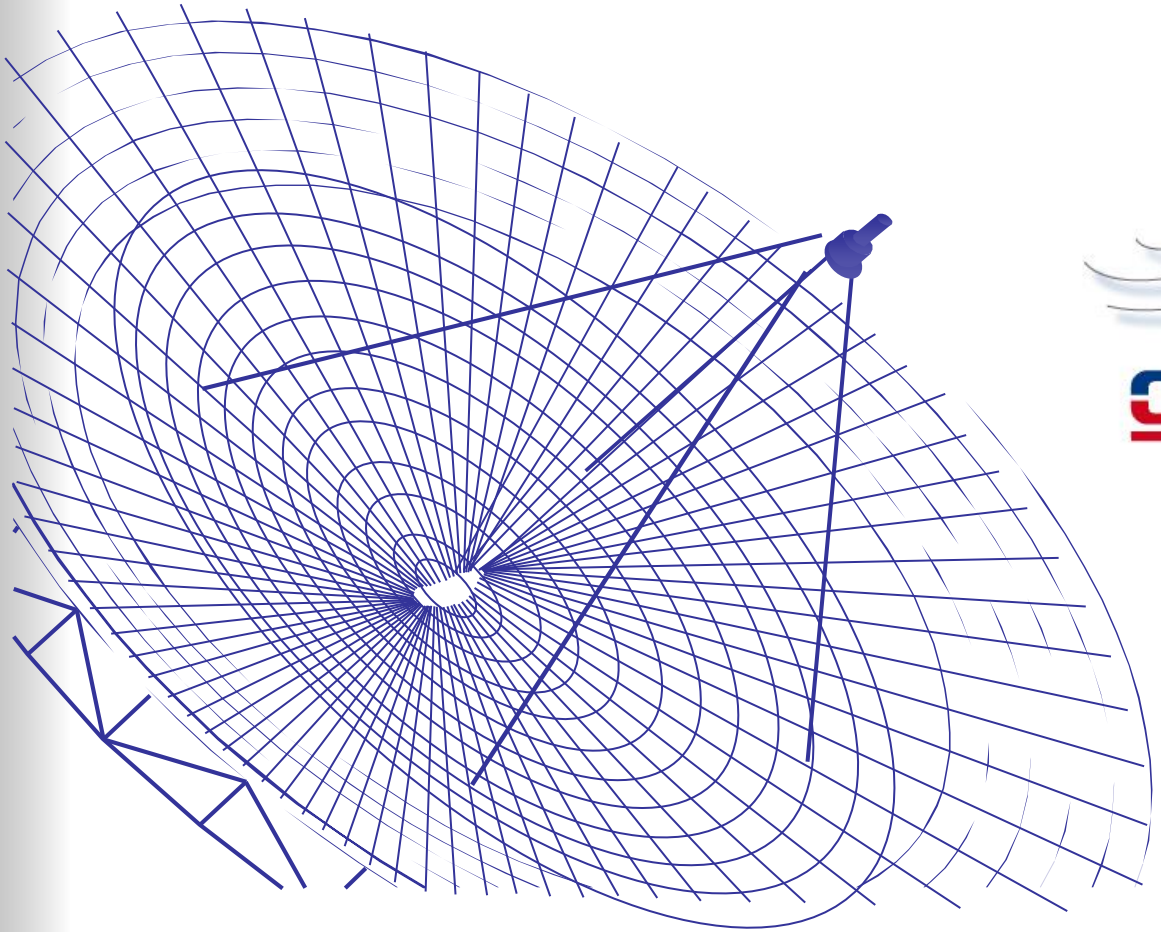
Verschlüsselungs-/Sicherheitskonzept



AUSBILDUNG
BOS-Bayern
digitalFunk

Lerninhalte

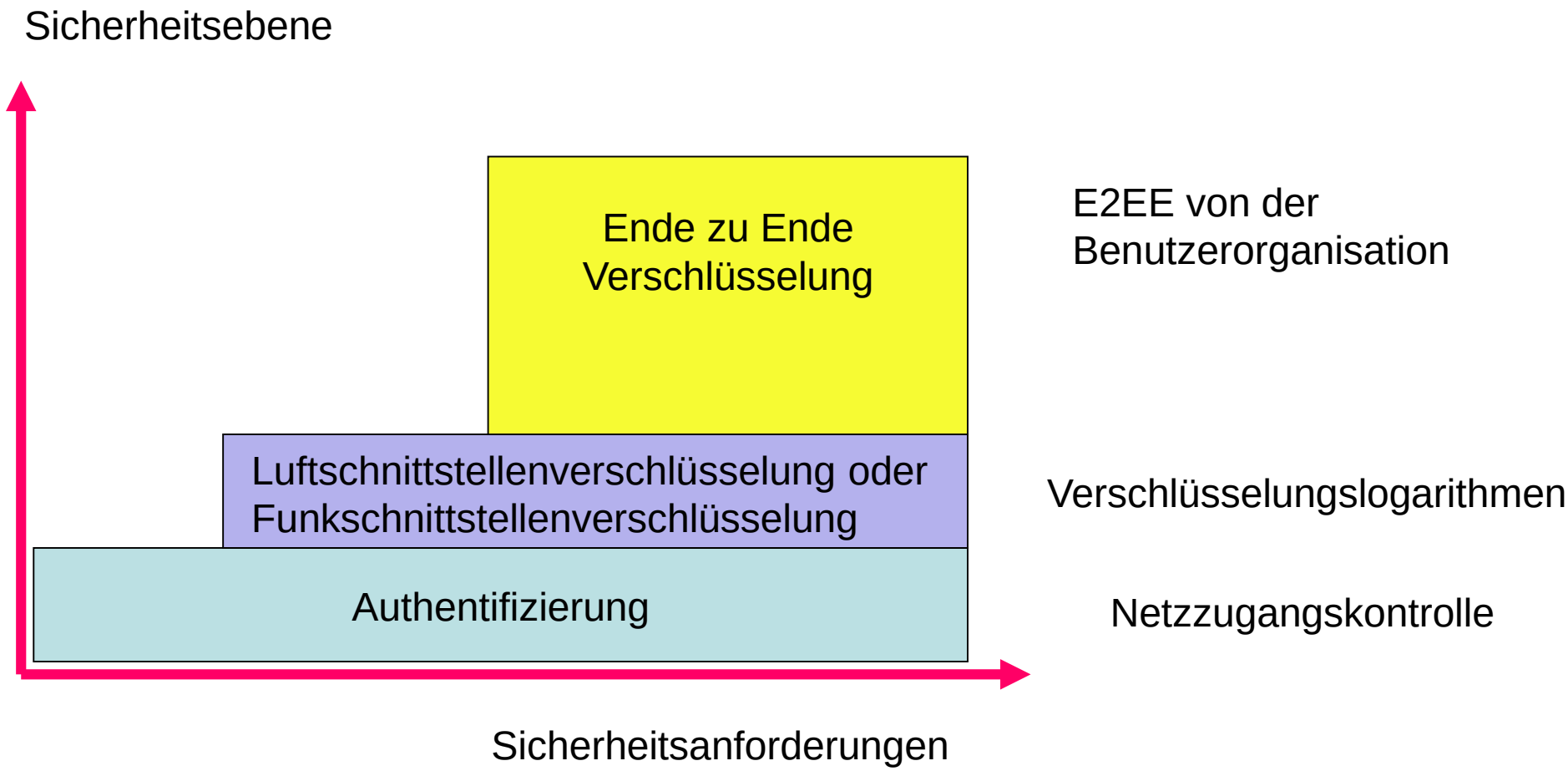
- Sicherheitsvorkehrungen
- Sicherheitsanforderungen
- Authentifizierung
- Verschlüsselungen
- Aktivierung/Deaktivierung
  - ITSI basiert
  - OPTA basiert
  - Gerätenummer basiert
- Sicherheitskarte

Verschlüsselungs- u.Sicherheitskonzept

Trifft Sicherheitsvorkehrungen vor:

- Abhören
- Diebstahlsicherung
- Vandalismus
- Sabotage
- Maskierung als berechtigter Benutzer (Masquerading)
- Nachrichtenverfälschung (Tampering)
- Wiedergabe (Replaying)
- Störsignalerkennung (Jamming)

Tetra - Sicherheitsfunktionen



Struktur der TETRA-Teilnehmer-Identität

ITSI oder GTSI		
		ISSI oder GSSI
MCC (Mobile Country Code)	**MNC** (Mobile Network Code)	**SSI** (Short Subscriber Identity)
0262	**1001**	**03051067**
ITU-T X.121	Vergabe durch die Bundesnetzagentur	Koordination durch die BDBOS
max. 4 Dezimalstellen	max. 5 Dezimalstellen	max. 8 Dezimalstellen

