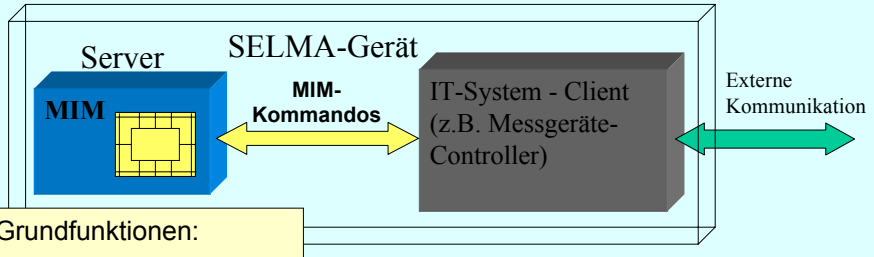
Funktionen des SELMA-Sicherheitsmoduls

Norbert Zisky
Physikalisch-Technische Bundesanstalt

MIM-Kommando:
Kurzer eindeutig festgelegter SELMA-Befehl

SELMA-Sicherheitsmodul - MIM als physikalisch separate Einheit



Grundfunktionen:

- Schlüsselerzeugung
- Schlüsselspeicherung
- Hashen von Daten
- Signieren von Daten
- Verifizieren von Daten

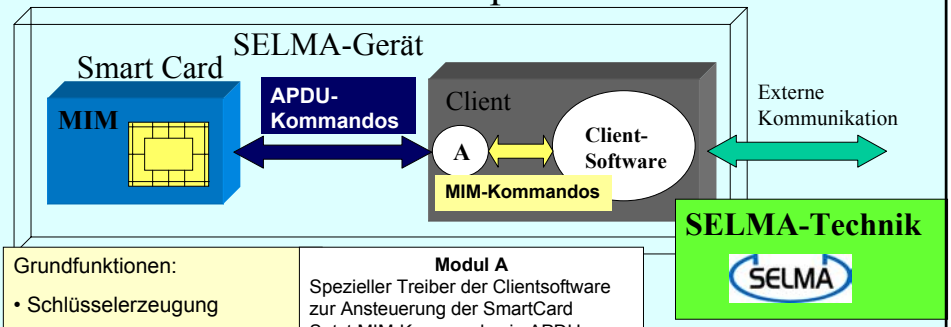
Alle sicherheitsrelevanten Funktionen laufen im MIM ab

Manipulation nur mit sehr hohem Aufwand möglich,

Restrisiko gering

APDU-Kommando: Komplizierte ISO-7816- und SmartCard-spez- Befehle (herstellerspez.)

SELMA-Sicherheitsmodul - MIM als Smart Card mit speziellem Treiber



Grundfunktionen:

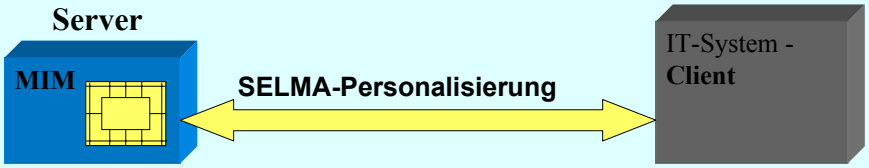
- Schlüsselerzeugung
- Schlüsselspeicherung
- Hashen von Daten
- Signieren von Daten
- Verifizieren von Daten

Modul A
Spezieller Treiber der Clientsoftware zur Ansteuerung der SmartCard
Setzt MIM-Kommandos in APDU-Kommandofolgen um.

Alle sicherheitsrelevanten Funktionen laufen im MIM ab

Manipulation nur mit hohem Aufwand möglich, Restrisiko gering

SELMA-Sicherheitsmodul - MIM Initialisierung des MIM (Personalisierung)



Voraussetzung für alle kryptographischen Funktionen

- Anlegen einer Filestruktur
- Schreiben der Domänparameter
- Setzen von Sicherheitsoptionen

