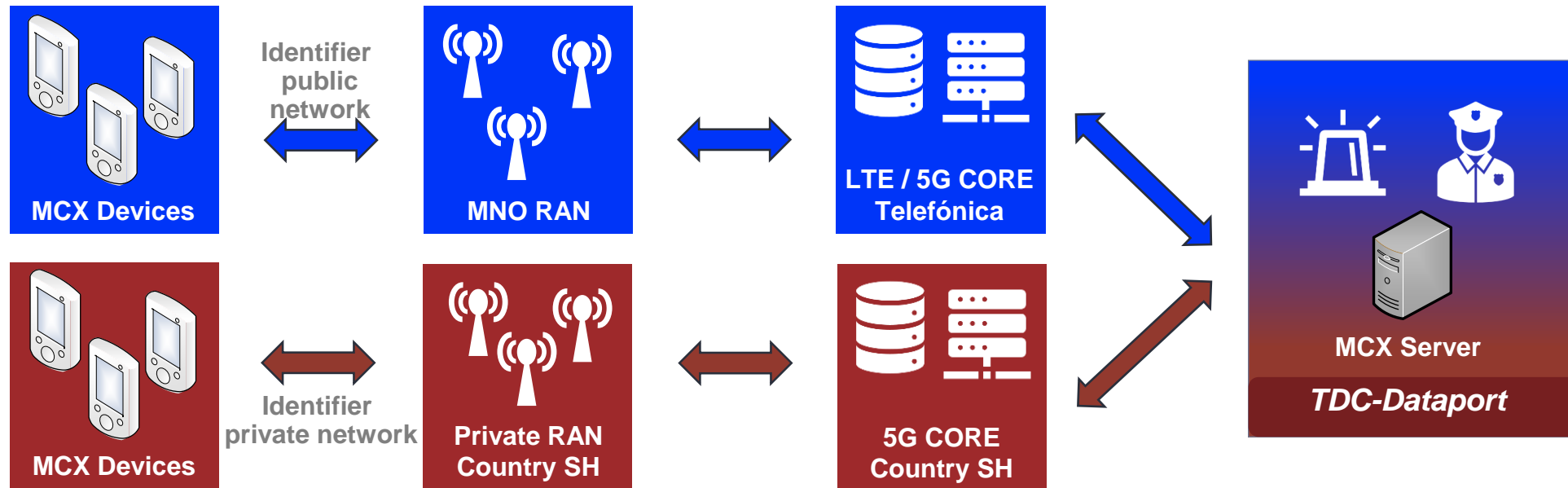


– Network slicing/QoS to secure the available system resources

# 5G campus networks – Building blocks for digital sovereignty and crisis prevention

## Multi Operation Core Network (MOCN)

### 2. Parallel operation of public mobile network // p5G



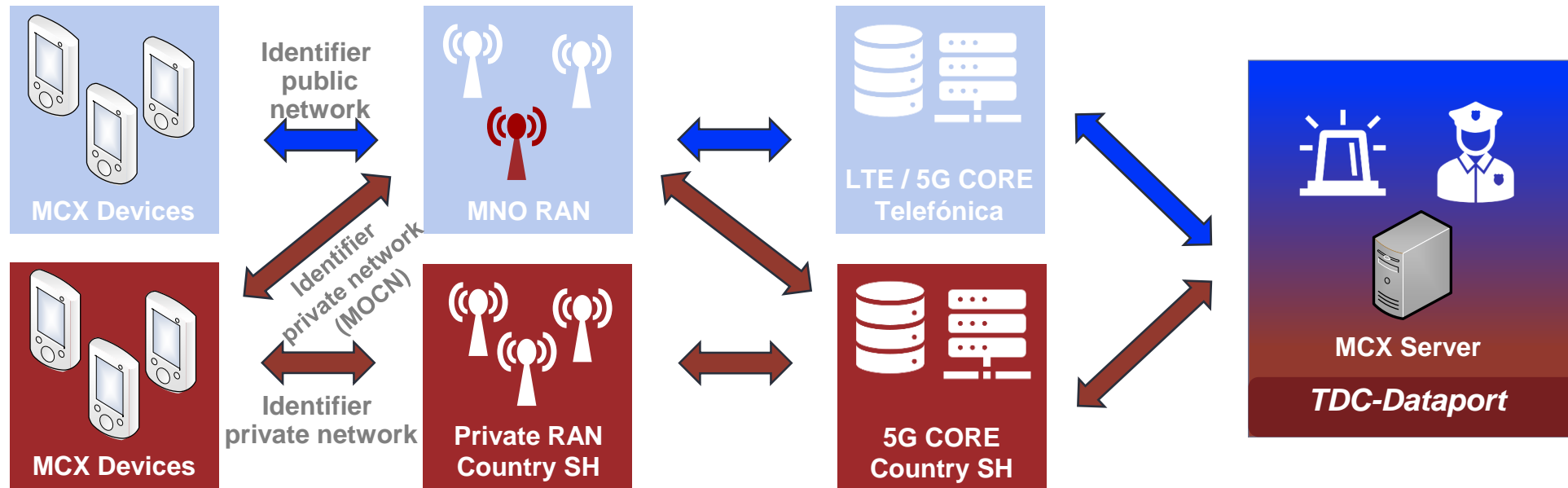
- Closed p5G campus network; exclusive availability of all resources and data sovereignty
- Interoperability, e.g. through dual SIM devices



# 5G campus networks – Building blocks for digital sovereignty and crisis prevention

## Multi Operation Core Network (MOCN)

### 3. Integration of RAN in p5G



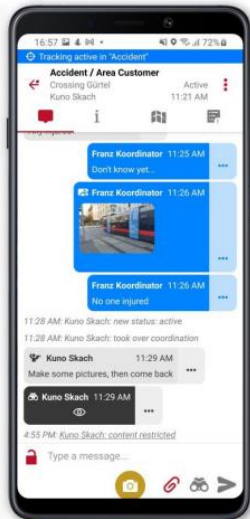
— Extended p5G campus network exclusive availability of all resources and data sovereignty

