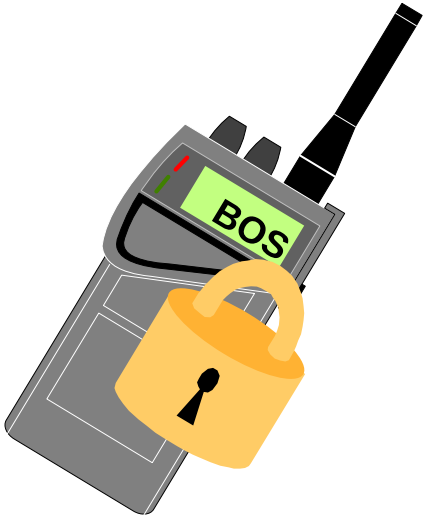
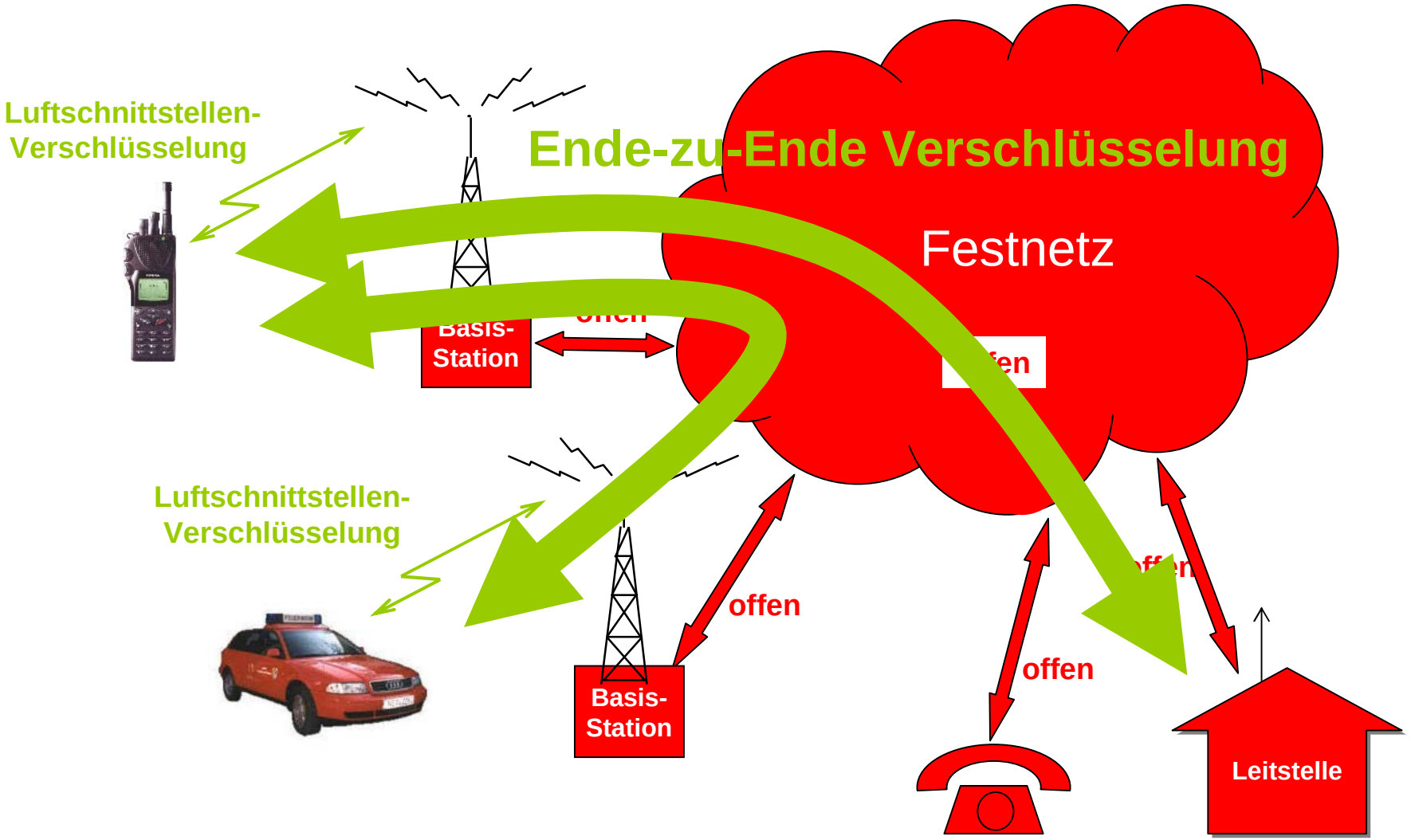
Ende- zu Ende- Verschlüsselung
BOS