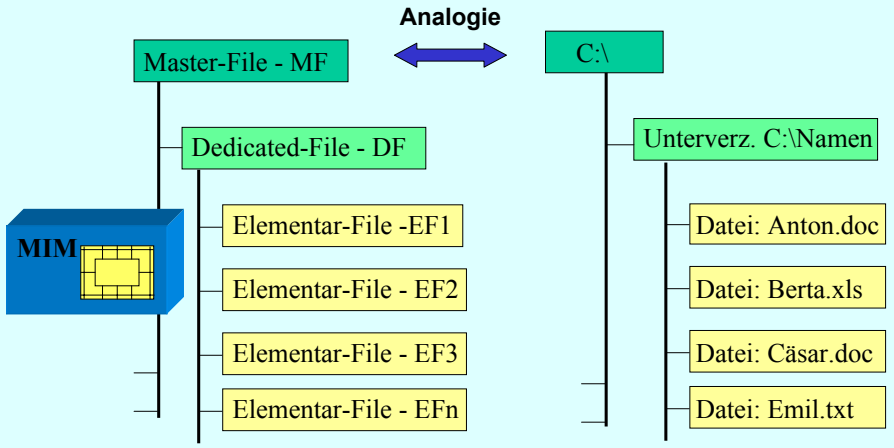
SELMA-Zusatzfunktionen

- Eintragen externer öffentlicher Schlüssel

Anlegen der MIM-Filestruktur

- **Anlegen einer Filestruktur**
- Schreiben der Domänparameter
- Setzen von Sicherheitsoptionen

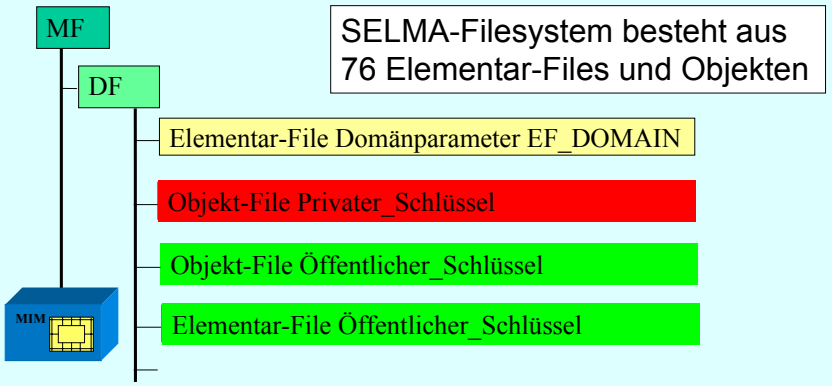
> Struktur ist mit normalen Datenträgern aus der PC-Welt vergleichbar



Anlegen von Elementarfiles

- **Anlegen einer Filestruktur**
- Schreiben der Domänparameter
- Setzen von Sicherheitsoptionen

