UKD Universitätsklinikum Düsseldorf

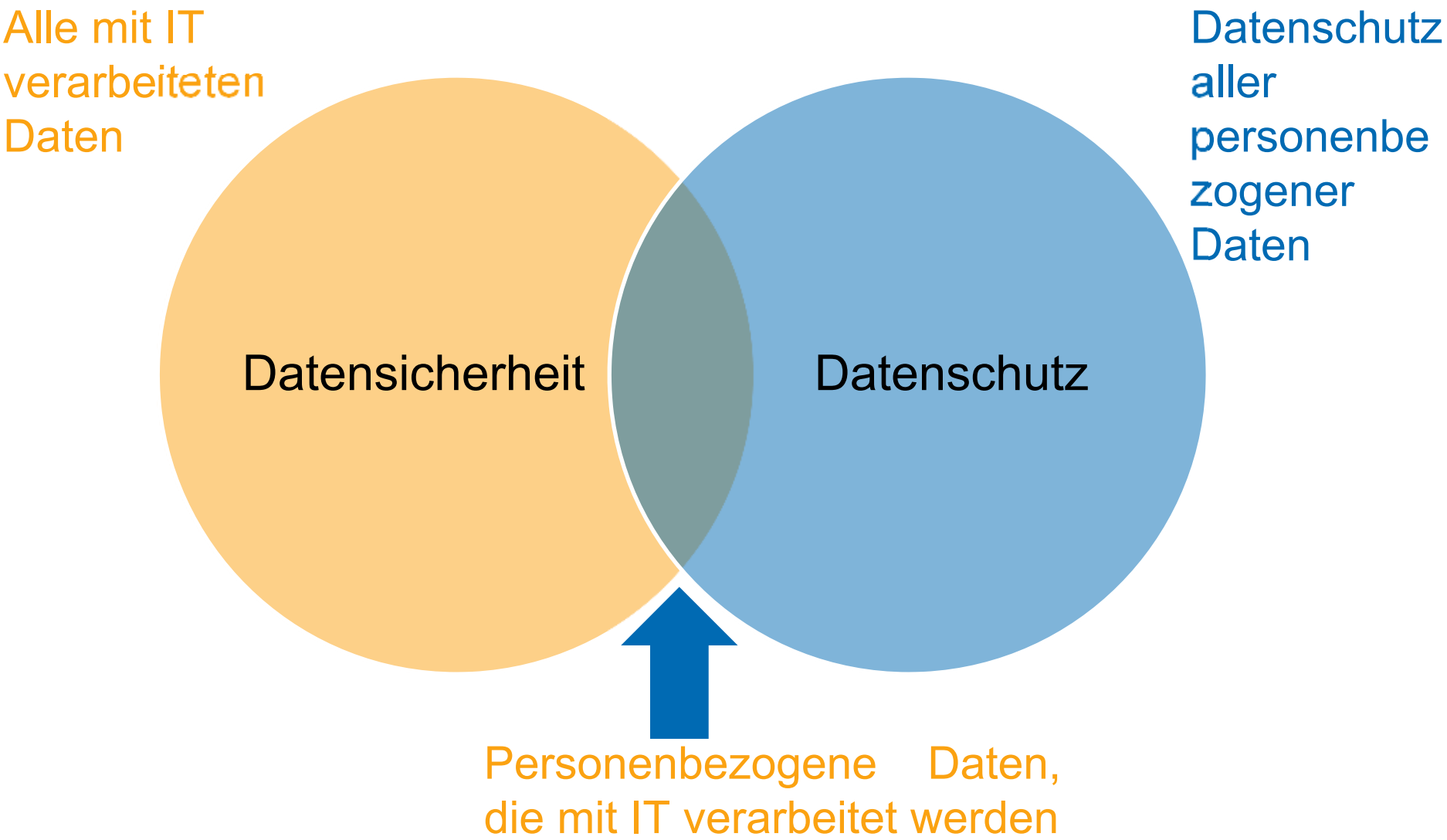
hhu Heinrich Heine Universität Düsseldorf

GIGA FOR HEALTH x EURIALE - Datenschutz

Dr. Jenny Roßbach
Datenschutzbeauftragte des UKD
Leitung Stabsstelle Datenschutz

jenny.rossbach@med.uni-duesseldorf.de
0211 – 81 18419

Datenschutz und Datensicherheit



Datenschutz – Grundsätzlich

informationelle Selbstbestimmung jedes Einzelnen

Personenbezogene/ Personenbeziehbare Daten

Personenbezogene Daten

Name

Adresse

IP-Adresse

Geburtsjahr

Telefon-nummer

Politische Meinung

Besondere Kategorien (Art. 9 DSGVO)

Ethnische Herkunft

Religiöse Überzeugung

Gesundheit

Sexual-leben

Ziele Datenschutz:

- Verfügbarkeit
- Vertraulichkeit
- Zweckbindung/ Datenminimierung
- Transparenz
- Integrität