Übersicht

- **Informationssicherheit im TETRA-Standard**
- **Verschlüsselungssystem, Komponenten, Funktionen**
- **Verteilung der BOS-Sicherheitskarte (Prozesskette)**
- **Simulationssystem**

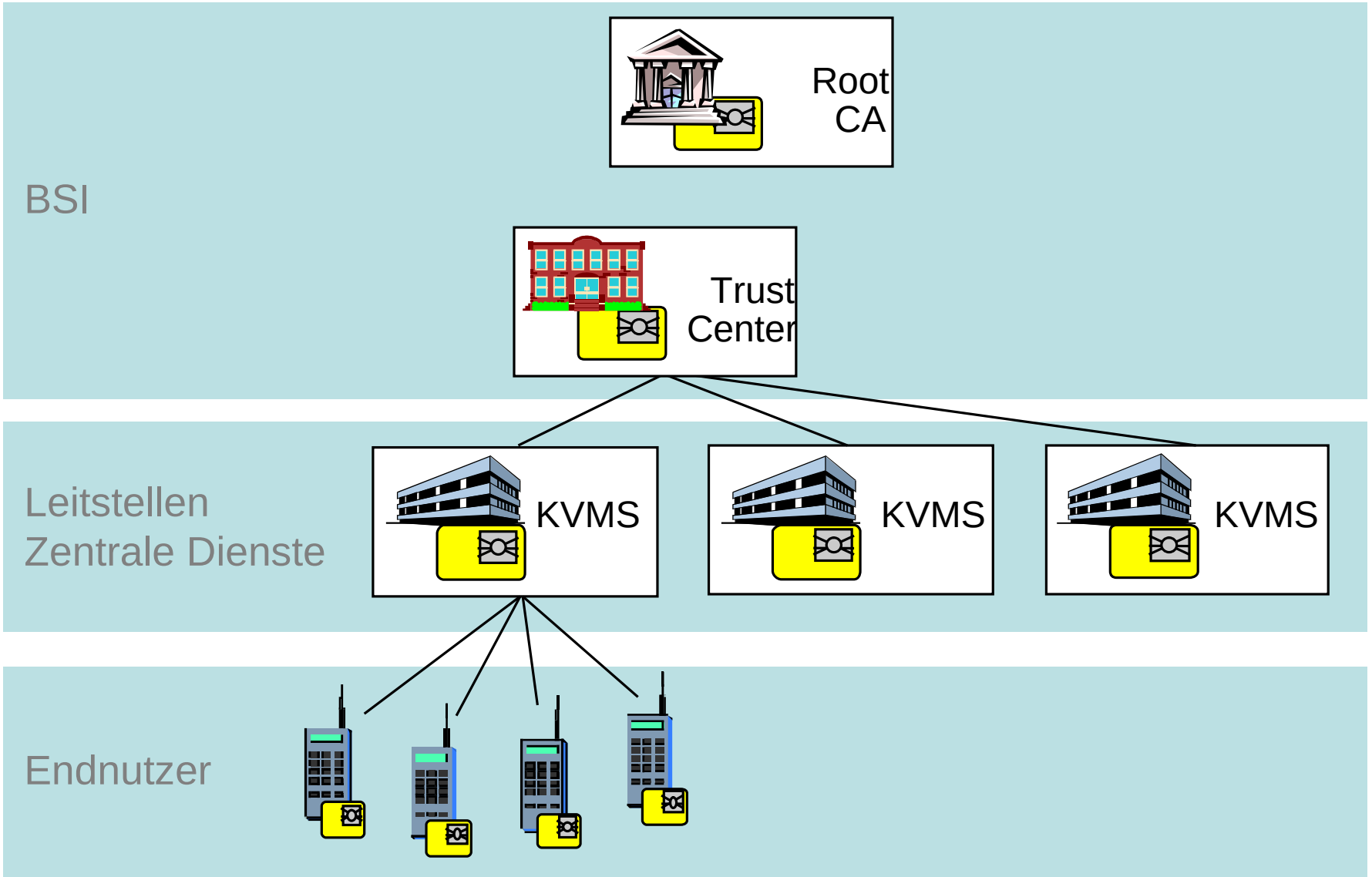
Informationssicherheit im Mobilfunkstandard TETRA