- **ITSI** = **I**ndividual **T**ETRA **S**ubscriber **I**dentity
- **GTSI** = **G**roup **T**ETRA **S**ubscriber **I**dentity
- **ISSI** = **I**ndividual **S**hort **S**ubscriber **I**dentity
- **GSSI** = **G**roup **S**hort **S**ubscriber **I**dentity
- Subscriber = Teilnehmer

Struktur der TETRA-Teilnehmer-Identität

Geburts- OPTA

Zeichen																					
01	02	03	04	05	06	07	08	09	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24
Blöcke																							
1		2			3			0															
Bun-des-land		Behörden-Und Organisa-tionskenn-zeichnung			Regionale Zuordnung			Teilnehmernummer Individual Tetra Subscriber Identifikation (ITSI) Oder - Sofern eineindeutig – die Blöcke 4 und 5 gem Ziff. 2.2/2.3															
								MCC				MNC				ISSI							
B	Y	F	W		R	#		0	2	6	2	1	0	0	1	0	3	0	5	1	0	6	7

Alias-OPTA

Zeichen																						
01	02	03	04	05	06	07	08	09	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24
Blöcke																							
1		2			3			4.1					4.2								4.3		5
Bundesland		Behörden- Und Organisationskennzeichnung			Regionale Zuordnung			Örtliche Zuordnung					Funktionszuordnung								Ordnungskennung		Ergänzung
B	Y	F	W		A			1					K	D	O	W			1	0		2	1

Operative Taktische Adresse (Alias-OPTA)

Senden der OPTA bei Drücken der Sprechtaste

BY/FW/A/1/KDOW

Beispiel:

Bundesland Baye	BY
Organisation F	FW
Kreis	A
Stand	1
F ...andowagen	KDOW
...:	2
1. HRT im KDOW	1