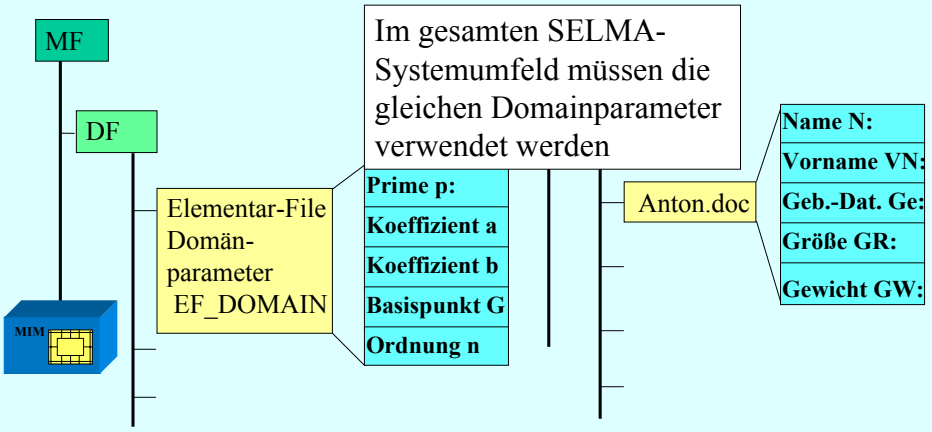
> Elementarfiles und Datenobjekte



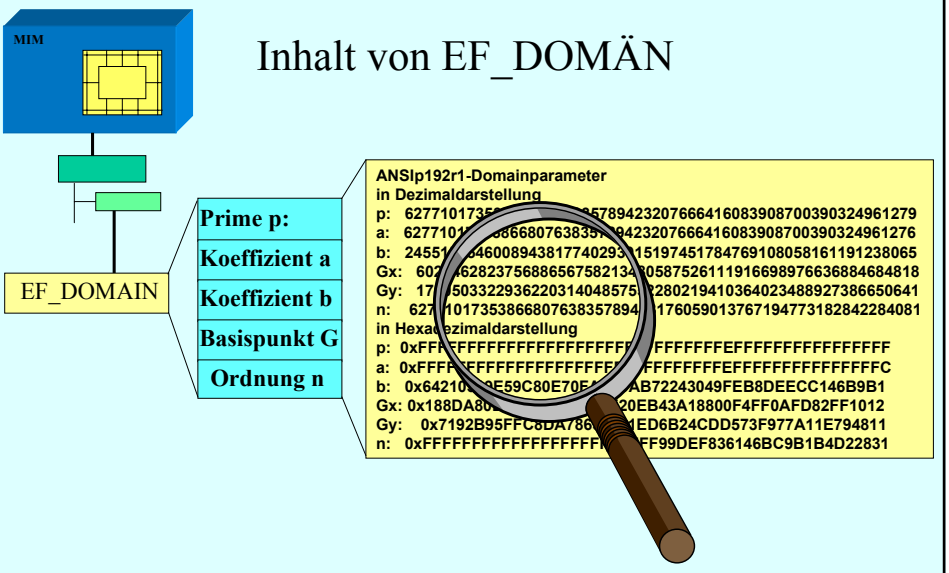
Schreiben Domänparameter

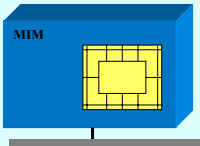
- Anlegen einer Filestruktur
- **Schreiben der Domänparameter**
- Setzen von Sicherheitsoptionen

> Elementarfiles können auch Datenstrukturen enthalten



Inhalt von EF_DOMÄN





Inhalt von EF_DOMÄN

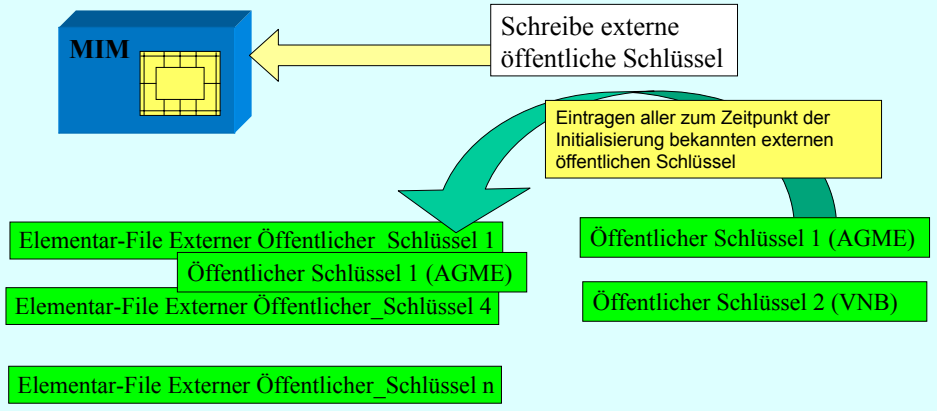
ANSIp192r1-Domainparameter
in Dezimaldarstellung

p: 6277101735386680763835789423207666416083908700390324961279
a: 6277101735386680763835789423207666416083908700390324961276
b: 2455155546008943817740293915197451784769108058161191238065
Gx: 602046282375688656758213480587526111916698976636884684818
Gy: 174050332293622031404857552280219410364023488927386650641
n: 627710173538668076383578942317605901376719477318284228 4081

