Data Centric Security Architecture

Bonn, 17. November 2016

Oberstleutnant i.G.
Stefan Eisinger
BMVg CIT II 1

Gliederung

- **Problemstellung**
- Data Centric Security (DCS) – DEU Ansatz
- Weiteres Vorgehen

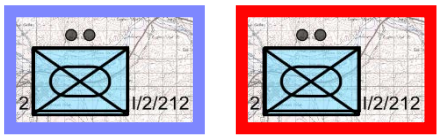
Klassifizierung von Informationen

Klassifizierung von Informationen

Nicht-technische Anwendung von Einstufungskriterien

Klassifizierung von Daten

Definition der Schutzbedürftigkeit gespeicherter Daten



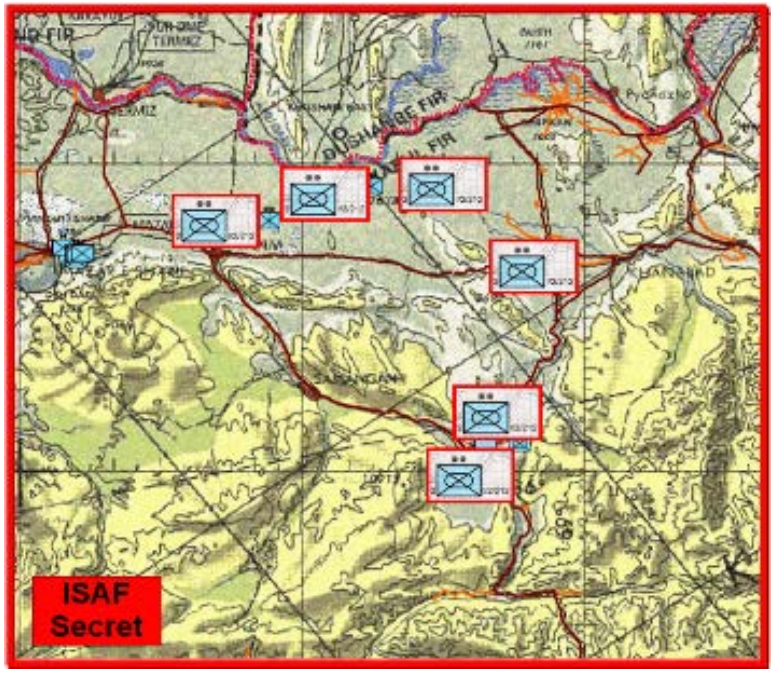
Klassifizierung von Systemen

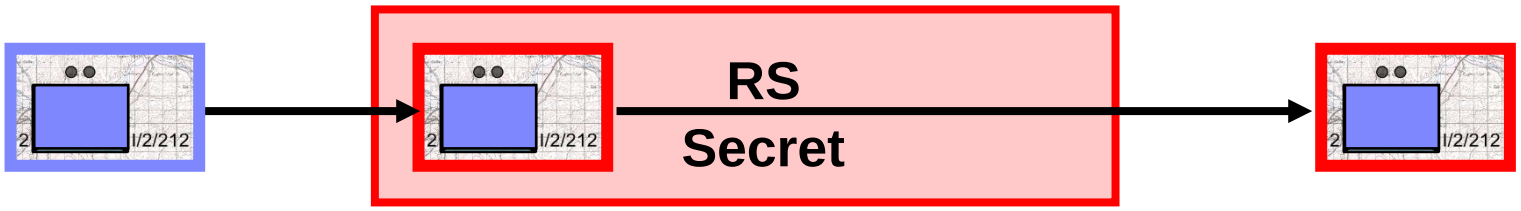
IT-basierter Schutz von Daten bis zu einer bestimmten Sicherheitseinstufung

- **Schutz von Gesamtsystemen** wird realem Schutzbedarf der Datenobjekte nicht gerecht.

Grundsatz „Need-To-Know“

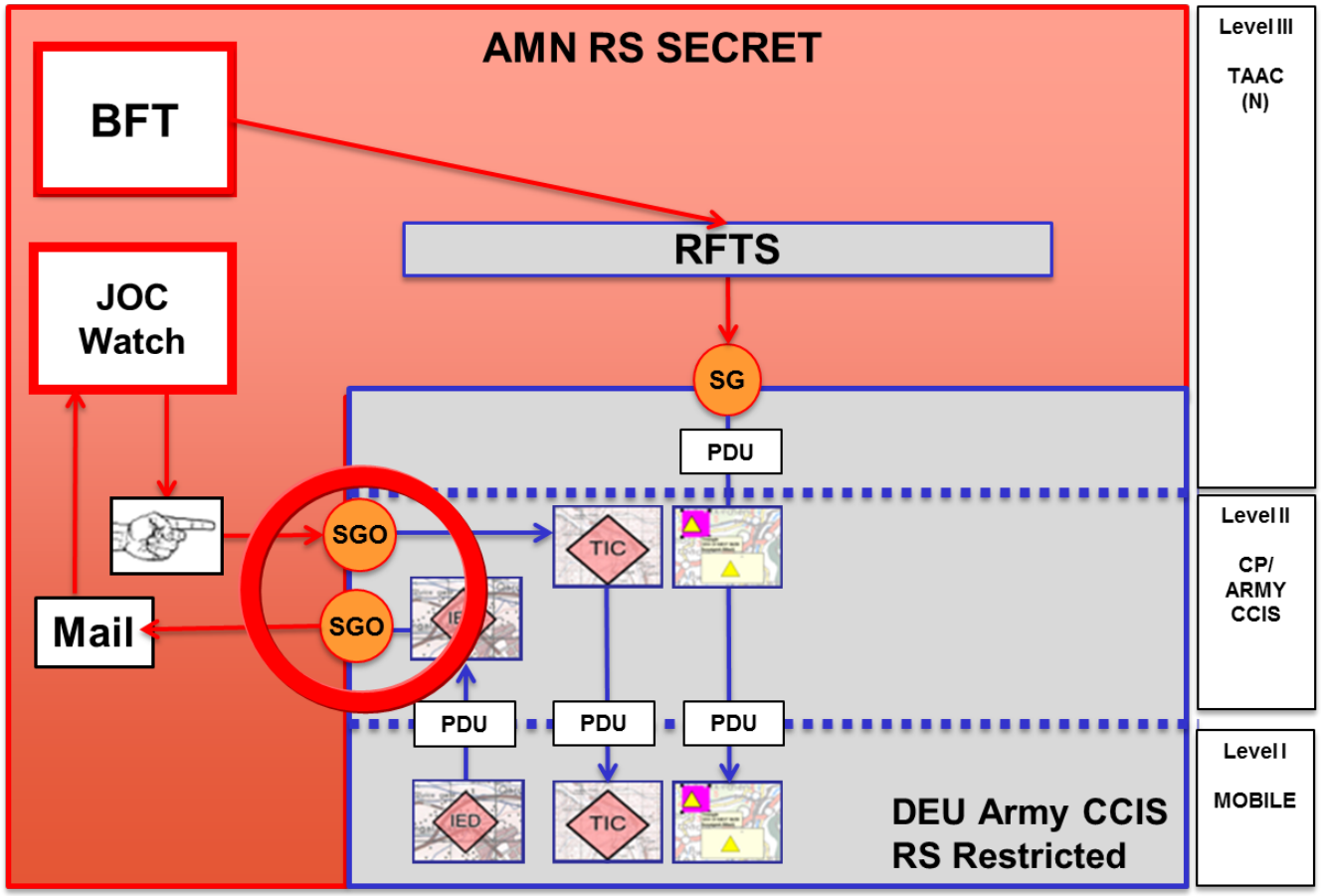
- Maximaler Schutzbedarf für alle Daten wird unterstellt.
- Labelling in Systemen nicht umgesetzt.