Verschlüsselte Funkbetriebsarten der Endgeräte

- **Gruppenruf in TMO und DMO**
- **Einzelruf in TMO und DMO**
- **Kurznachrichten SDS in TMO und DMO**
- **Datenbetrieb in TMO und DMO (noch nicht spezifiziert)**
- **Operativ-taktische Adresse in TMO und DMO**

Gesamtsystemarchitektur



Sicherheitskarte

- **Einkanalkryptokomponente für:**

  Mobile Funkstationen
  Ortsfeste Funkstationen

- **1 Kommunikationskanal (duplex)**

Grundfunktionen der Sicherheitskarte

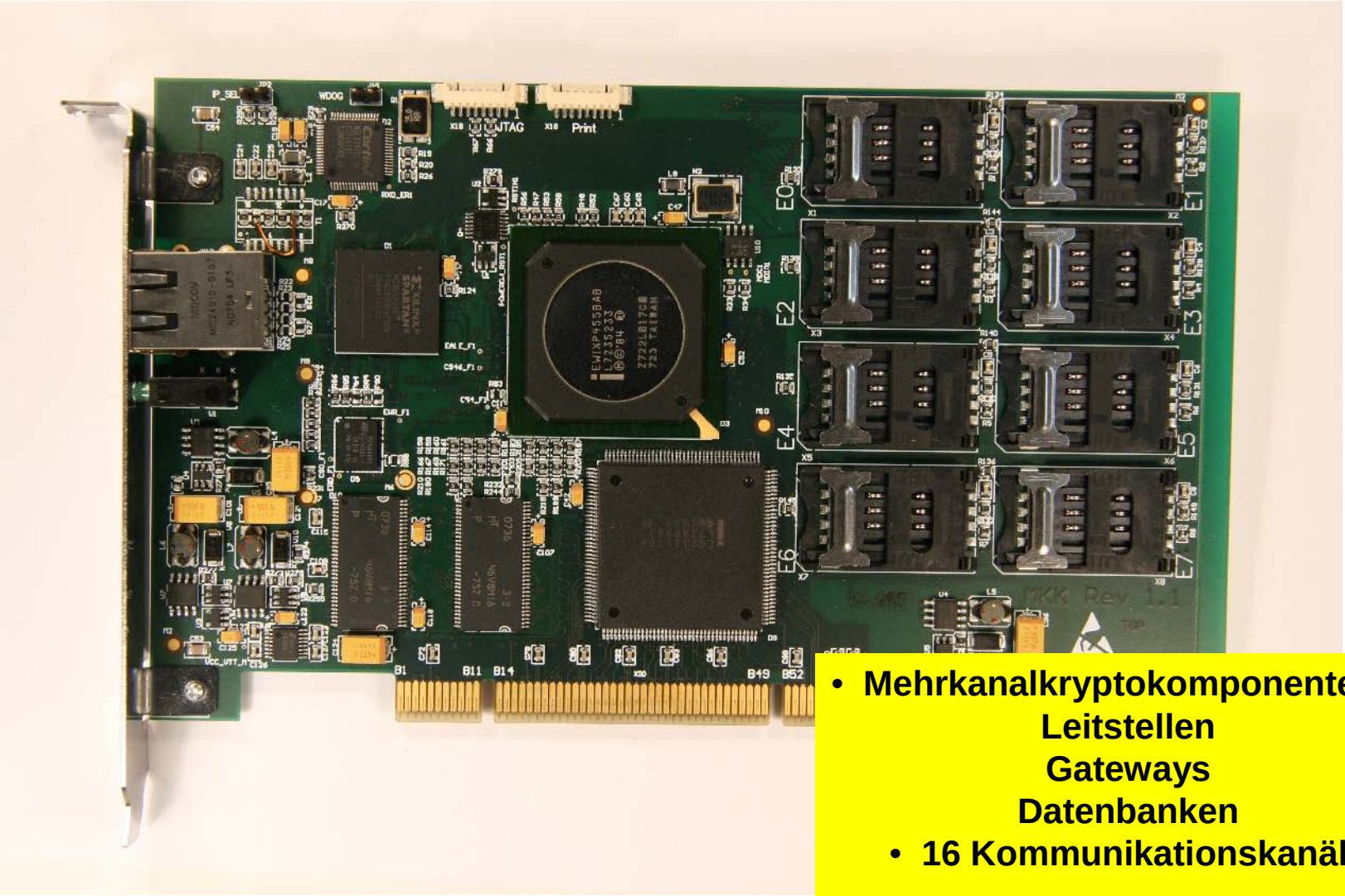
Ende-zu-Ende Verschlüsselung
Schlüsselmanagement