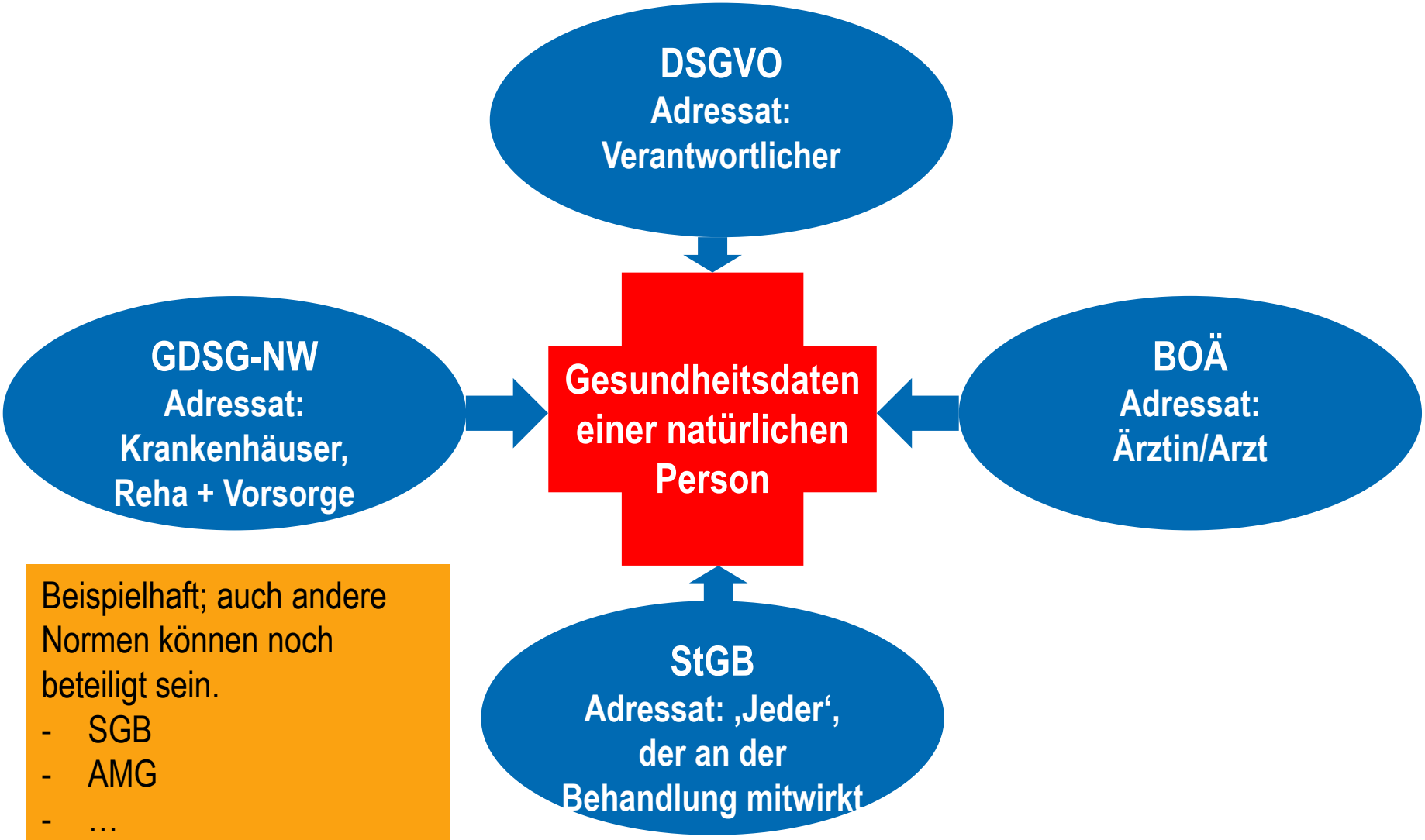
Bes. Kategorien – Bes. Sicherheitsstandards

Unter besonderen Voraussetzungen erlaubt

- Zugriffsprotokollierung
- Sensibilisierung der beteiligten Mitarbeiter
- Pseudonymisierung
- Benennung von Datenschutzbeauftragten
- Implementierung von TOMs
- …

Besondere Kategorien (Art. 9 DSGVO)