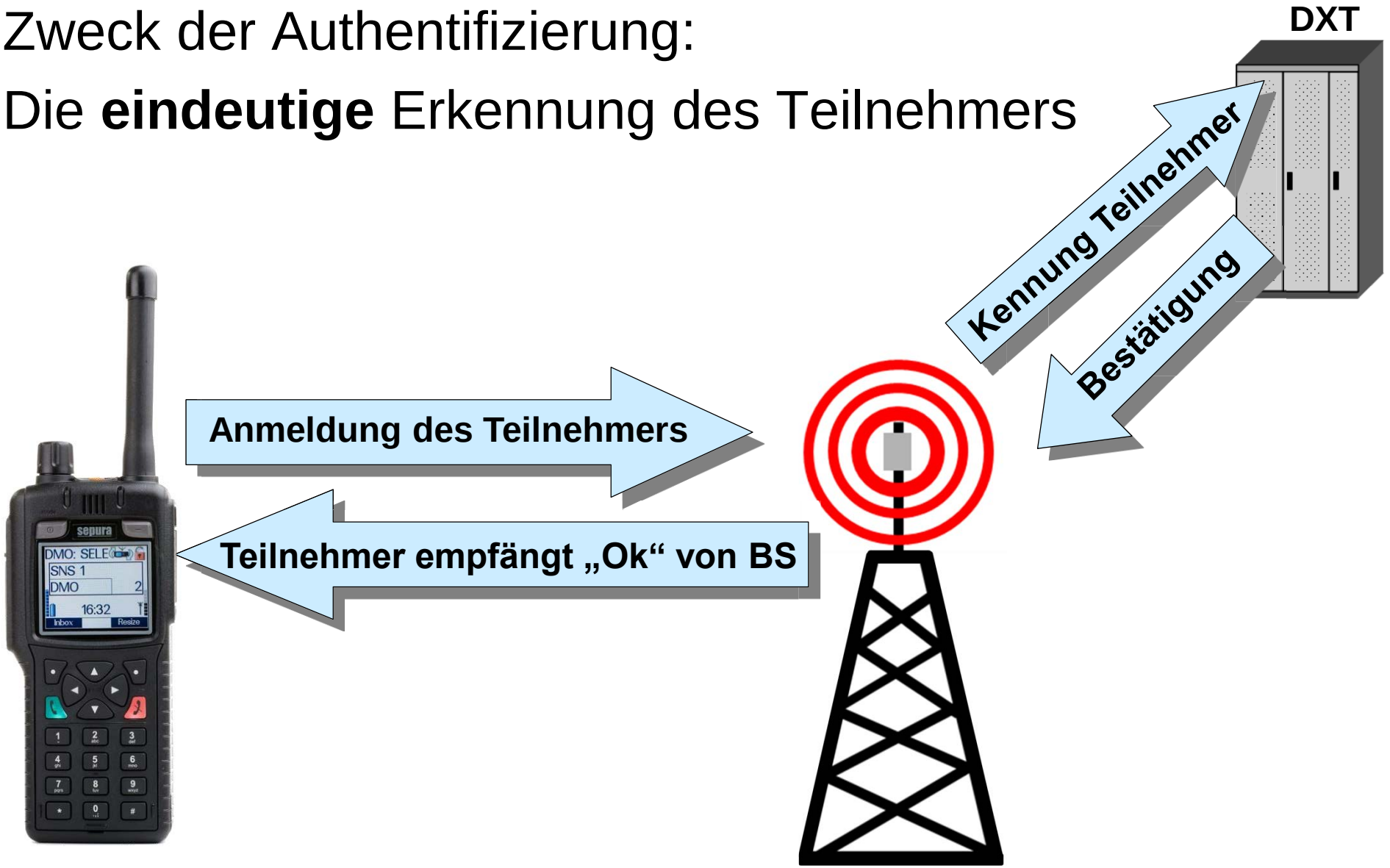
Anzeige im Display:
BYFW A 1 KDOW 10 21

Folie soll entfallen

- Die Alias-OPTA kann z.B. von der Leitstelle geändert werden