Netzzugangsberechtigung
SIM-Funktion

Taktische Funktionen
Speicherung der operativ-taktischen Adresse

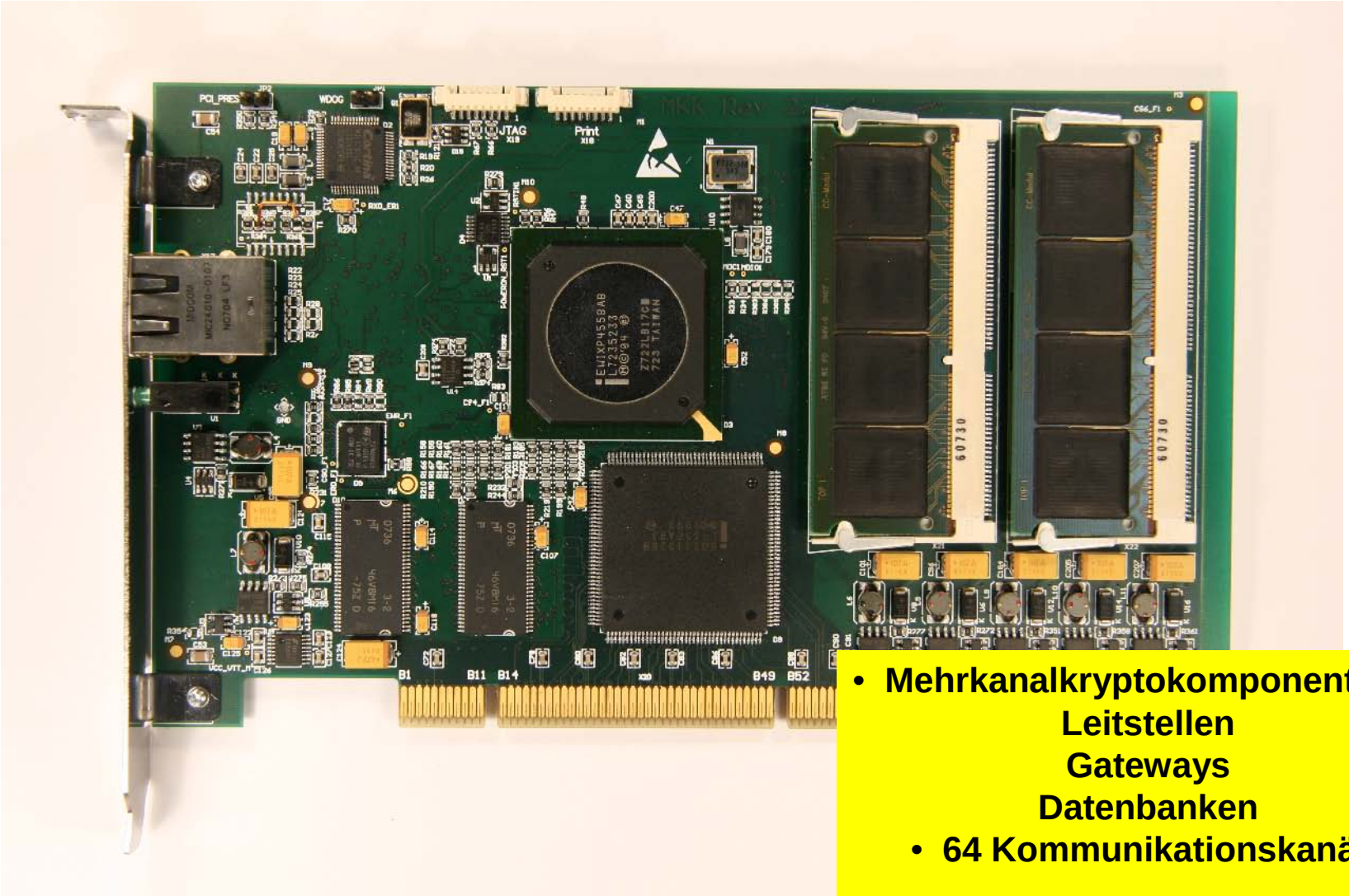
Sichere Datenspeicherung
Endgerätedaten nach ETSI Standard
ETSI ES 200 812-2 V2.4.1 (2005-08)