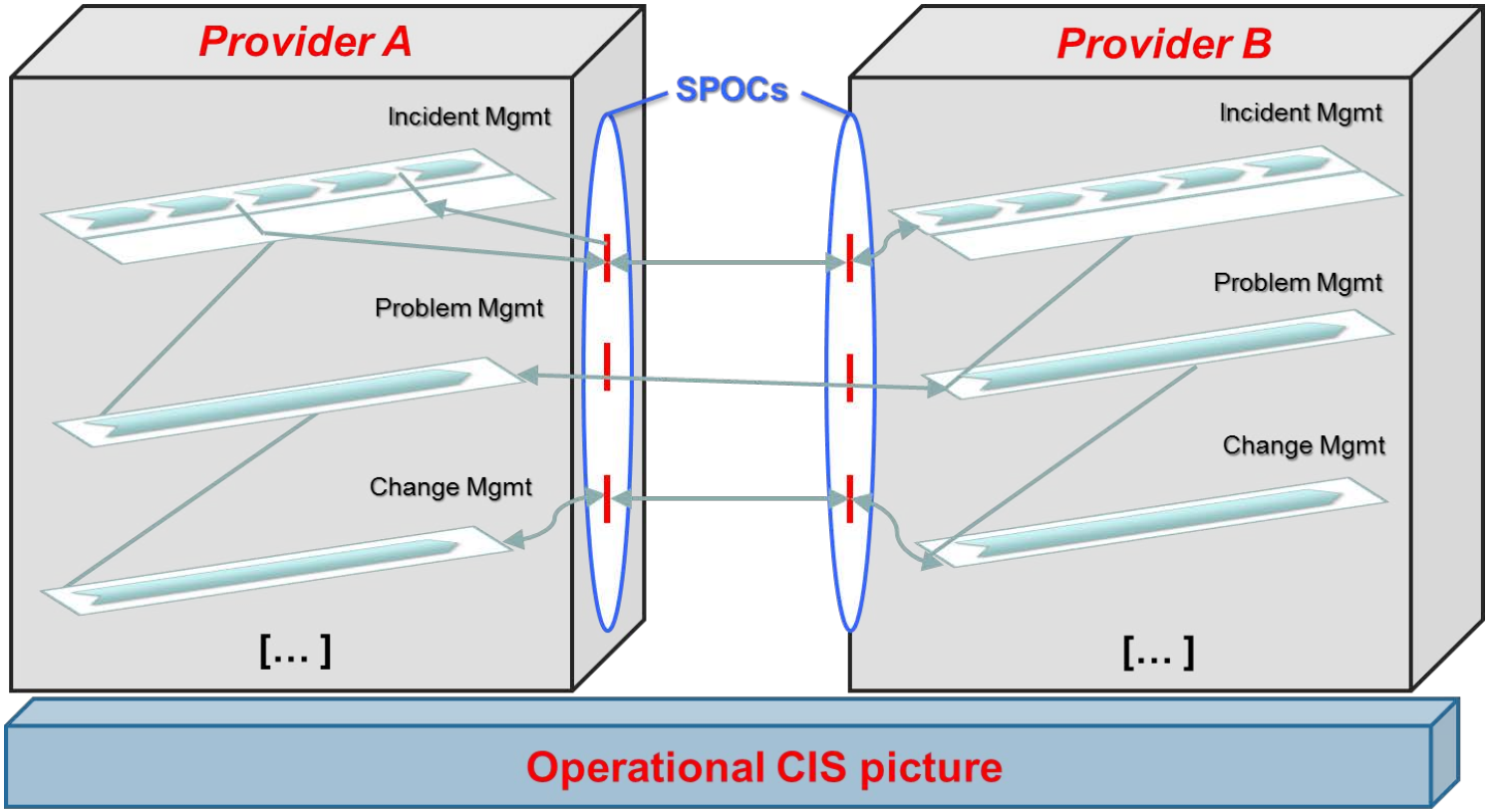
- **Realer Schutzbedarf** der Daten wird **ignoriert**.
- **Herausforderung:** Operative Nutzbarkeit;

Incident Management Prozess in Resolute Support (RS)



- **Weitergabe wichtiger Lageinformation** an mobile taktische Ebene derzeit technisch **nur eingeschränkt möglich**.

IT-Service Management (ITSM) im multinationalen Umfeld



- **Austausch von ITSM-Informationen** zwischen IT-Service Providern über unterschiedlich klassifizierte Netzwerke derzeit **nicht möglich**.

Federated Mission Networking (FMN)- Operative Forderungen

1. Permit **sharing of commander's intent** and communication of mission orders.
2. Provide mission participants with **situational awareness** and a **planning environment**.
3. Provide an environment in which mission participants use their **own tools** linked to authoritative data sources.
4. Rapidly create a **single** information sharing environment.
5. Exchange information between the mission environment and **other information domains**.

