

Ende- zu Ende- Verschlüsselung BOS

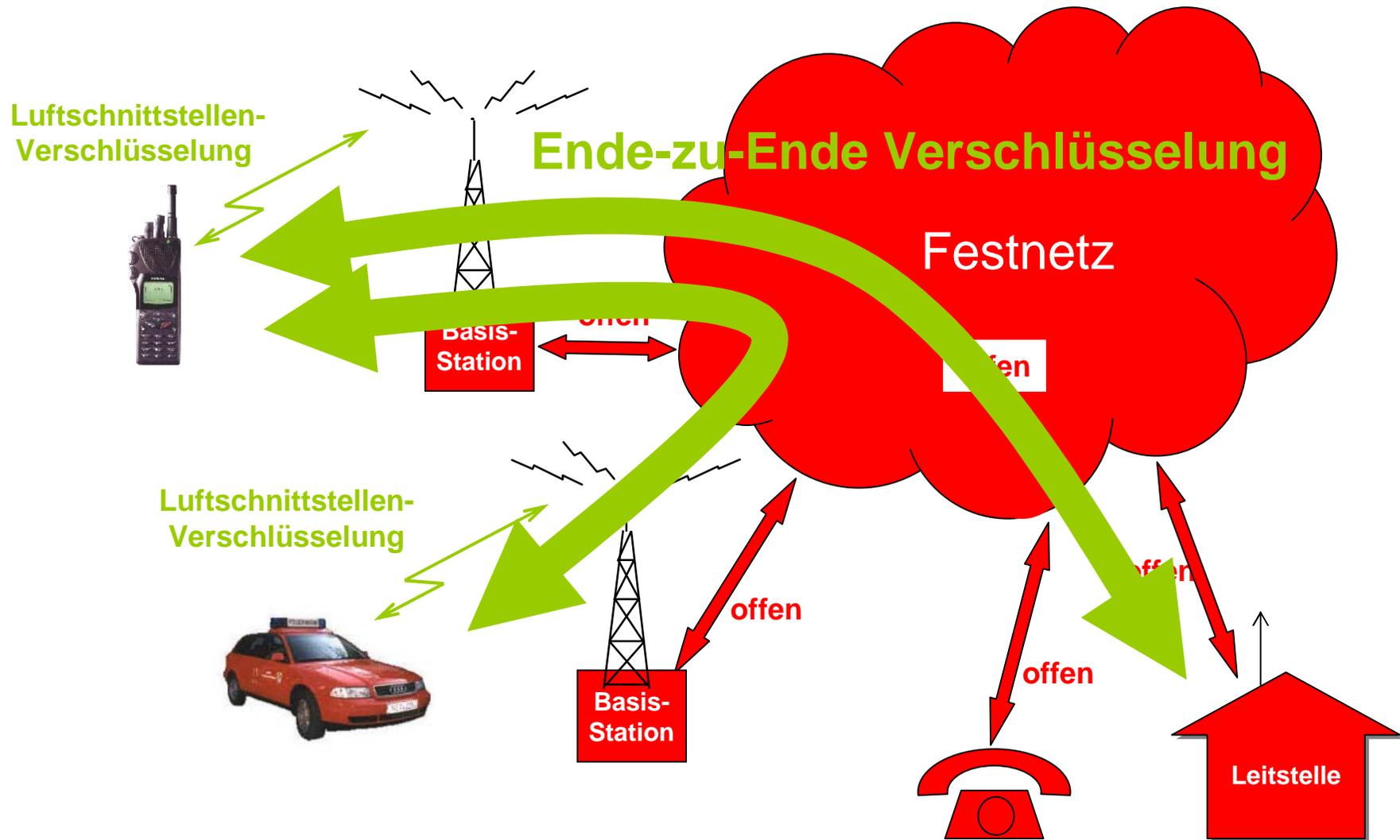


Übersicht

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



Informationssicherheit im Mobilfunkstandard TETRA

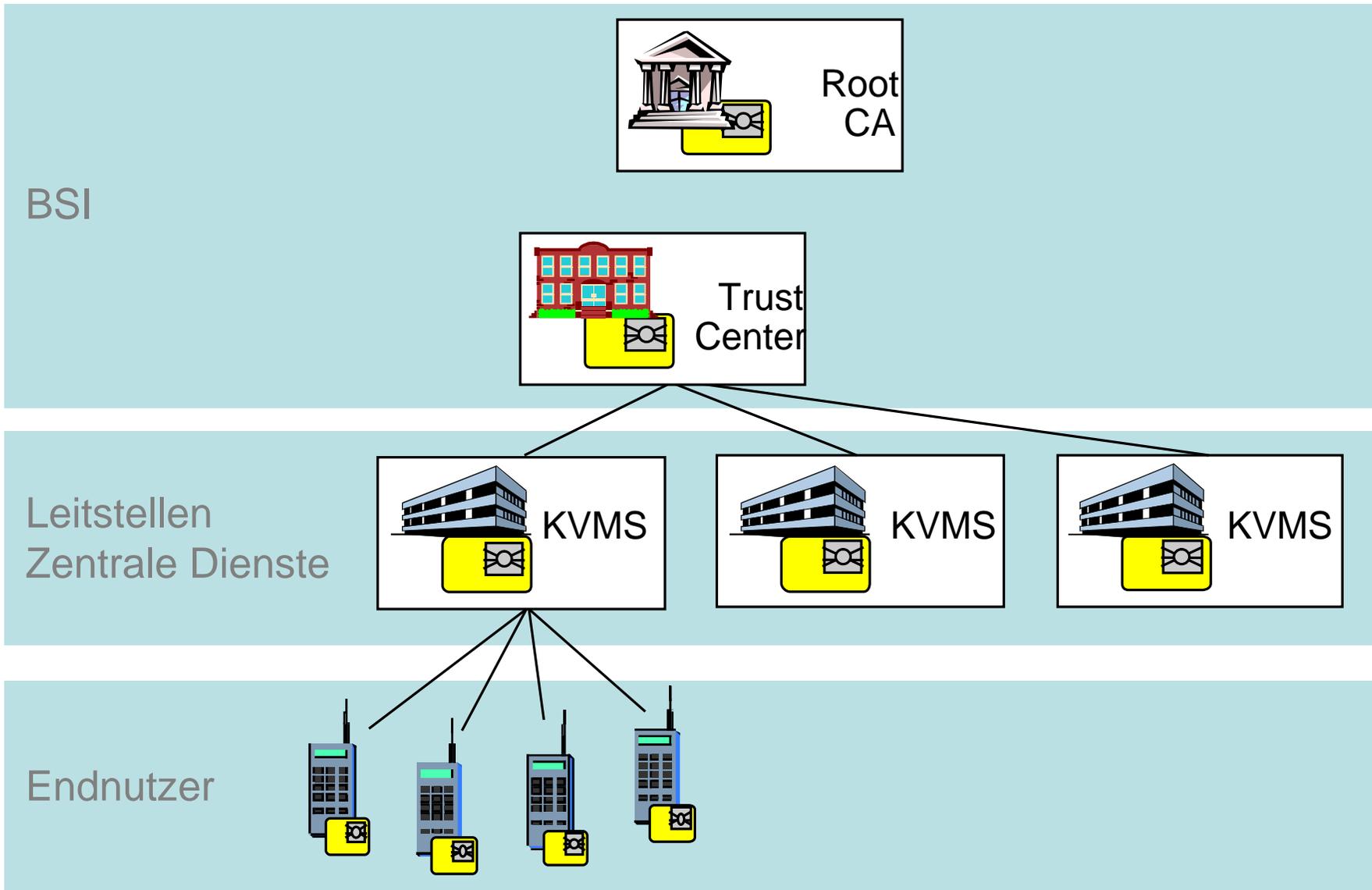


Verschlüsselte Funkbetriebsarten der Endgeräte

- **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