BOS Mehrkanalkryptokomponente MKK I



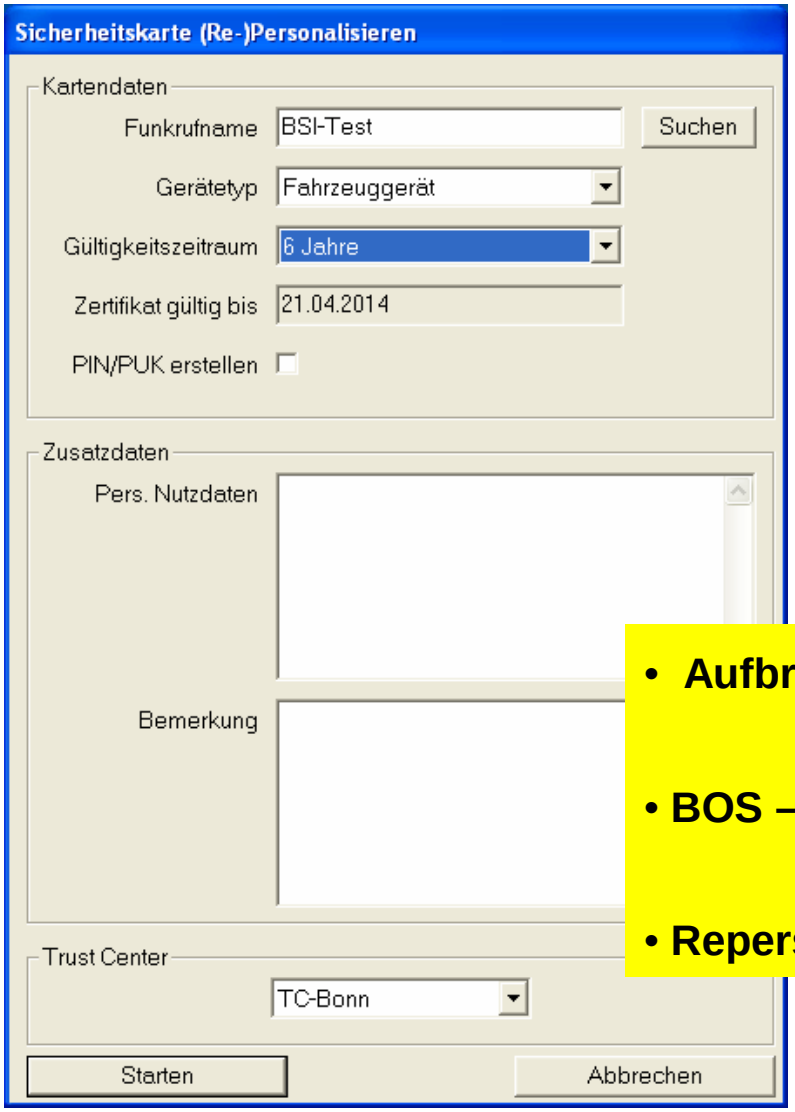
- **Mehrkanalkryptokomponente für:**
  Leitstellen
  Gateways
  Datenbanken
- **16 Kommunikationskanäle**