Gliederung

- Problemstellung
- **Data Centric Security (DCS) – DEU Ansatz**
- Weiteres Vorgehen

DEU Ansatz - Zieldefinition

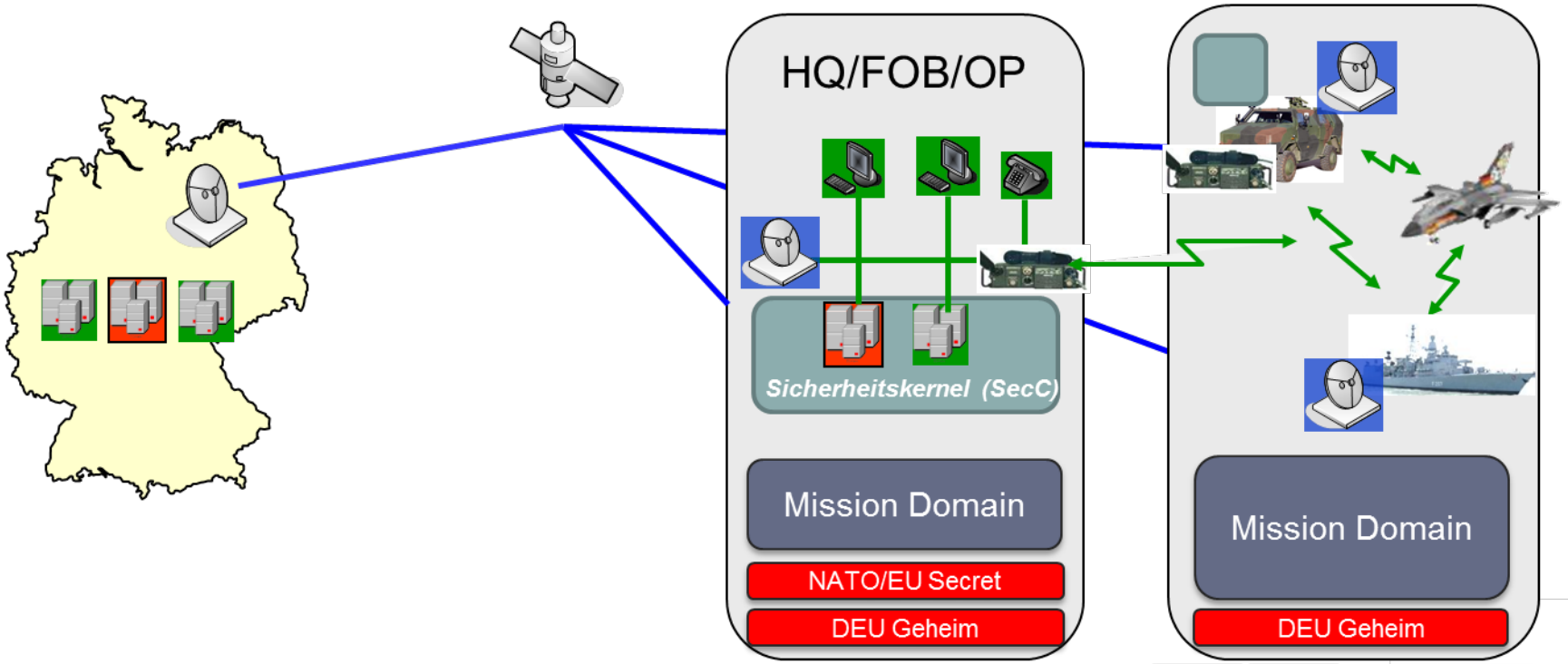
FüUstg für Dienststellen im In- und Ausland