- Je nach Standort ist eine verkürzte Anzeige der OPTA möglich

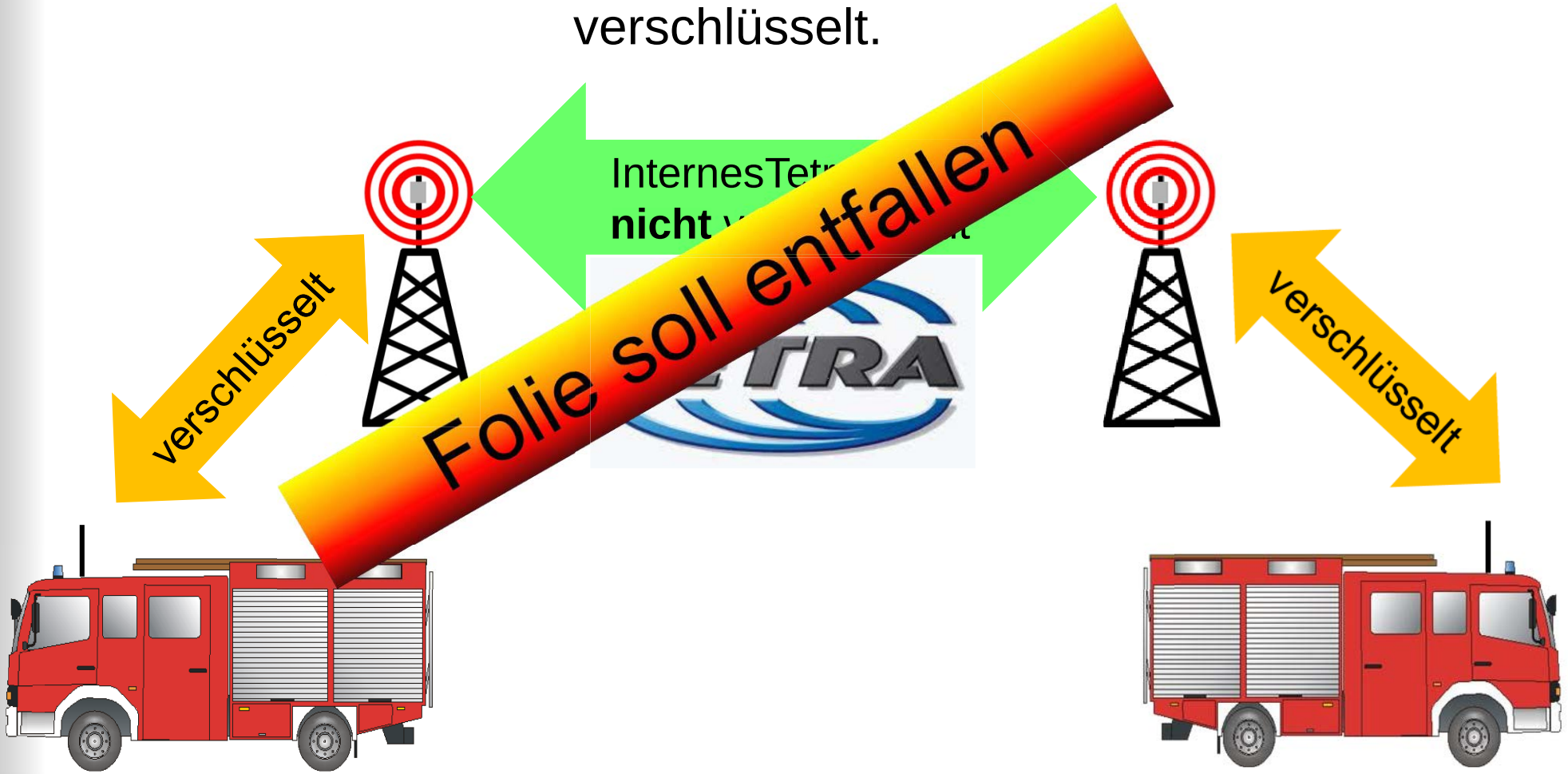
Zweck der Authentifizierung:

Die **eindeutige** Erkennung des Teilnehmers



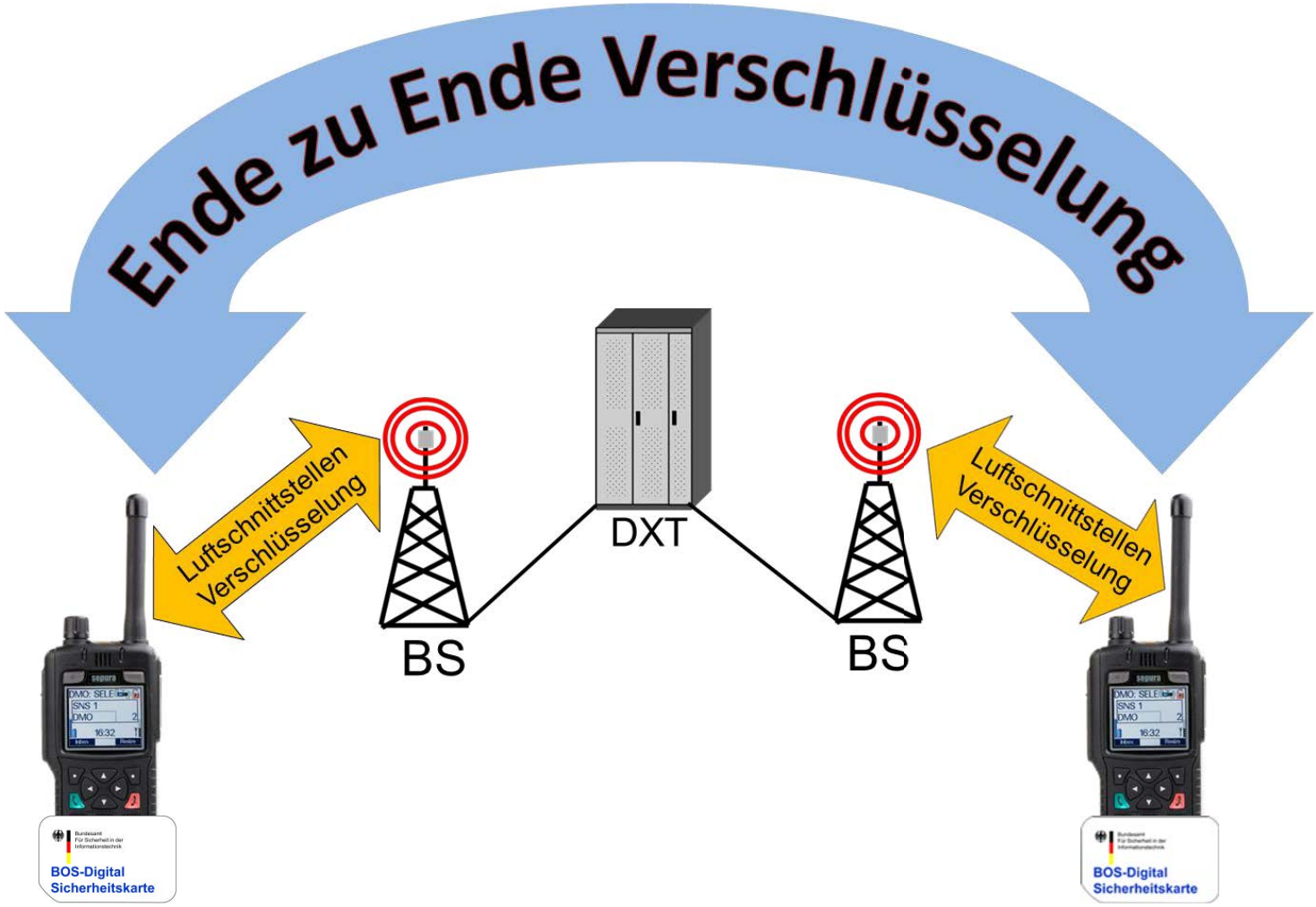
Luftschnittstellen-Verschlüsselung

Luft(Funk)schnittstelle zwischen Basisstation und Endgerät ist verschlüsselt.