Datenschutz – im Gesundheitswesen

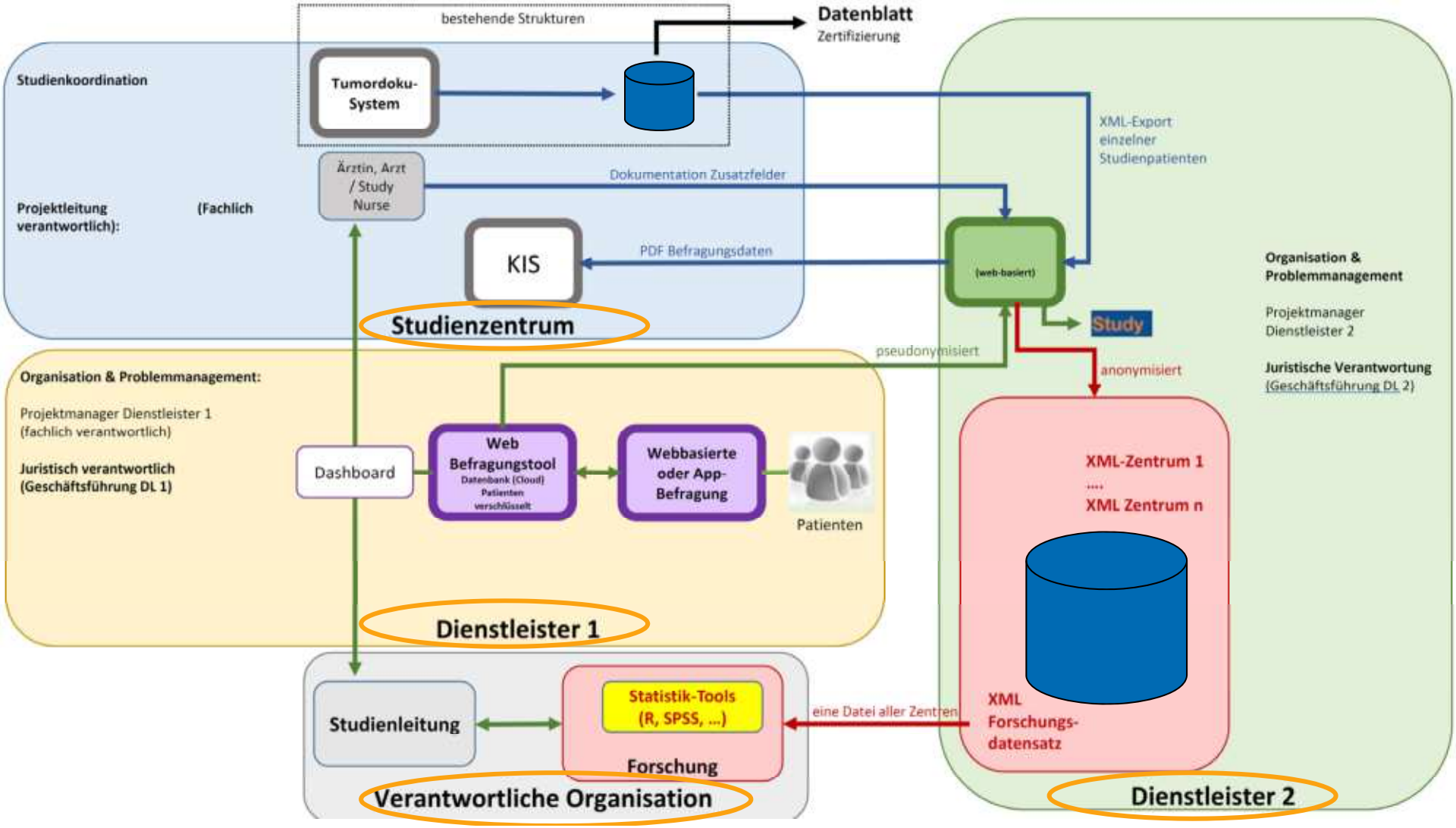


Beispielhaft; auch andere Normen können noch beteiligt sein.

- SGB
- AMG
- …

Datenverarbeitung – im Gesundheitswesen

Neue Projekte: Datenflüsse müssen bekannt sein – dem Fachverantwortlichen



Datenverarbeitung – im Gesundheitswesen

Zusammenarbeit von mehreren Rechtspersonen: Datenübermittlung beachten

- Datenempfänger ist Auftragsverarbeiter (gemäß Art. 28 DSGVO)
- Datensender und –empfänger sind gemeinschaftlich Verantwortliche (gemäß Art. 26 DSGVO)
- Datensender und –empfänger sind jeweils eigenständige Verantwortliche

Internationaler Datentransfer

- Drittland (Regelungen zur Datenübermittlung in Drittländer)
  - Keine Kontrolle über das Datenschutzniveau im Zielland
  - EU-Recht greift nicht im Drittland
  - Der Schutz der betroffenen Person muss auch im Drittland gewährleistet sein

Datenverarbeitung – im Gesundheitswesen

Internationaler Datentransfer

- Drittland (Regelungen zur Datenübermittlung in Drittländer)
  - Keine Kontrolle über das Datenschutzniveau im Zielland
  - EU-Recht greift nicht im Drittland
  - Der Schutz der betroffenen Person muss auch im Drittland gewährleistet sein

Voraussetzung

- Datenübermittlung aufgrund eines Angemessenheitsbeschluss (Art. 45 DSGVO)
- Datenübermittlung vorbehaltlich geeigneter Garantien (Art. 46 DSGVO)
- Ausnahmen von Art. 45 und 46 DSGVO (Art. 49 DSGVO; z.B. eine Einwilligung)

Datenverarbeitung – im Gesundheitswesen

Beispiel: US- amerikanischer Cloudanbieter mit Rechenzentrum in Irland als Auftragsverarbeiter

Datenzugriff kann gem. **CLOUD Act** aus den USA erfolgen

- Es liegt kein Angemessenheitsbeschluss gem. Art. 45 DSGVO vor
- Voraussetzung sind geeignete Garantien gem. Art. 46 DSGVO
- Es liegen keine Ausnahmen gem. Art. 49 DSGVO vor
- Abschluss von EU-Standardvertragsklauseln (04.06.2021) Modul 2

Zusätzliche Garantien:
Verschlüsselung der Daten ohne Zugriff des Dienstleisters auf die Daten des Schlüssels (at rest) .

Datenverarbeitung – im Gesundheitswesen

Wichtig:

Für die Vorabprüfung von Verfahrenstätigkeiten:
Daten und Datenflüsse genau kennen

- Geeignete Maßnahmen (Verschlüsselung/ Pseudonymisierung, etc.) ergreifen
- Bei möglichem hohem Risiko ist vorab eine Datenschutzfolgenabschätzung durchzuführen.

https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Informationen-und-Empfehlungen/5-G/Absicherung-5G-Campusnetze/IT-Grundschutz/IT-Grundschutz-Absicherung-5G-Campusnetze.html

Geschafft!

❤-lichen Dank für Ihre Aufmerksamkeit!

IT Sicherheit mit 5G

TBS- Robin Friedrich
Manager Converged Network Development, Vodafone GmbH

Robin Friedrich
Manager Converged Network Development, Vodafone GmbH

Desk: +49 211 533 1806
Mobile: +49 172 2663860
Email: Robin.Friedrich@vodafone.com

Vodafone GmbH
Ferdinand-Braun-Platz 1
40549 Düsseldorf

5G | ITU-Anforderungen an die 5. Generation

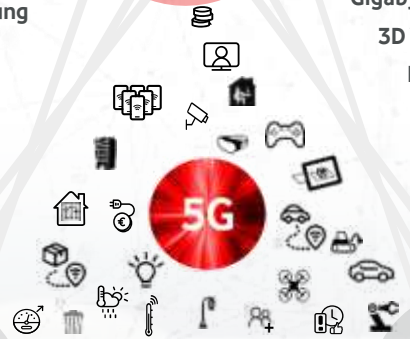
eMBB — Enhanced Mobile Broadband

Gigabytes in Sekunden
3D Video, 4k/8k UHD, Hologramm
Real Time Cloud Gaming
Augmented/Virtual Reality
Kran-& AGV Steuerung
Autonomes Fahren
Automatisierte Fertigung
Missionskritische Anwendungen

Vernetzter Rettungswagen

Fernchirurgie

Fern-Video Konsultationen



mMTC — Massive Machine-Type Communication

Videoüberwachung
Gebäude-Automatisierung
Intelligente Gebäude
Tracking
Zählerstände

Sichere Umgebungen

Asset-Tracking-Lösung

cMTC — Critical Machine-Type Communication

Verkehrssicherheit
- & Kontrolle

Sensore

Patient
onitoring

Patientenüberwachung mit IoT-Sensoren

5G bietet Möglichkeiten für innovative Gesundheitsversorgung

Native Security

SIM basierte Security bietet Anonymisierung von Anwender-daten und hohen Grad an Datenverschlüsselung.