Weitreichende Anbindung und Vernetzung

FüUstg für stationäre u. verlegefähige Einrichtungen

FüUstg für mobile Elemente

Bereitstellen von IT-Services

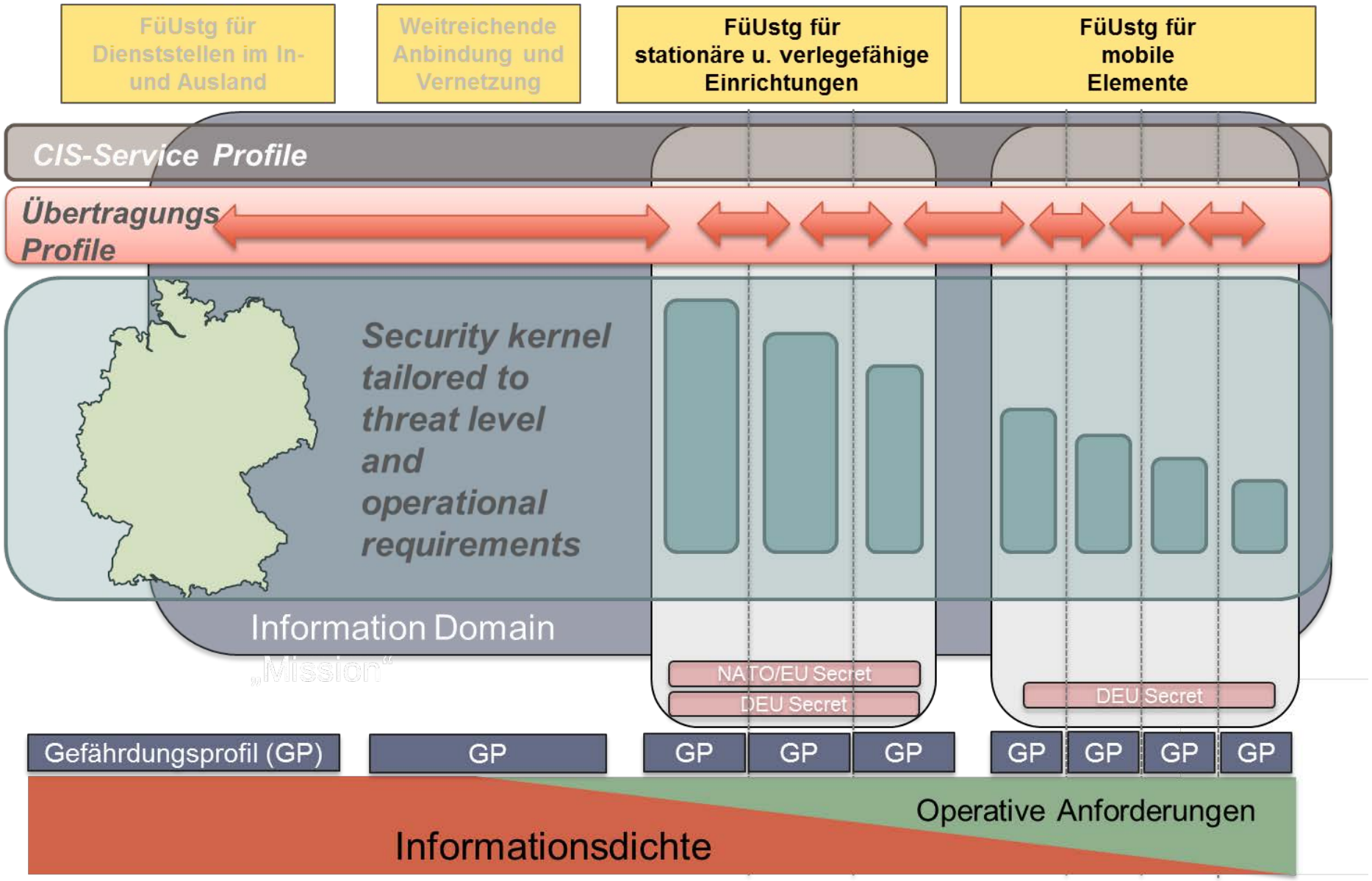


Gefährdungsprofil (GP) | GP | GP | GP | GP | GP | GP | GP

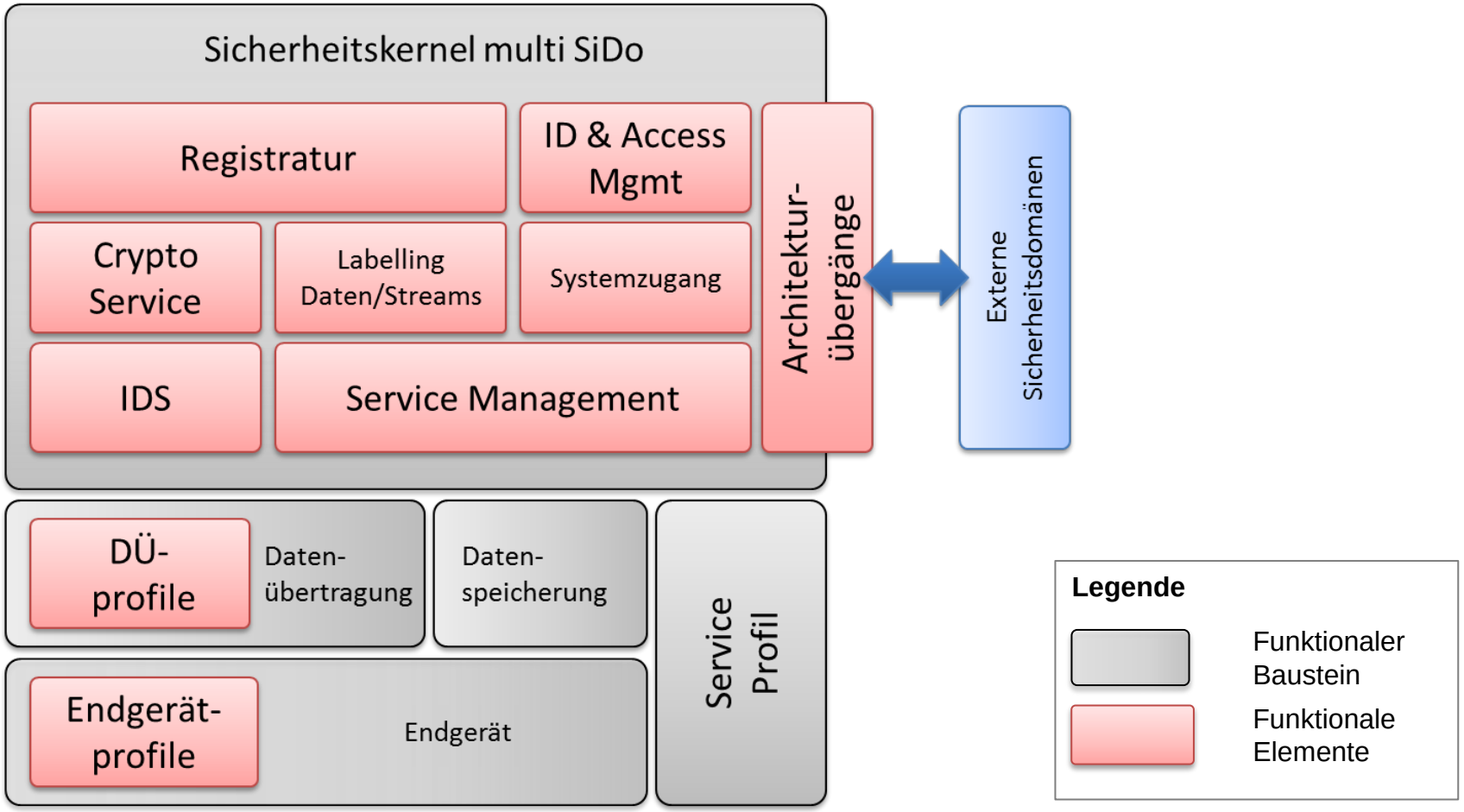
Informationsdichte

Operative Anforderungen

Gefährdungsprofile



Funktionale IT-Sicherheitsarchitektur (FITSA)



- **Konzept FITSA** beschreibt notwendige **funktionale Bausteine** zur Realisierung einer DCS.

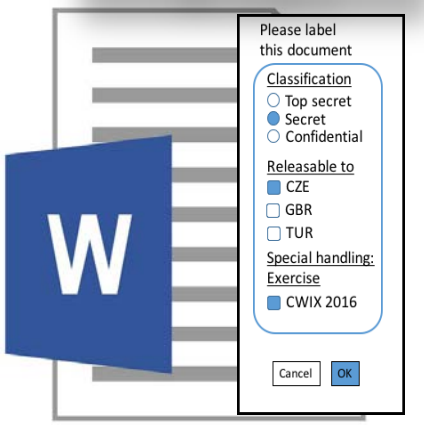
Gliederung

- Problemstellung
- Data Centric Security (DCS) – DEU Ansatz
- **Weiteres Vorgehen**