# 5G campus networks – Building blocks for digital sovereignty and crisis prevention

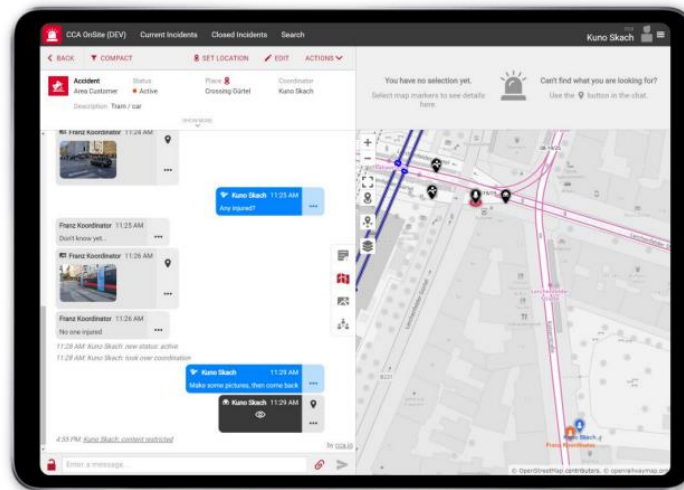
Mission Critical Services (MCX services)

5G Standard 3GPP:  
push-to-talk, QoS, MCDATA, MCVideo, MCVoice

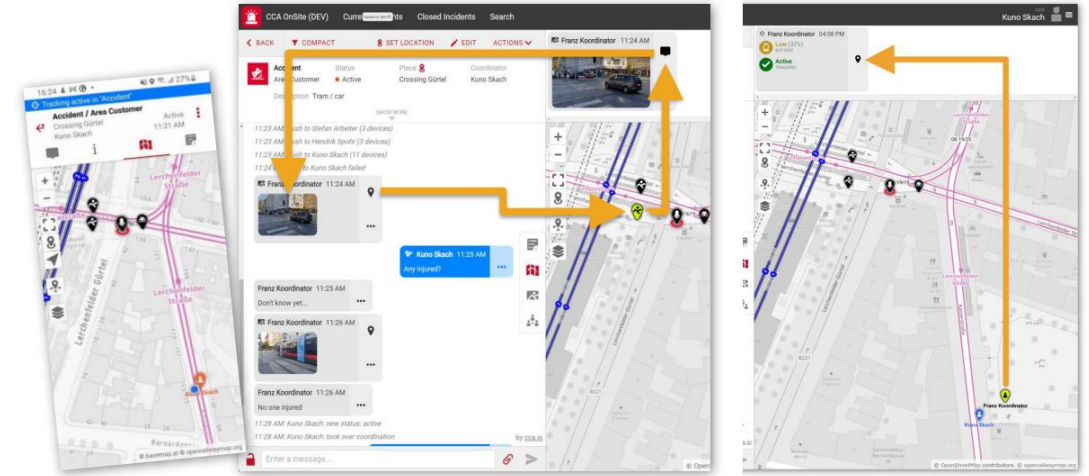
User Clients



Mobile App  
for mobile users



Web App for tablet & PC  
for coordinator, control center or management



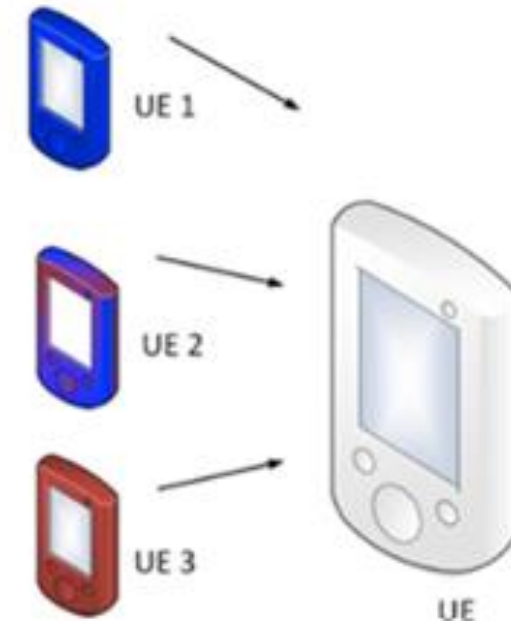
MissionX:  
End-to-end communication without media discontinuity  
across the entire IT network

Source: [www.FREQUENTIS.com](http://www.FREQUENTIS.com)

# 5G campus networks – Building blocks for digital sovereignty and crisis prevention

## Centralized Unified Endpoint Management (UEM) system

- Validation and use of standardized end devices
- Provision, configuration and management of new MCX applications via the central Unified Endpoint Management (UEM) system
- Subscriber management: prioritization for regular operation and in case of a crisis
- Consolidation of end device management



# 5G campus networks – Building blocks for digital sovereignty and crisis prevention

Dataport strives to ensure that

- the proposed solution can be designed holistically across the entire IT network using the example of Schleswig-Holstein,
- works end-to-end in the PoC,
- the essential requirements of a pilot user are consistently met
- the basis for a later transformation of the solution at federal level can be laid through conception and documentation
- digital sovereignty in the sense of public services of general interest in the future can also be ensured with regard to self-controlled digital infrastructures and services

Thank you very much for your attention!

Peter Oelrichs

Solutions Digital Infrastructures, LD13/01

[peter.oelrichs@dataport.de](mailto:peter.oelrichs@dataport.de)

Phone: +49 40 42846-2616