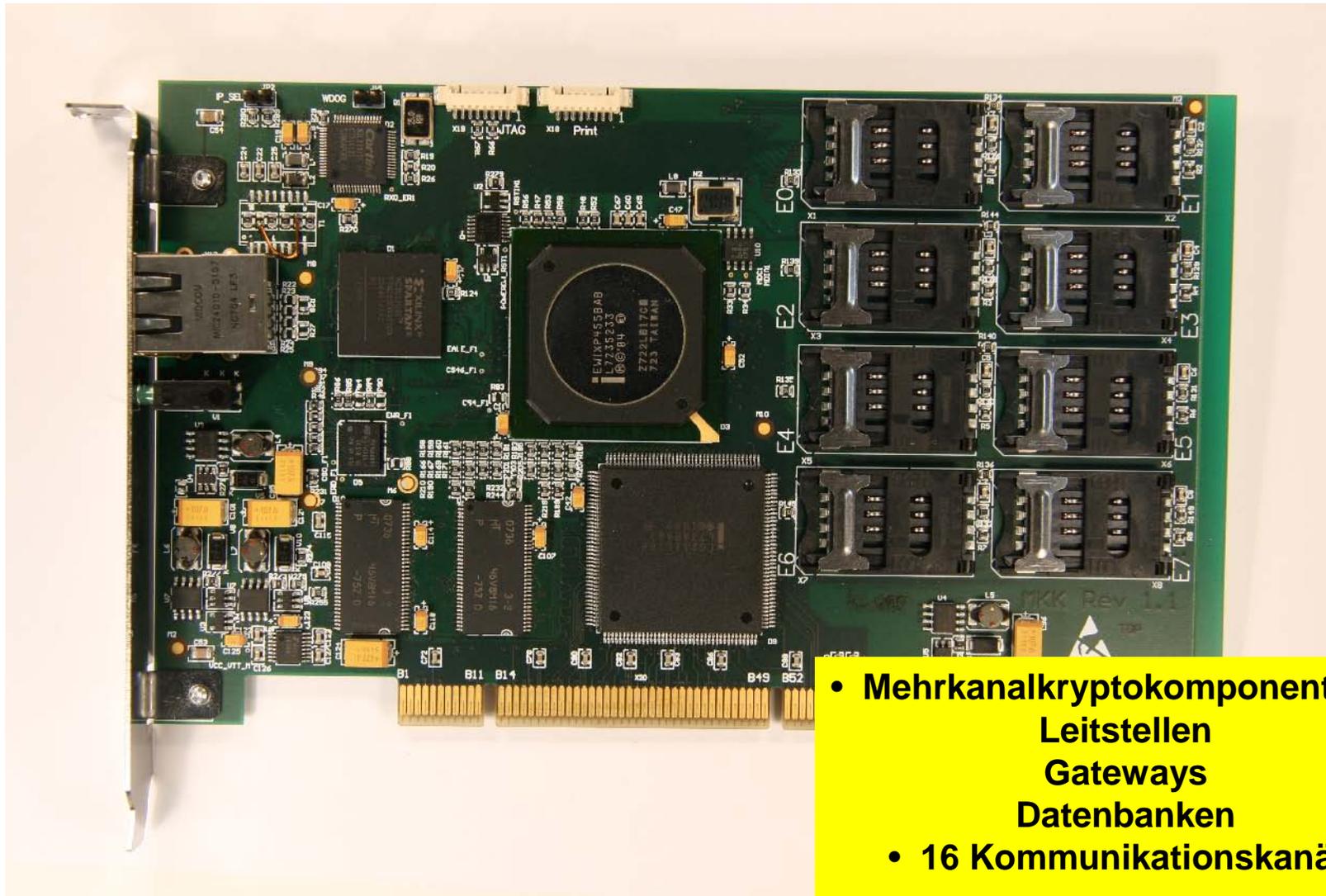


Taktische Funktionen
Speicherung der operativ-taktischen Adresse

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



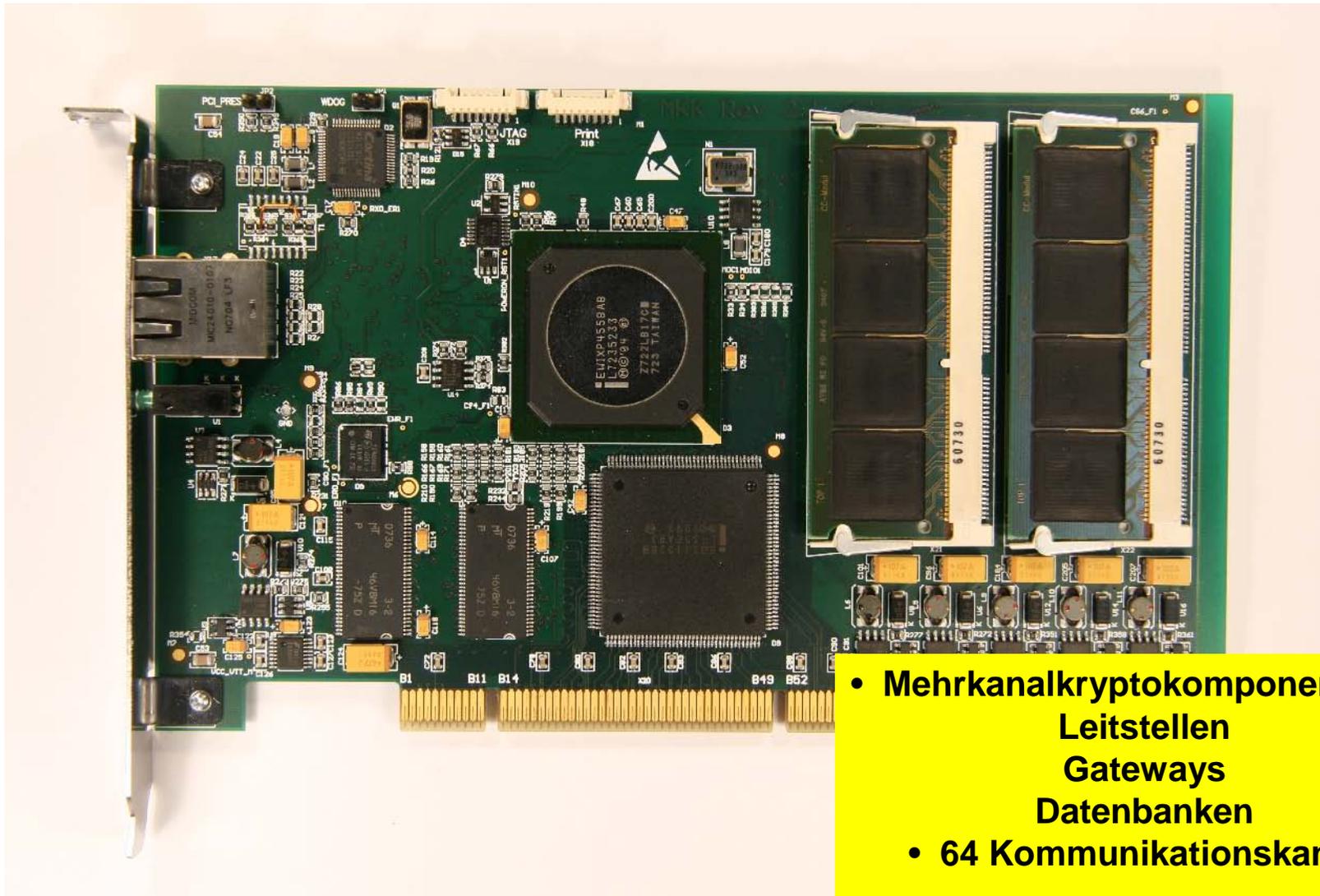
BOS Mehrkanalkryptokomponente MKK I



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



BOS Mehrkanalkryptokomponente MKK II