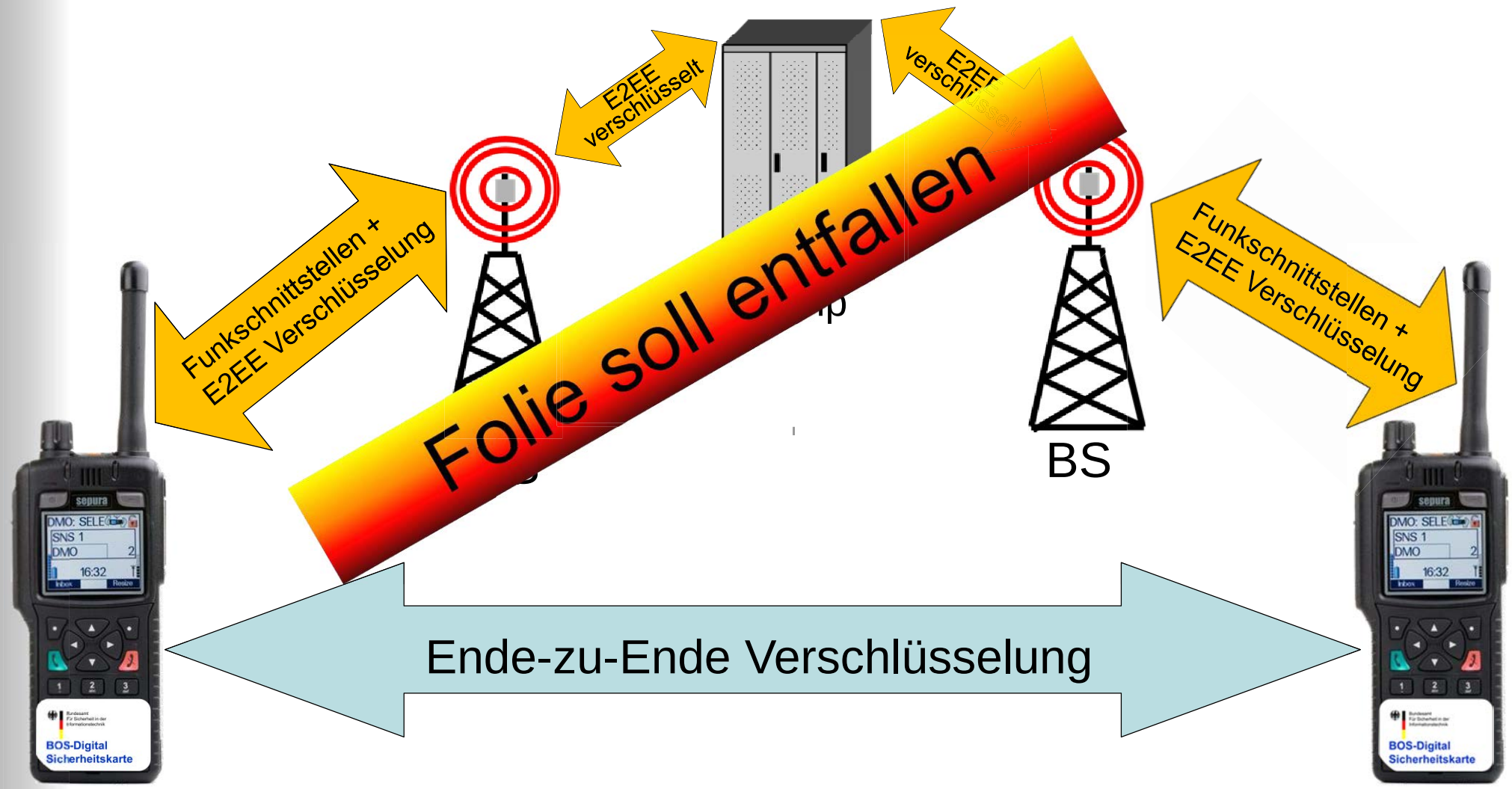
Ende-zu-Ende Verschlüsselung

leistungsstärkste Verschlüsselungsmethode in TETRA

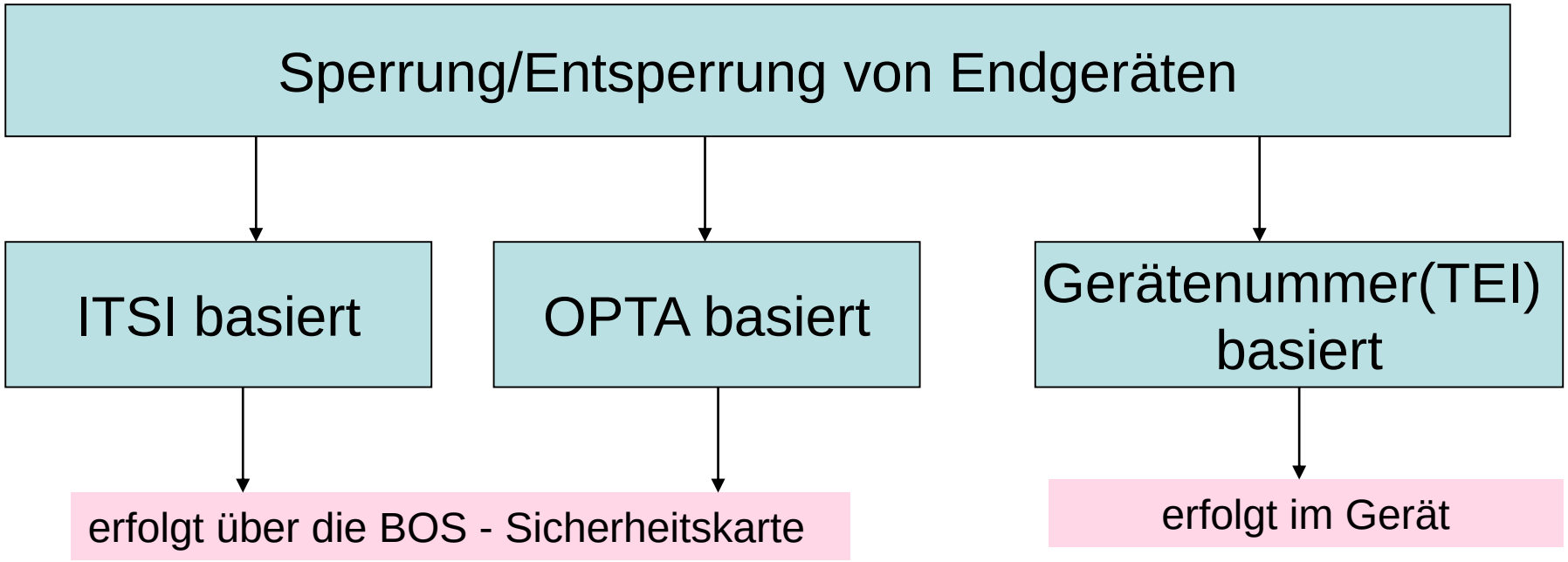


Ende-zu-Ende Verschlüsselung

leistungsstärkste Verschlüsselungsmethode in TETRA



Aktivierung/Deaktivierung



Temporär oder permanent durch

- TTB (z. B. Leitstelle)
- Autorisierte Stelle
- NMC

NEM = Nutzereigenes Management

NMC = Network Management Center

TEI = Terminal Equipment Identity

Sperren des Endgerätes

Verlustmeldung von Endgerät an TTB

TTB/Endnutzer entscheidet über Art der Sperrung

- Temp. Sperrung der BOS - Sicherheitskarte
- Temp. Sperrung des Endgerätes
- Löschung der Daten Endgerät und BOS-Sicherheitskarte aus dem System