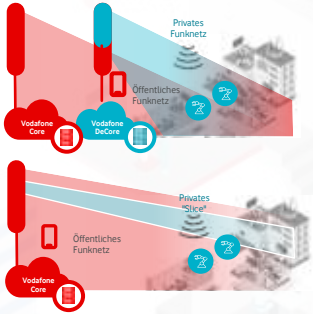
Hohe Kapazität

Hohe Bandbreiten von theoretisch bis zu 1 Gbps im Download möglich. Mit neuen, höheren Frequenzen bis zu 10 Gbps. Sowie hohe Kapazitäten für massive Gerätedichte

Kurze Latenzen & MEC

Geringe Latenzzeit von wenigen Millisekunden, somit optimal für zeit- & missionskritische Anwendungen geeignet.

Campus Netze & Slicing



Dedizierte, individuelle Nutzung von Mobilfunk Ressourcen mittels „lokaler Campus Netze“ oder im öffentlichen Netz mittels „Slicing“.

Coverage & Störfestigkeit

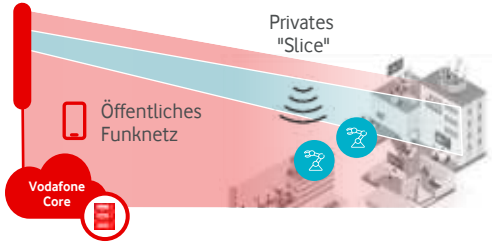
Nicht nur Indoor, sondern auch Outdoor und bundesweit verfügbar. Störfestigkeit durch lizensierter Bänder.

... und weitere Services und technisches Möglichkeiten in einem mobilem, globalem Standard der stetig weiterentwickelt wird