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

Personalisierungsfunktion KVMS

Sicherheitskarte (Re-)Personalisieren

Kartendaten

Funkrufname

Gerätetyp

Gültigkeitszeitraum

Zertifikat gültig bis

PIN/PUK erstellen

Zusatzdaten

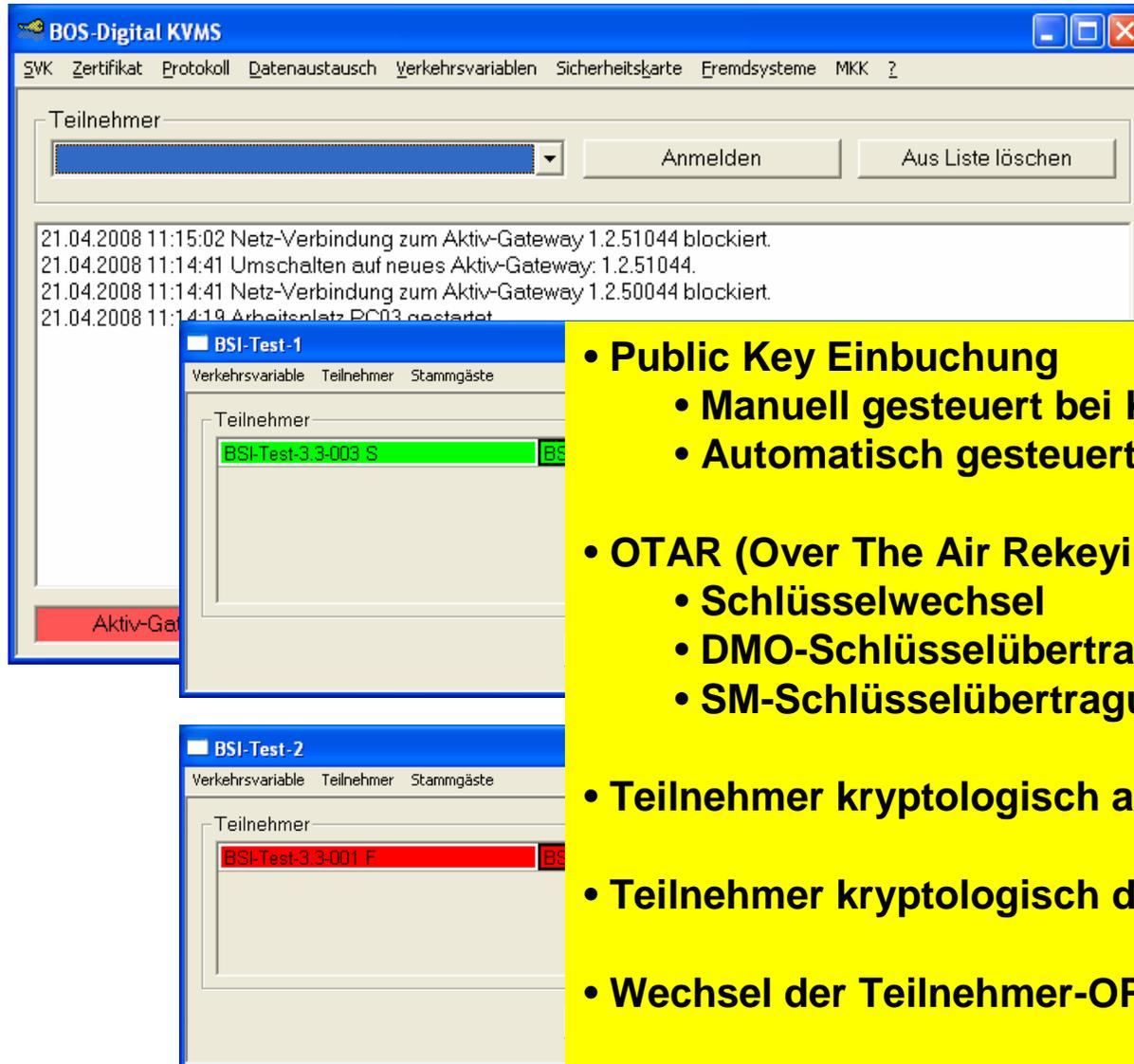
Pers. Nutzdaten

Bemerkung

Trust Center

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