Durchführung der Sperrung über die AS

Grundfunktionen der BOS Sicherheitskarte

Ende zu Ende Verschlüsselung
Schlüsselmanagement

Netzzugangsberechtigung
SIM-Funktion

Taktische Funktion
Speicherung der operativ-taktischen Adresse

Sichere Datenspeicherung
Endgerätedaten nach ETSI Standard
ETSI ES 200 812-2 V2.4.1 (2005-08)

Kategorien der Sicherheitskarte

- **Unpersonalisierte Karte (BSI-Rohling)**
  vom BSI programmiert:
  Netzzugangsberechtigung (ITSI), Verschlüsselung

- **Personalisierte Karte**
  von der AS Bayern programmiert:
  (taktische Funktion: Geburts- und Alias-OPTA)

- **Eingelegte personalisierte Karte mit Endgerä**

Grundsätzlich gilt:

Vor Abgabe des Endgeräts außerhalb des Verfügungsbereich Endnutzers ist die BOS-Sicherheitskarte zu entfernen.

AS = Autorisierte Stelle
BSI = Bundesamt für Sicherheit in der Informationstechnik

Sicherheitshinweise im Umgang mit der BOS-Sicherheitskarte

- **Ohne Sicherheitskarte kein Teilnahme im Funknetz**
- **Bei Defekt eines Gerätes ist die Sicherheitskarte zu entfernen**
- **Nicht eingesetzte Sicherheitskarten sind sicher zu verwahren**
- **Sicherheitskarten von ausgemusterten Geräten sind an die BDBOS zurück zu senden**

Umgang mit der BOS - Sicherheitskarte

Folgende Schritte sind bei einer temporären Sperrung zwingend durchzuführen:

Vor Abgabe des Fahrzeugs:

1. **Vorläufige Sperrung der BOS Sicherheitskarte im NeM Werkzeug Tactilon durch die TTB.**

2. **Nach erfolgter Sperrung muss eine Anmeldung des Gerätes in betrieb Modus (TMO) erfolgen. Durch die Verbindung zum Net Sperrung wirksam, und das Gerät ist mit dieser Karte nicht mehr bedienbar.**

3. **Ausschalten des Gerätes**

Nach Rücknahme des Fahrzeugs:

4. **Entsperrung der BOS Sicherheitskarte in Tactilon**

5. **Einschalten des Geräts und Anmeldung im Netzbetrieb Modus (T Verbindungsaufnahme zum Netz wird die Karte entsperrt und das wieder bedienbar.**

Bestellvorgang BOS-Sicherheitskarte

Die Bestellung der BOS-Sicherheitskarten erfolgt durch den Endnutzer über die jeweils zuständige **TTB** an die **AS BY** unter folgender Adresse:

Bayerisches Landeskriminalamt
SG 324 Service und Betrieb Digitalfunk
Autorisierte Stelle Bayern
(Endgerätemanagement)

TTB = Taktisch-Technische-Betriebsstelle

Ende

Technische Informationen

Quellennachweis:

- Bayerisches Staatsministerium des Innern - Projektgruppe DigiNet
- Institut der Feuerwehr Nordrhein-Westfalen

Cliparts:

- A & C Lochmeier, Firegrafics GmbH, CH- 8570 Weinfelden, www.firegrafics.ch.

Änderungsnachweis:

- 23.02.2010 Erstfassung
- 28.05.2010 Folie „TBS Fallback“ entfernt. Folien 17 und 23 aktualisiert.
- 14.07.2010 Folie 11 aktualisiert.
- 28.11. 2011 kompletten Foliensatz überarbeitet / Ingenpaß
- 19.12.2012 Änderung Bearbeiter und Versionstand 1.0 / Jaensch
- 12.03.2013 Änderung von BSI Sicherheitskarte nach BOS Sicherheitskarte auf diversen Folien
- 22.07.2014 Änderungen durch Andreas Kreuzpaintner
- 11.07.2017 komplett überarbeitet und im AKAD abgestimmt