Sichere Netze für eHealth

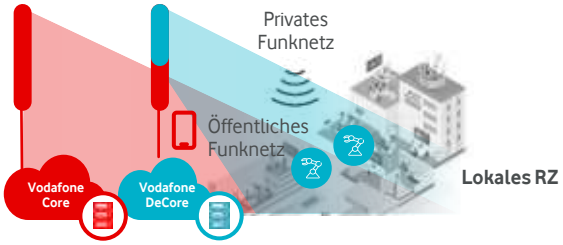
01

Campus-Netze | Portfolio Vodafone Business Campus

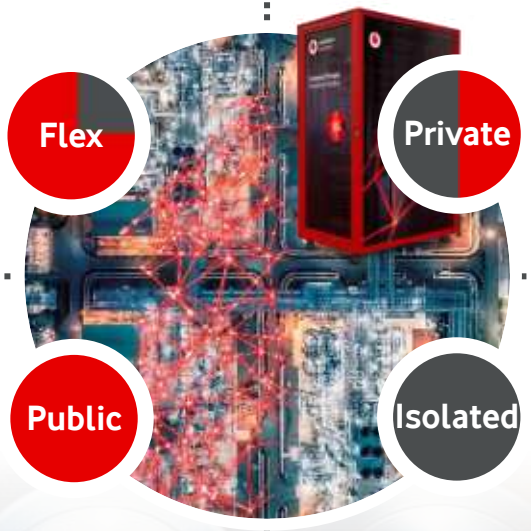


Vodafone-Frequenzen

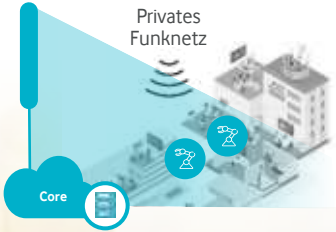
Klinik-Campus



Vodafone- und Industrie-Frequenzen

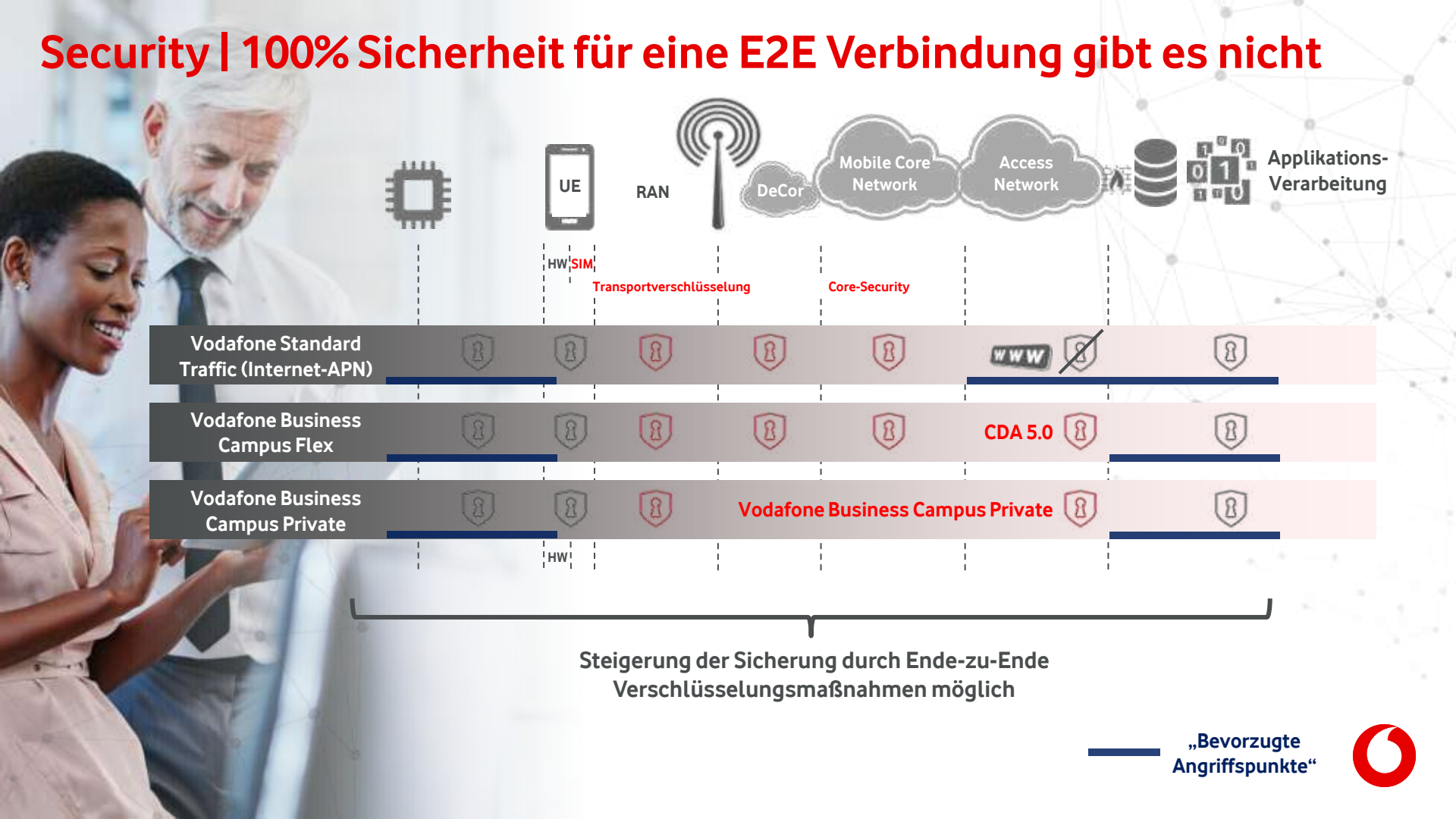


Vodafone-Frequenzen



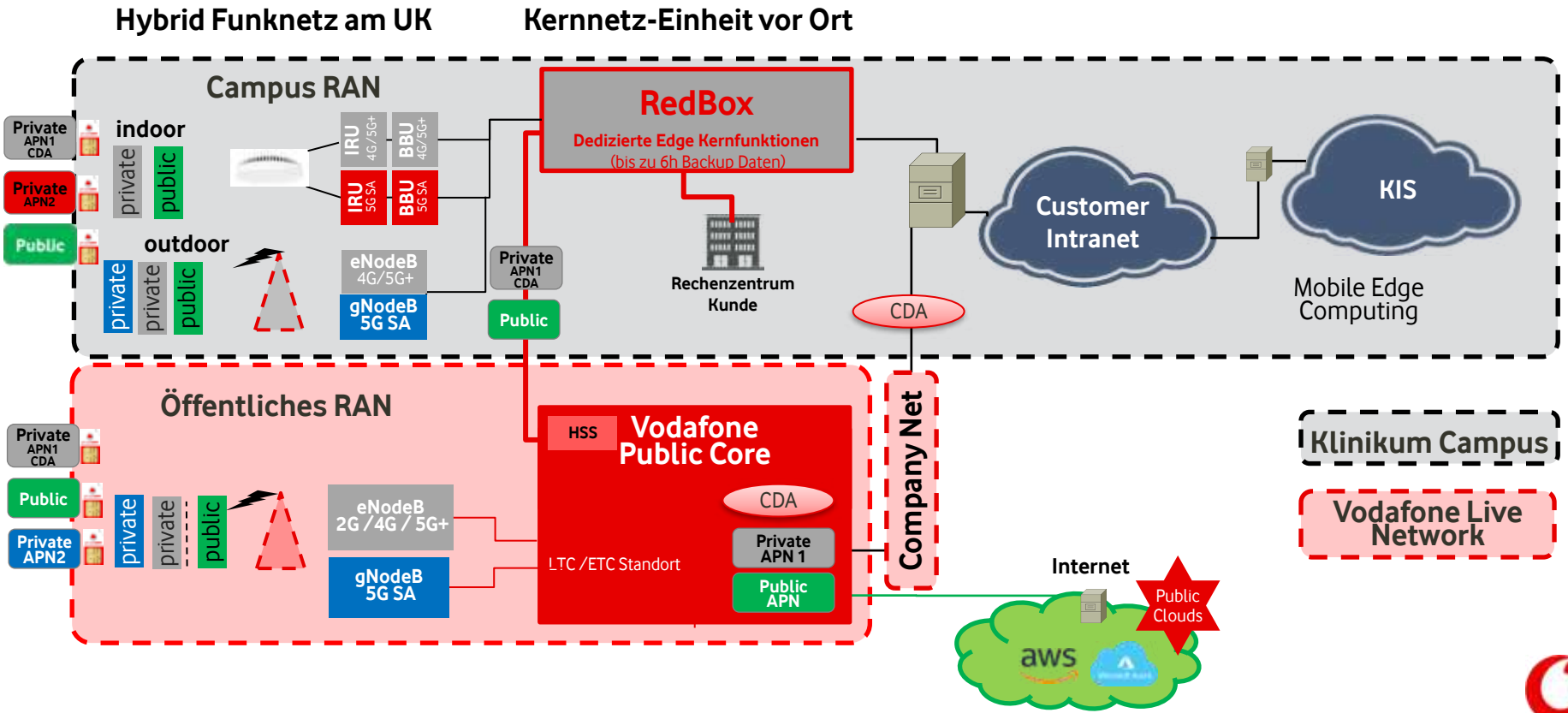
Industrie-Frequenzen

Security | 100% Sicherheit für eine E2E Verbindung gibt es nicht



Privates 5G Hybrid Netz I
Hybride Lösung mit dedizierten Kernnetzfunktionen im Makro-Netz