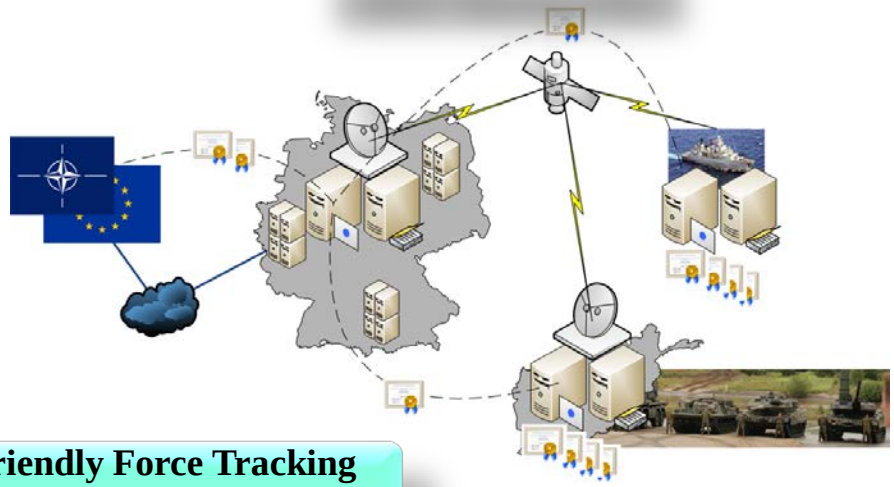
Ergebnisse in 2016

Coalition Warrior **I**nteroperability e**X**ploration, e**X**perimentation, e**X**amination, e**X**ercise (**CWIX**)

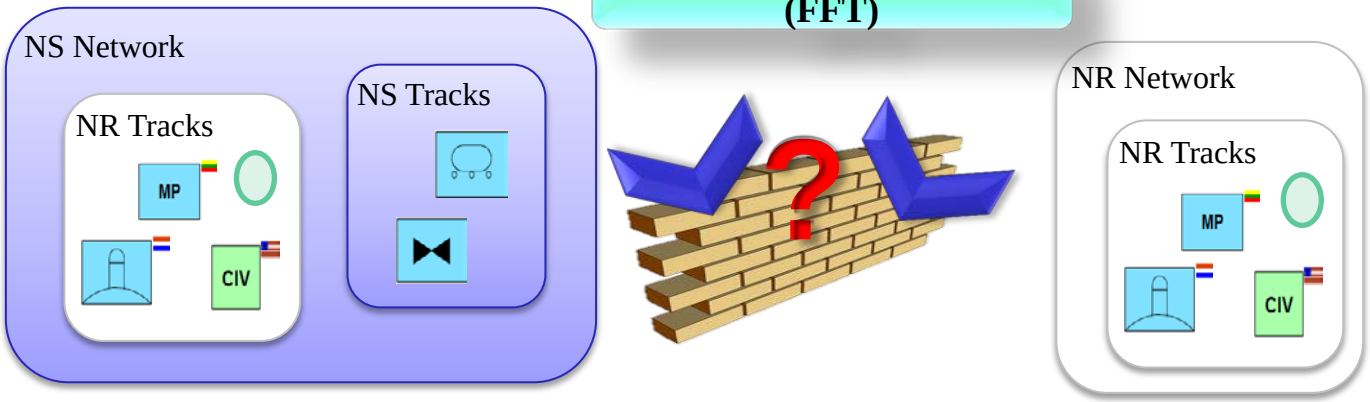
DCA/DCI



DEU Mission PKI



Friendly Force Tracking (FFT)



Fazit CWIX 2016

1. Permit sharing of commander's intent and communication of mission orders
2. Provide mission participants with situational awareness and a planning environment