Schlüsselmanagementfunktion KVMS



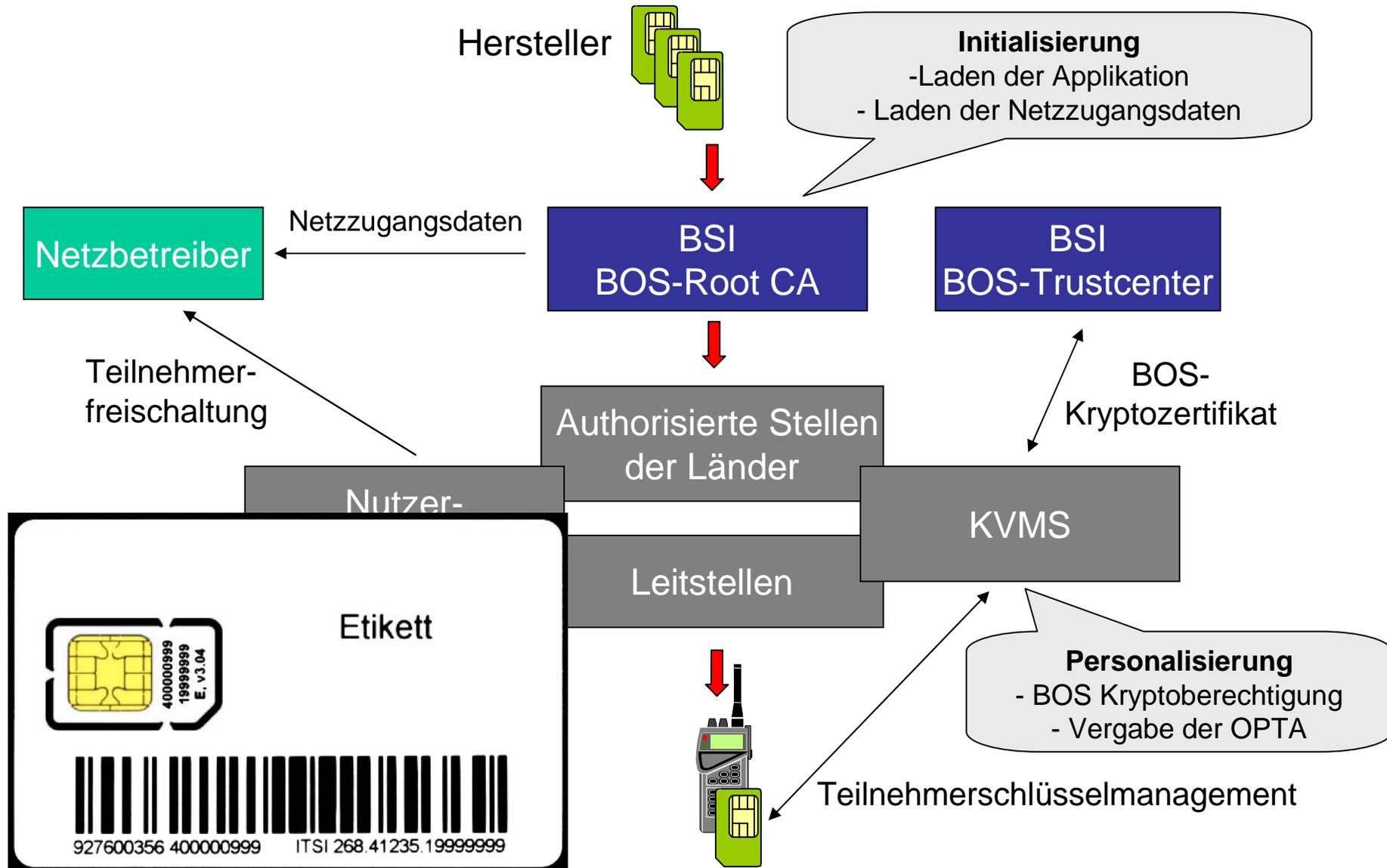
The screenshot displays the BOS-Digital KVMS interface. The main window has a menu bar with options: SVK, Zertifikat, Protokoll, Datenaustausch, Verkehrsvariablen, Sicherheitskarte, Fremdsysteme, MKK, and a help icon. Below the menu is a 'Teilnehmer' section with a dropdown menu and buttons for 'Anmelden' and 'Aus Liste löschen'. A log window shows the following entries:

- 21.04.2008 11:15:02 Netz-Verbindung zum Aktiv-Gateway 1.2.51044 blockiert.
- 21.04.2008 11:14:41 Umschalten auf neues Aktiv-Gateway: 1.2.51044.
- 21.04.2008 11:14:41 Netz-Verbindung zum Aktiv-Gateway 1.2.50044 blockiert.
- 21.04.2008 11:14:19 Arbeitsplatz PC03 gestartet.

Below the log, there are two smaller windows, 'BSI-Test-1' and 'BSI-Test-2', each with a 'Teilnehmer' list. In 'BSI-Test-1', the participant 'BSI-Test-3.3-003 S' is highlighted in green. In 'BSI-Test-2', the participant 'BSI-Test-3.3-001 F' is highlighted in red. A red bar at the bottom of the main window is labeled 'Aktiv-Gat'.