Redundantes Campus-Netz



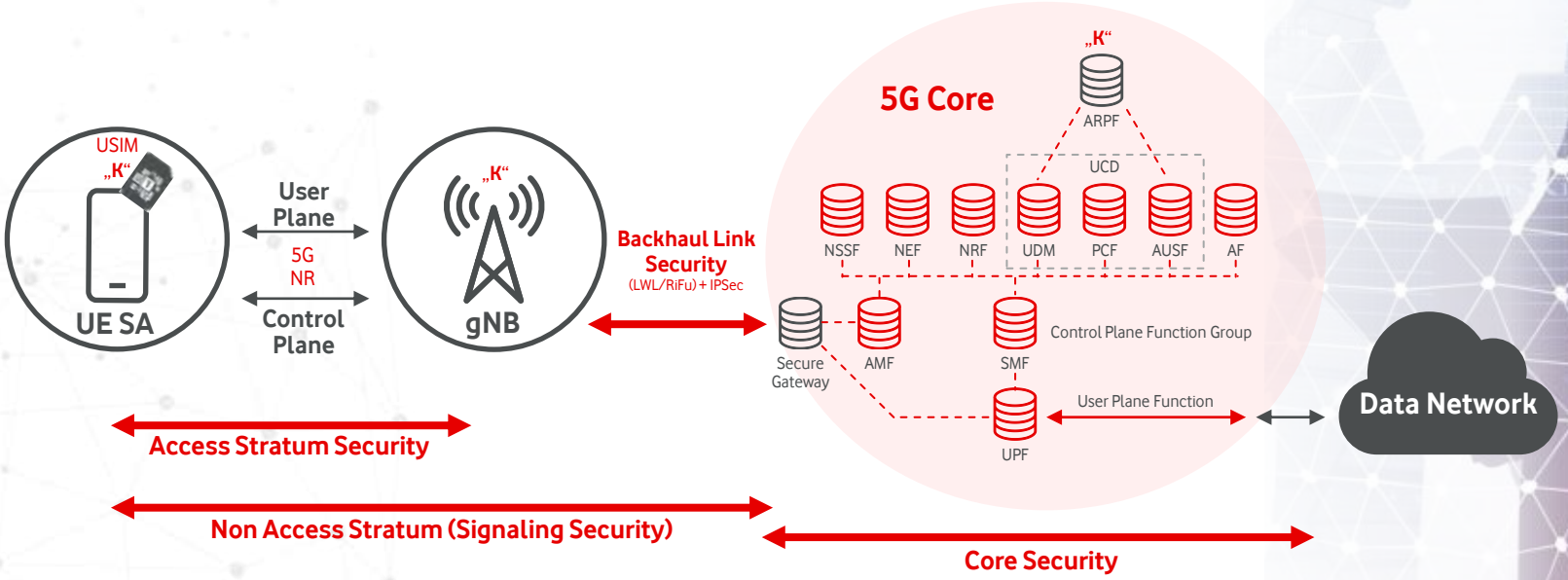
5G+
Eingebaute Sicherheit

02

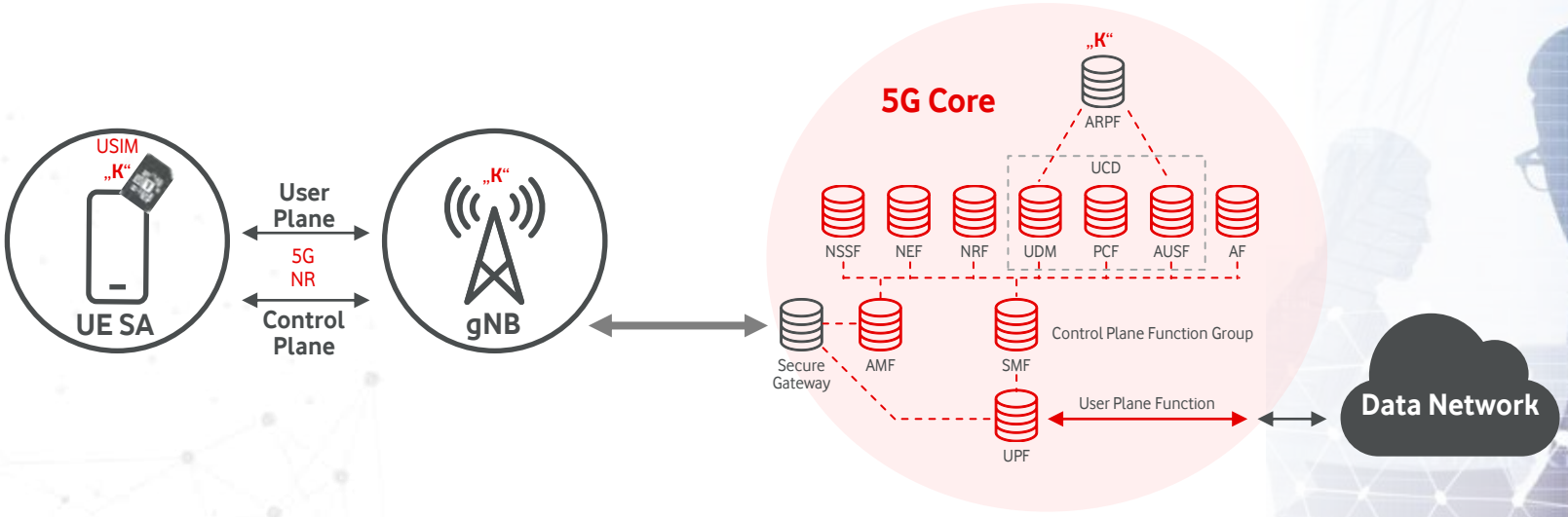
Eingebaute Sicherheit durch die Netzwerk-Architektur in 5G