BOS Mehrkanalkryptokomponente MKK II



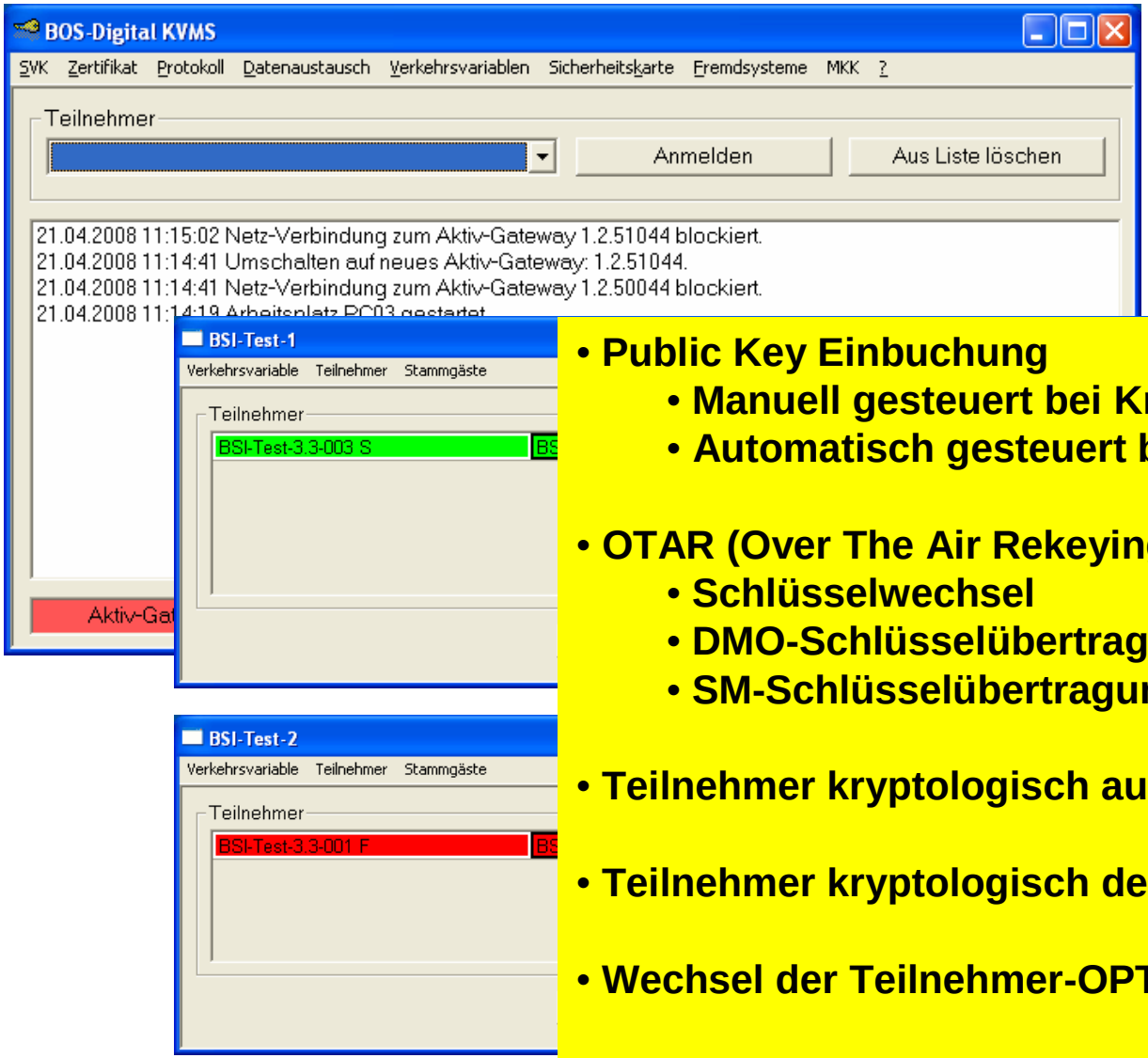
- **Mehrkanalkryptokomponente für:**
  Leitstellen
  Gateways
  Datenbanken
- **64 Kommunikationskanäle**