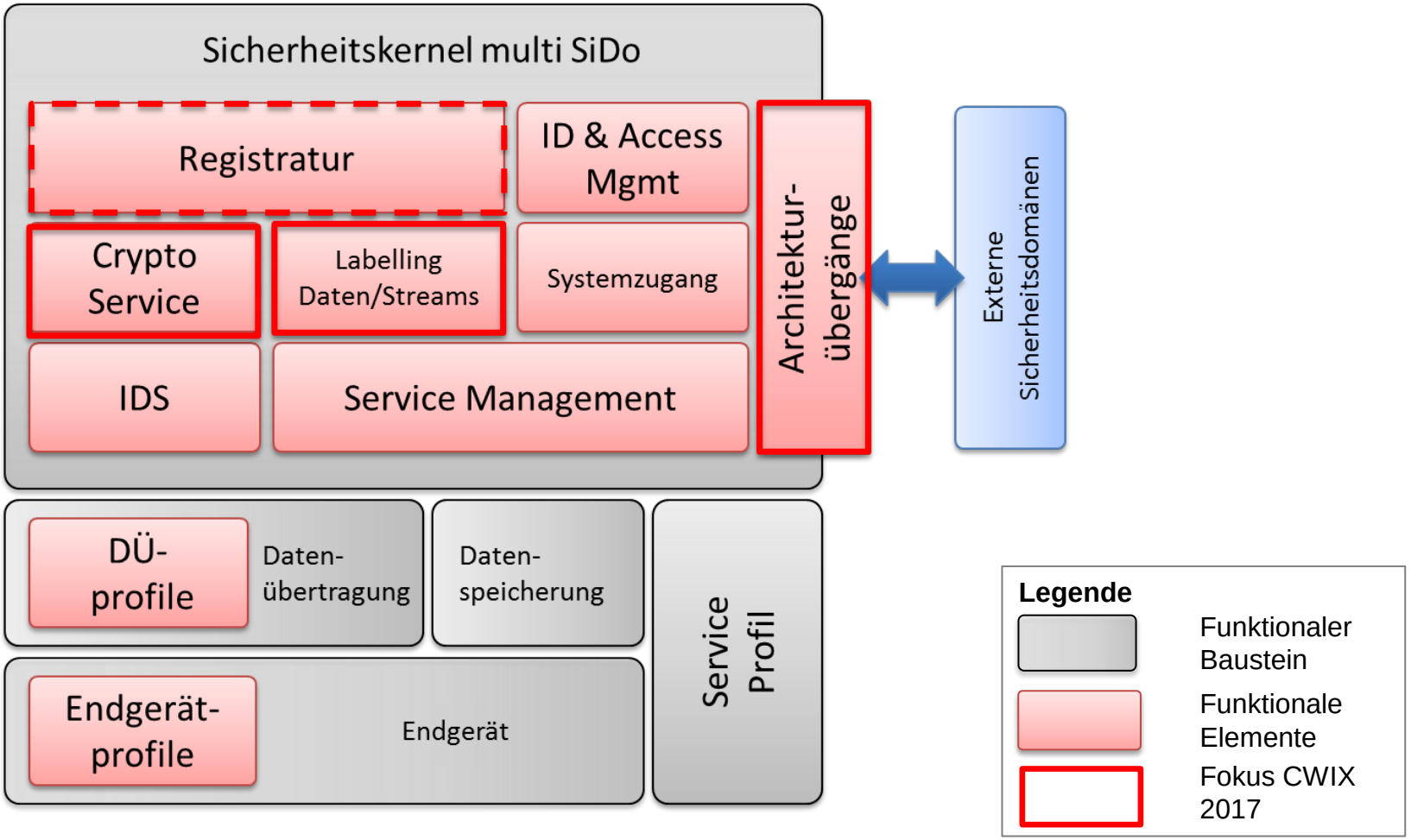
Traditioneller Ansatz

3. Provide an environment in which mission participants use their own tools linked to authoritative data sources
4. Rapidly create a single information sharing environment
5. Exchange information between the mission environment and other information domains

DCS Ansatz

- Wesentliche Funktionalitäten **in Einzelsystemen** getestet.
- Integration in **einen** Demonstrator für CWIX 2017 ist anzustreben.

CWIX 2017 – Fokus

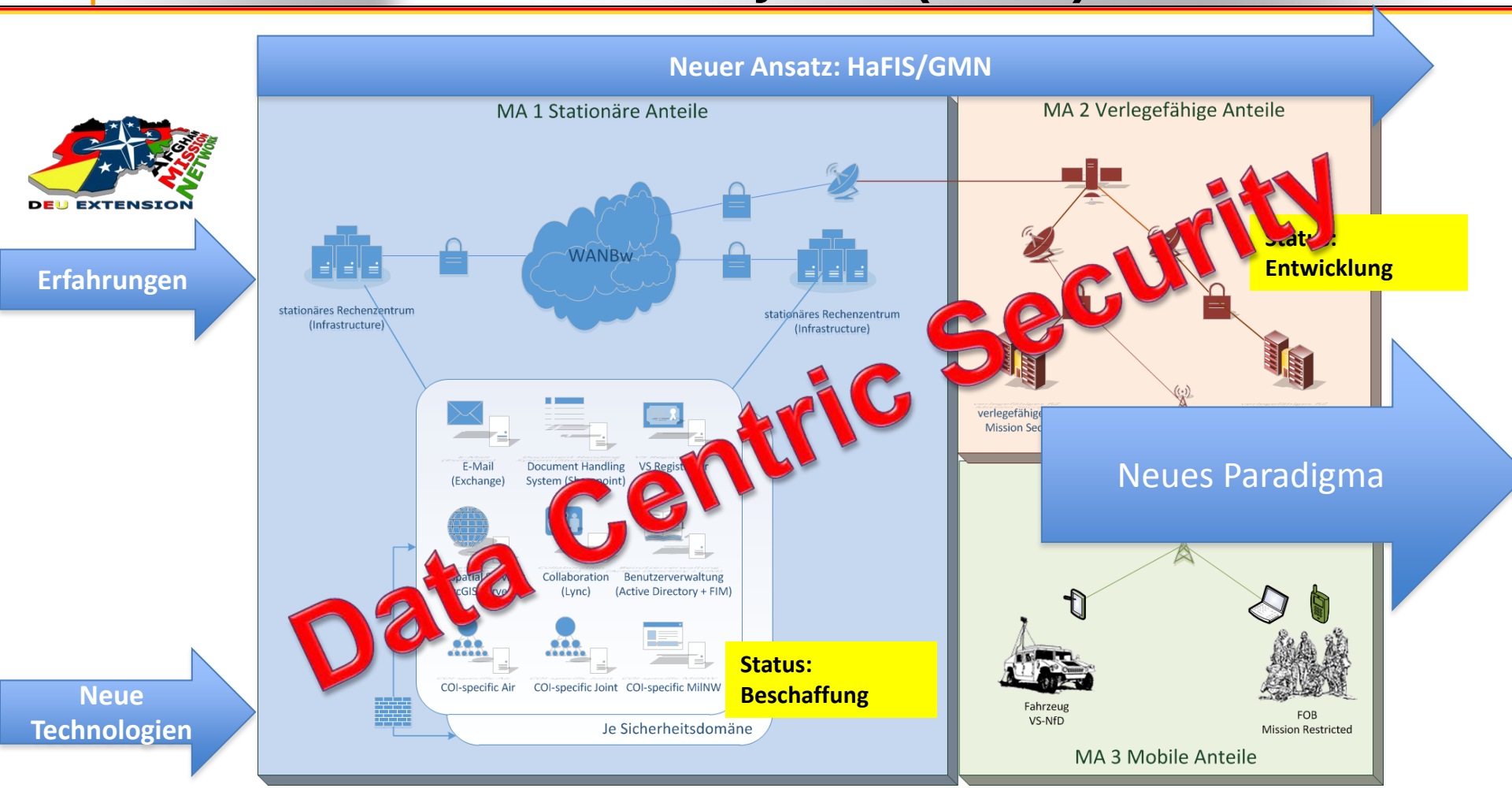


- **Wesentliche funktionale Bausteine** einer DCS stehen im Fokus der CWIX 2017.

CWIX 2017 -Fokus

- Funktionale Forderungslage (FüUstgKdoBw)
  - „Labelling“ und „Binding“
  - Trust Models
  - National Mission Public Key Infrastructure
  - Border Policy Enforcement Point
  - Datenobjekte:
    - SMC Data (ITSM-records in XML-Format)
    - File Service (xls, doc, ppt)
    - Tactical Data (FFT)
  - HAFIS-konforme Architektur

Harmonisiertes Führungs- und Informationssystem (HaFIS)



- **Integration in HaFIS** als wesentliche Herausforderung.

Die nächsten Schritte…

- Sachstand durch **FüUstgKdoBw** erarbeitet sowie multinational in Teilen abgestimmt.
- Ziel: Ministeriell Abstimmen und Festlegen der **Federführung** noch in **2016**!