5G SA baut auf bewährte 3GPP Sicherheitsmechanismen auf +

- Gegenseitige Authentisierung
- Verschlüsselung
- Integritätsprüfung
- Schutz der Teilnehmer-Identität



Eingebaute Sicherheit durch die Netzwerk-Architektur in 5G



Better radio interface security	**Enhanced** user privacy	**Stronger** cryptographic algorithms	**Flexible** security policy	**Improved** roaming security
User Plane Integrity Protection	Concealed identities	256 bit encryption	User-level security policy	Security Edge Protection Proxy

Together we can
vodafone
business

5G.NRW
Competence Center

UDE

Projektvorstellung: EURIALE

Workshop: Datenschutz & sichere Datenübertragung mit 5G

UNIVERSITÄT DUISBURG ESSEN
Offen im Denken

Gefördert durch:
Ministerium für Wirtschaft, Industrie, Klimaschutz und Energie des Landes Nordrhein-Westfalen

Projekt: euriale

5G.NRW
Competence Center

- Projektbeteiligte:

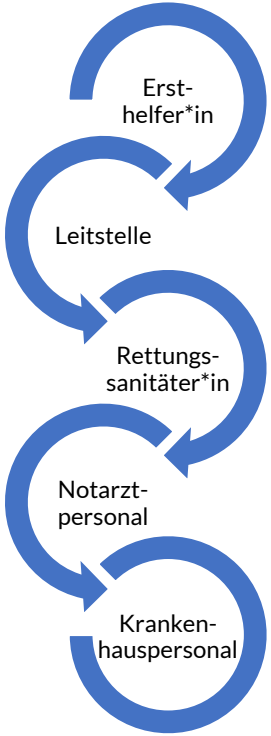
Fraunhofer IML
UKM Universitätsklinikum Münster
IFR Institut für Feuerwehr- und Rettungstechnologie der Feuerwehr Dortmund
Universität Duisburg Essen – Offen im Denken
adesso mobile solutions

- Ziel: Einsatz von 5G in Kombination mit Edge Computing zur störungsfreien und sicheren Übertragung von Daten in Notfallsituationen

Herausforderungen

5G.NRW
Competence Center

- Betrachtung der gesamten Rettungskette
- Erfassung vieler personenbezogener / medizinischer Daten:
  Name, Alter, Anschrift, …, Puls, Sauerstoffsättigung,
  Temperatur, …, aktueller Standort
- Beteiligte benötigen Zugriff auf Notfalldaten
- → Hohe Anforderung an Datensicherheit



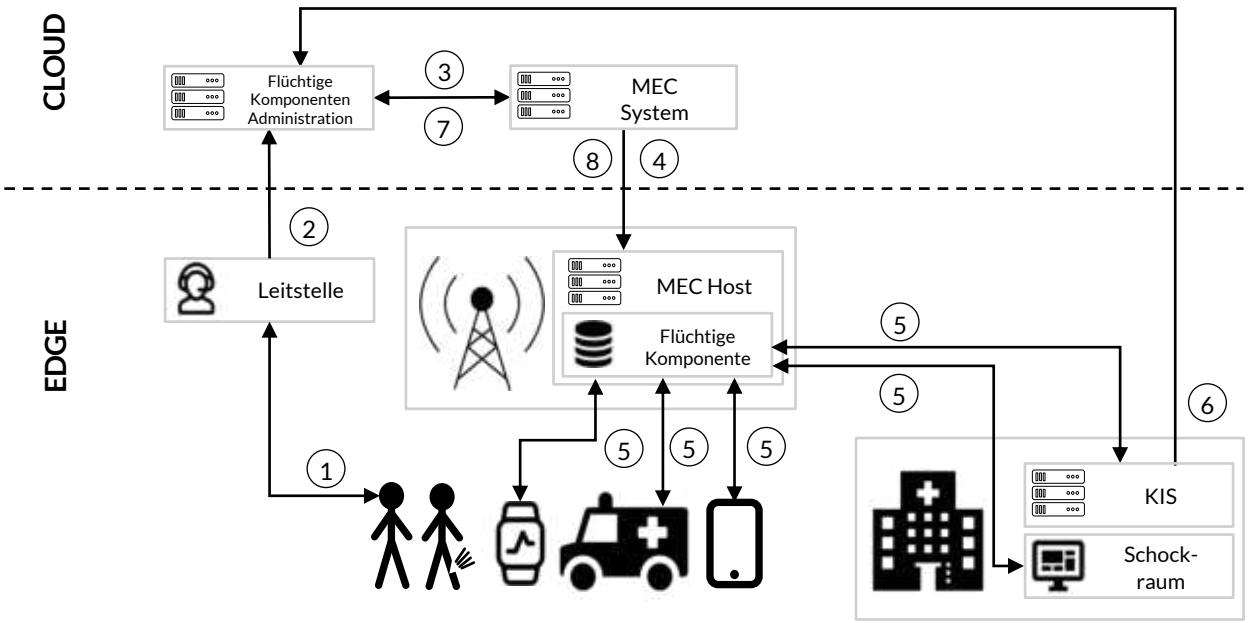
Technische Umsetzung

5G.NRW
Competence Center

- Konzept:
  - Hybride Edge-Cloud-Anwendung: Aufteilung der Software und Bereitstellung der Komponenten in der 5G-Edge und Cloud
  - Security by Design

- Umsetzung: Flüchtige Komponenten
  - Erfassung und Verarbeitung in der 5G-Edge
  - Speicherung der Daten während der Dauer des Notfalls
  - Nach Beendigung des Notfalls: Unwiederbringliche Löschung der Daten

Beispiel



Basierend auf: D. Schuster, C. Ehmke, M. Hesenius, C. Reichmann, J. Meis and V. Gruhn, "Towards an Architecture for Deploying Ephemeral Components on the Edge," *2022 IEEE 19th International Conference on Software Architecture Companion (ICSA-C)*, Honolulu, HI, USA, 2022, pp. 25-29, doi: 10.1109/ICSA-C54293.2022.00012.