Personalisierungsfunktion KVMS



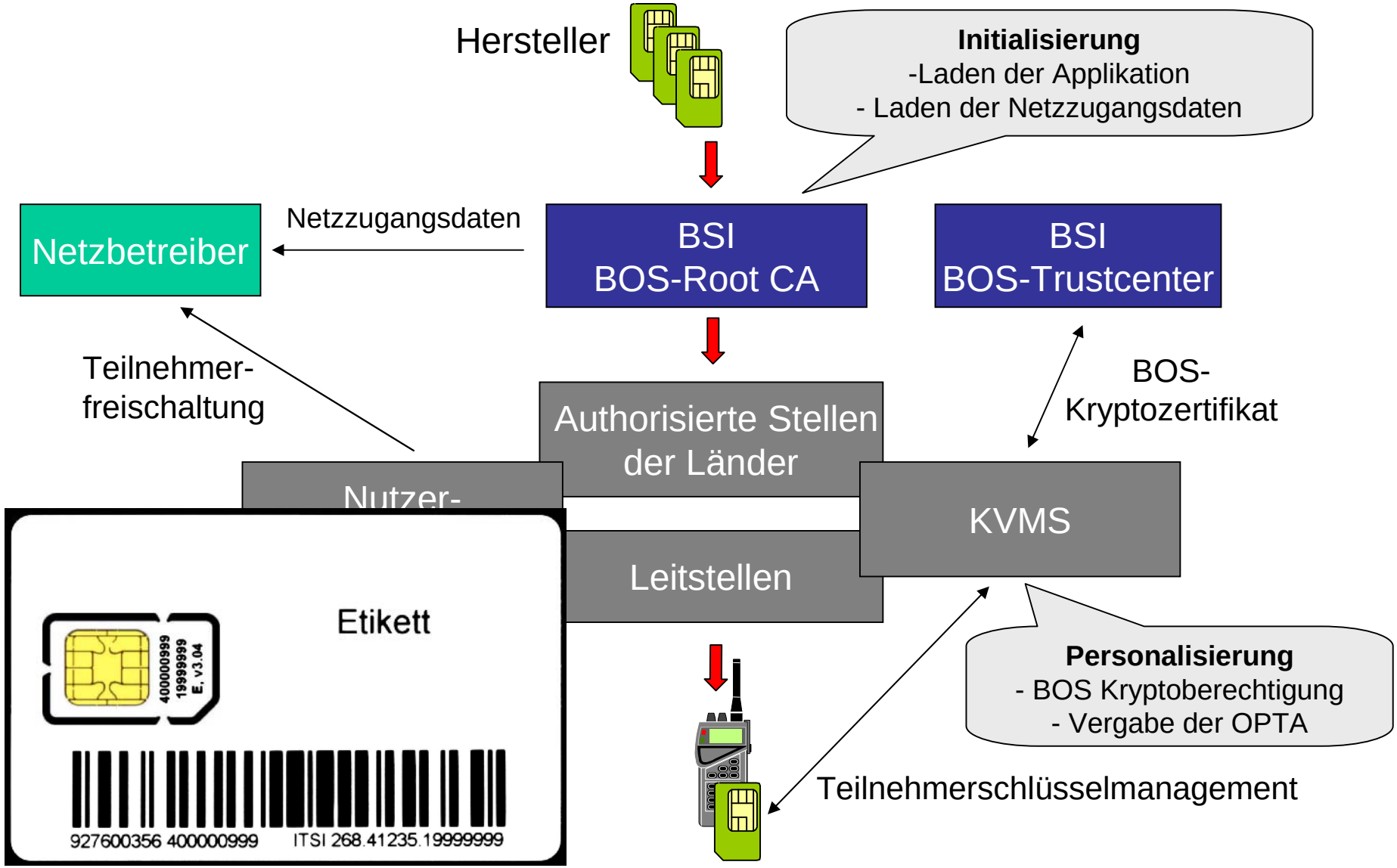
- **Aufbringen der operativ-taktischen Adresse (OPTA)**
- **BOS – Zertifikatsdownload vom Trustcenter**
- **Repersonalisieren von Sicherheitskarten**