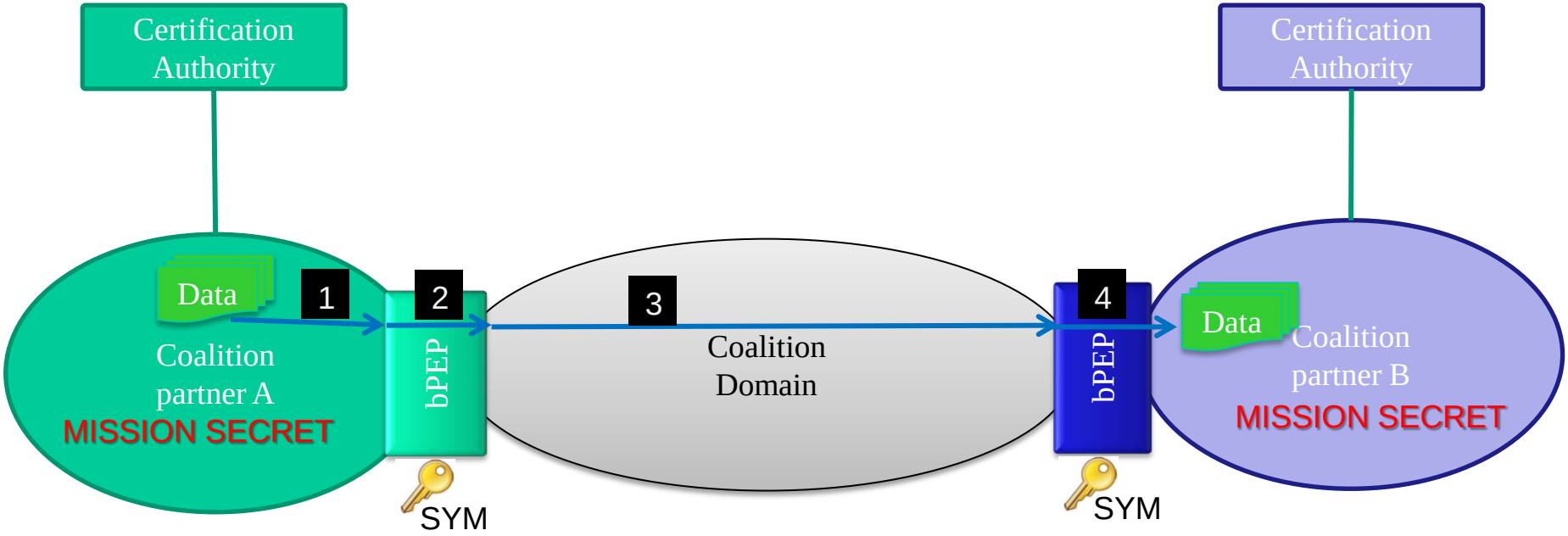
Data Centric Security Architecture

Bonn, 17. November 2016

Oberstleutnant i.G.
Stefan Eisinger
BMVg CIT II 1

Backup Folien

Szenario 1: Coalition Partner w/o Trust

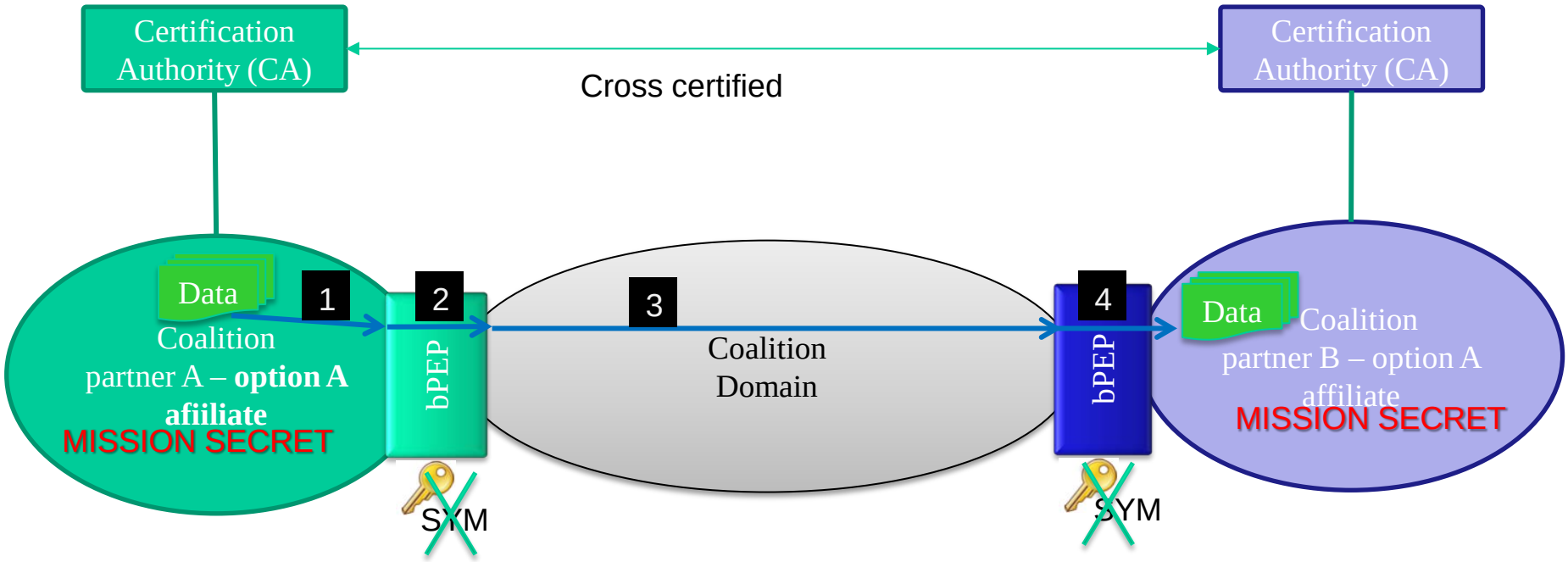


Scenario 1: No trust between coalition partner A + B
➔ Mission PKI @partner A does not reach out to partner B

1. bPEP @ partner A checks for releasability/security label
2. bPEP breaks label, decrypts data object, encrypts with coalition domain distributed symmetric key (SYM KEY)
3. bPEP sends data object to partner B
4. bPEP @ partner B decrypts data object and label is bound to data object @ partner B via national cryptographic means

bPEP: Border policy enforcement point

Scenario 2: Coalition Partner w/ full Trust



Scenario 2: Full trust between coalition partner A + B, coalition domain is secure