5G.NRW
Competence Center

Vielen Dank für Ihr Interesse!

Kontakt:

David Schuster, M. Sc.
Universität Duisburg-Essen
Lehrstuhl für Software Engineering
david.schuster@uni-due.de
https://www.linkedin.com/in/david-schuster-de/

UNIVERSITÄT DUISBURG ESSEN
Offen im Denken

Lehrstuhl für Software Engineering

Gefördert durch:
Ministerium für Wirtschaft, Industrie, Klimaschutz und Energie des Landes Nordrhein-Westfalen

	Technik	Bereitstellung / Vertrieb	Forschung	Anwendung	Andere
In welchem Kontext stehen Sie zu 5G ?			Lehre und Forschung e-health / DIGA Forschung und Lehre Vernetzter Rettungswagen Forschung-Vernetzter Rettungswagen Forschung und Lehre (Szenarioplan) 5G Fördergelder	PDMS-Anwendungsbeispiel Anwender nutzt Informationsplattform und erhält Informationen	Kostenrechner
Wurde das Thema IT-Sicherheit im Zusammenhang mit 5G in einer frühen Phase des Projektes / der Anwendung betrachtet? Falls, "ja", aus welcher Perspektive bzw. aus welchem Kontext haben Sie die IT-Sicherheit bzgl. 5G betrachtet?	Zusammenführung von anonymisierten und personenbezogenen Daten im KH Projektpartner ERNW war bei der Ausschreibung und bei der Entwicklung der Systemarchitektur eingebunden. Inkl. Anschließendem Review. Weiterhin wurde ein Datenschutzkonzept gemeinsam mit Datenschutzbeauftragen und Klinikern erarbeitet				
Welche Schnittstellen / Synergien waren bei der Umsetzung der IT-Sicherheit (nicht) relevant?	Noch keine Schnittstellen verfügbar IEEE 11073-SDC, FHIR, HL7v2 Einbindung der relevanten Stakeholder aus Bereich Ärztliche Versorung, Rettungsdienst, IT-Verantwortliche, IT-Sicherheitsexperten, Experten für Nachrichtentechnik, Bundesnetzagentur	Noch keine technische Umsetzung			
Welche Herausforderungen haben Sie bei der Umsetzung Ihres IT-Sicherheitskonzeptes identifiziert?	Medizingeräte mit 5G Technologie sind kaum am Markt verfügbar. Es fehlt an Standards der Dokumentation und Technik Informationsverfügbarkeit vs. Informationsnutzung Komplexe Systemarchitektur notwendig, wenn eine herstellerunabhängige Lösung entwickelt werden soll. Regulatorische Lücken (Einsatz von 5G-Campus in mobilen Zellen o.ä.)	hohe Sicherheitsanforderungen im Umgang mit med. Daten			
Konnten Sie die Akzeptanz gegenüber Ihrem Sicherheitskonzept bei Ihren Nutzer*innen / Anwender*innen / Kund*innen wahrnehmen / steigern?	Noch keine Erfahrung noch kein Austausch mit Endnutzern vorhanden Akzeptanz auf Ebene eine Forschungsprojektes kein Problem. Erste Gespräche mit Anwendern erfolgversprechend (was auch immer das heißen mag) :)	Keine Erfahrung			

	Technik	Bereitstellung / Vertrieb	Forschung	Anwendung	Andere
In welchem Kontext stehen Sie zu 5G ?	Technik / Architektur		(Video-) Daten-Übertragung Optimierungsmöglichkeiten durch 5G Campusnetze in IT-Anwendungen	Anbindung der IKT-Prozessbeteiligungen	Kostenrechner Beratung Rechtliche Perspektive
Wurde das Thema IT-Sicherheit im Zusammenhang mit 5G in einer frühen Phase des Projektes / der Anwendung betrachtet? Falls, "ja", aus welcher Perspektive bzw. aus welchem Kontext haben Sie die IT-Sicherheit bzgl. 5G betrachtet?	Von Tag 1 an, für Architektur und System	Ja, Sicherheit med. Daten / Austausch Cloud und 5G		Die nur ein isoliertes Campusnetz betrachtet wird, wie der Datenmaschinenaustausch von verschiedenen gegeben	
Welche Schnittstellen / Synergien waren bei der Umsetzung der IT-Sicherheit (nicht) relevant?	BSI, Ausrüster, interne Security, externe Prüfung	Noch nicht umgesetzt / evaluiert			
Welche Herausforderungen haben Sie bei der Umsetzung Ihres IT-Sicherheitskonzeptes identifiziert?	Betreibbarkeit	Sicherheit und Verarbeitung in der Cloud		Der Wunsch von Industriepartnern nach Hybridlösungen anstatt isolierten Campusnetzen	Wartung/Administration des Netzes
Konnten Sie die Akzeptanz gegenüber Ihrem Sicherheitskonzept bei Ihren Nutzer*innen / Anwender*innen / Kund*innen wahrnehmen / steigern?	Ja, :)				