Schlüsselmanagementfunktion KVMS

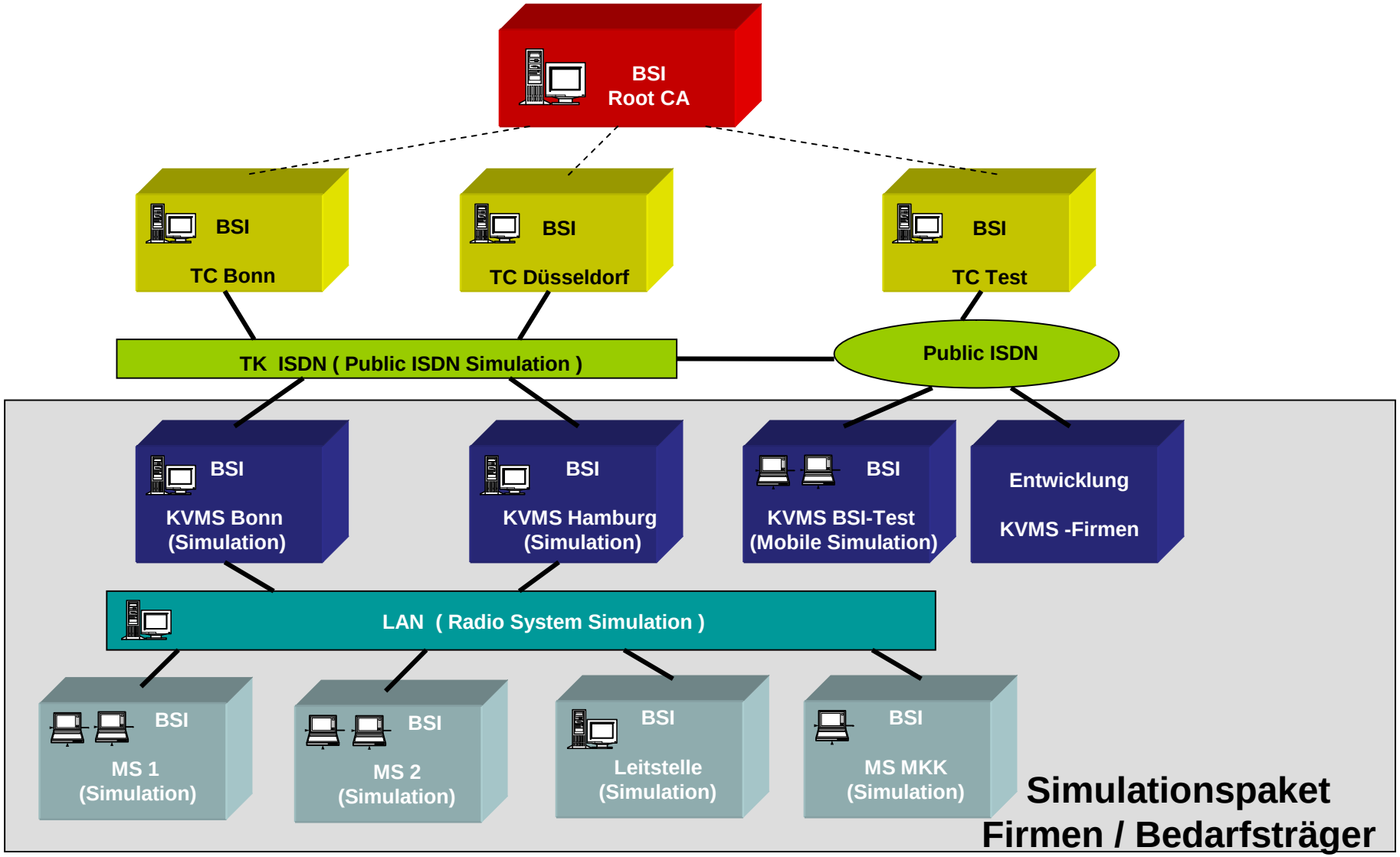


- **Public Key Einbuchung**
  - **Manuell gesteuert bei Kryptoverkehrskreiswechsel**
  - **Automatisch gesteuert bei Ersteinbuchung**
- **OTAR (Over The Air Rekeying)**
  - **Schlüsselwechsel**
  - **DMO-Schlüsselübertragung**
  - **SM-Schlüsselübertragung (SDS)**
- **Teilnehmer kryptologisch ausschließen**
- **Teilnehmer kryptologisch deaktivieren**
- **Wechsel der Teilnehmer-OPTA**

Verteilung der Sicherheitskarten (Prozesskette)



BSI Simulationssystem



Georg Merzbach
Dipl.-Ing.

Entwicklung von
Kryptosystemen

Tel.: +49 1888 9582-5541
Fax: +49 1888 9582-5755

E-Mail: Georg.Merzbach@bsi.bund.de

Bundesamt für Sicherheit
in der Informationstechnik