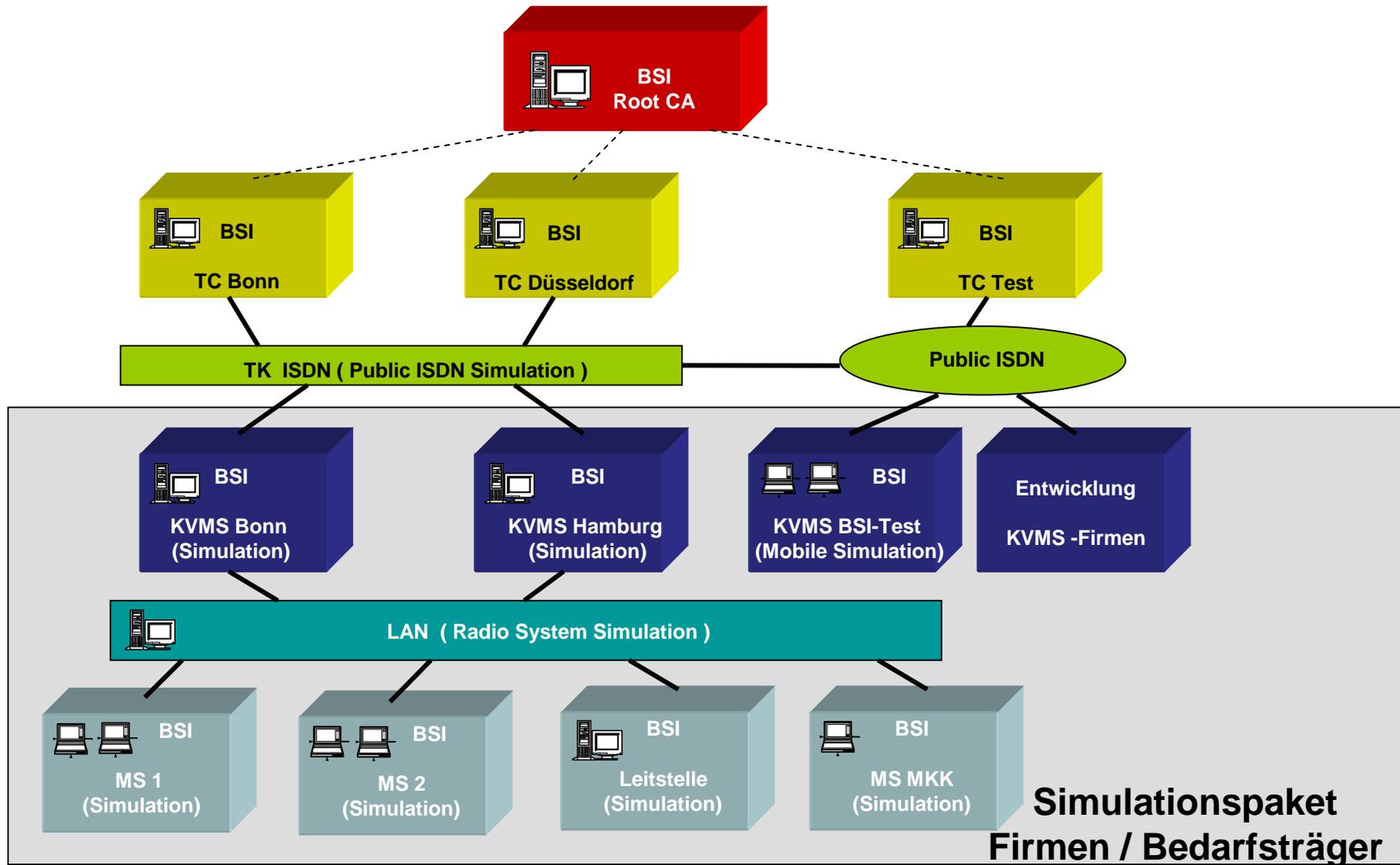
- **Public Key Einbuchung**
 - Manuell gesteuert bei Kryptoverkehrskreiswechsel
 - Automatisch gesteuert bei Ersteinbuchung
- **OTAR (Over The Air Rekeying)**
 - Schlüsselwechsel
 - DMO-Schlüsselübertragung
 - SM-Schlüsselübertragung (SDS)
- Teilnehmer kryptologisch ausschließen
- Teilnehmer kryptologisch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

Verteilung der Sicherheitskarten (Prozesskette)





BSI Simulationssystem





Vielen Dank für Ihre Aufmerksamkeit!

Georg Merzbach
Dipl.-Ing.

Entwicklung von
Kryptosystemen

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

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