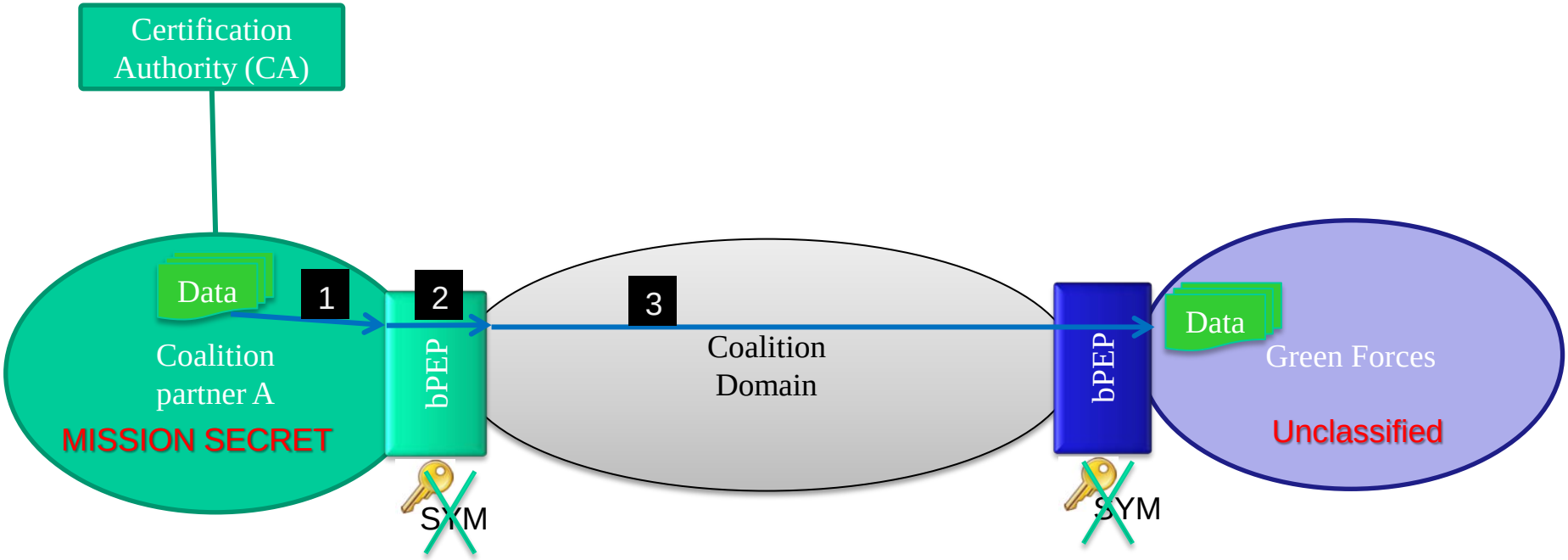
➔ **no SYM Key necessary**

➔ **Mission PKI @partner A reaches out to partner B**

1. bPEP @ partner A checks for releasability/security label
2. data releasable to bPEP @ partner B
3. bPEP @ partner B can check labeling due to CA-trust
4. Partner B can utilize data

bPEP: Border policy enforcement point

Scenario 3: Blue to Green Forces

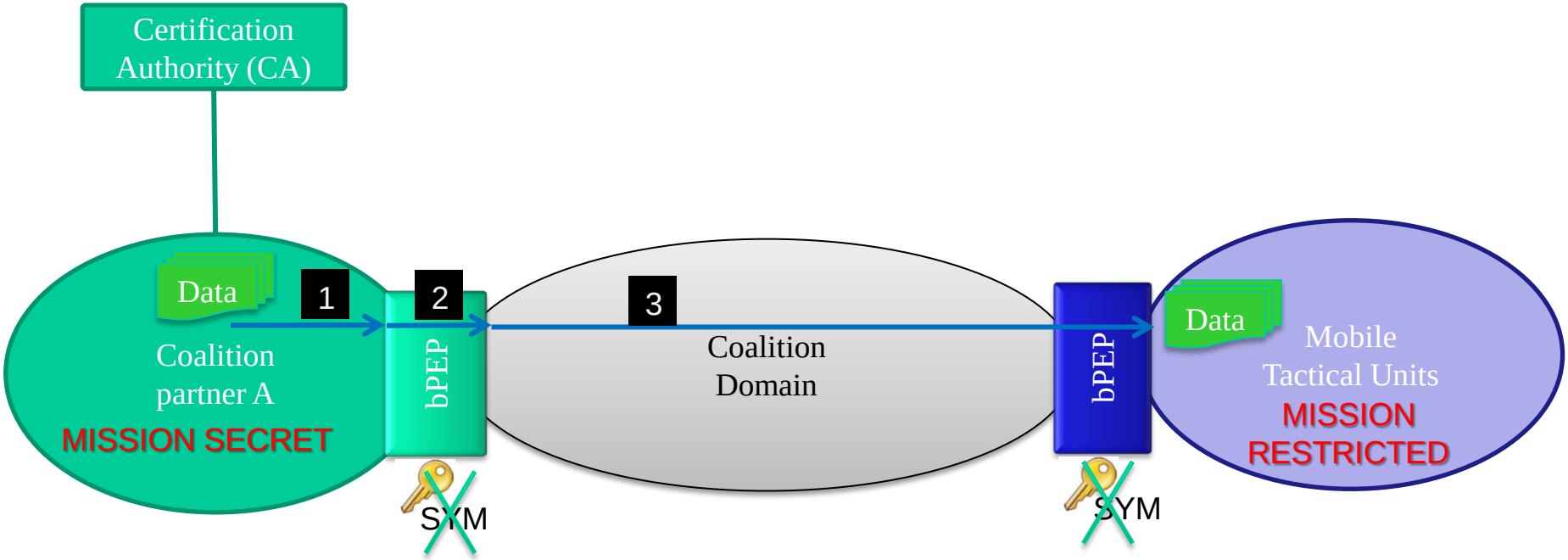


Scenario 4: Coalition partner A+B perform Blue-to-Green communication

1. bPEP @ partner A checks releasability (unclassified) and breaks binding
2. Strip label from data object
3. Send “clear text” data object to partner B

bPEP: Border policy enforcement point

Szenario 4: Friendly-Force-Tracking



Scenario 5: Coalition partner A+B perform Friendly-Force-Tracking

1. bPEP @ partner A checks releasability (RESTRICTED, rel. to mobile/tactical element) and breaks binding
2. Strip label from data object
3. Send “clear text” data object to mobile tactical units

bPEP: Border policy enforcement point