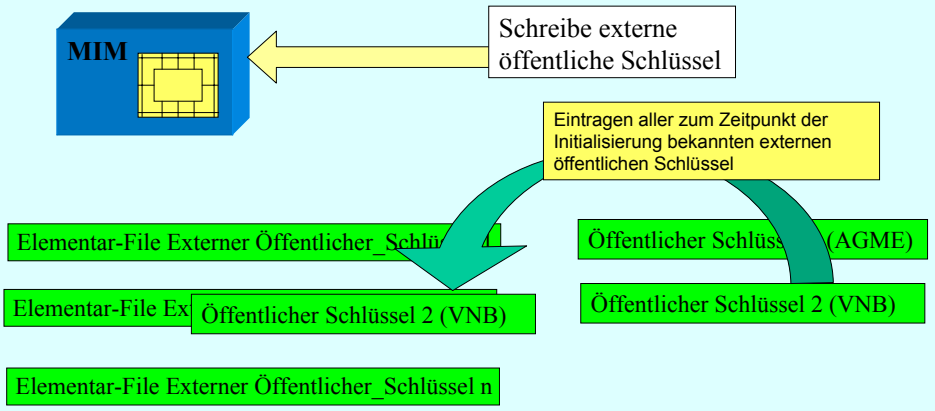
in Hexadezimaldarstellung

p: 0xFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFEFFFFFFFFFFFFFFF
a: 0xFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFEFFFFFFFFFFFFFFC
b: 0x64210519E59C80E70FA7E9AB72243049FEB8DEECC146B9B1
Gx: 0x188DA80EB03090F67CBF20EB43A18800F4FF0AFD82FF1012
Gy: 0x7192B95FFC8DA78631011ED6B24CDD573F977A11E794811
n: 0xFFFFFFFFFFFFFFFFFFFFFFFF99DEF836146BC9B1B4D22831

Eintragen externer öffentlicher Schlüssel



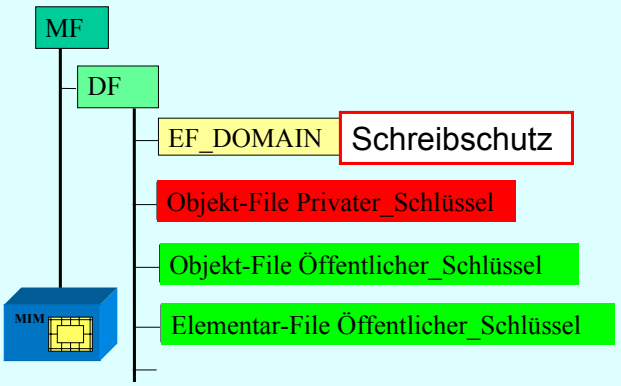
Eintragen externer öffentlicher Schlüssel



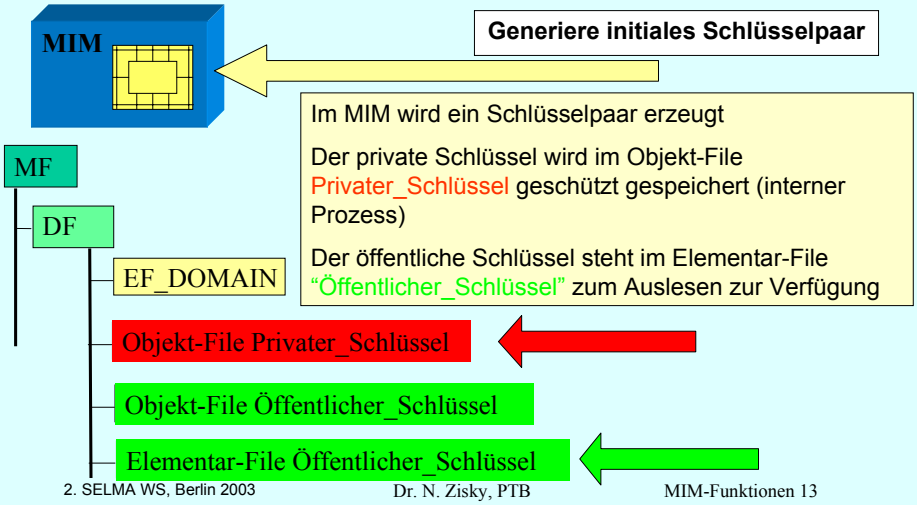
Setzen von Sicherheitsoptionen

- Anlegen einer Filestruktur
- Schreiben der Domänparameter
- **Setzen von Sicherheitsoptionen**

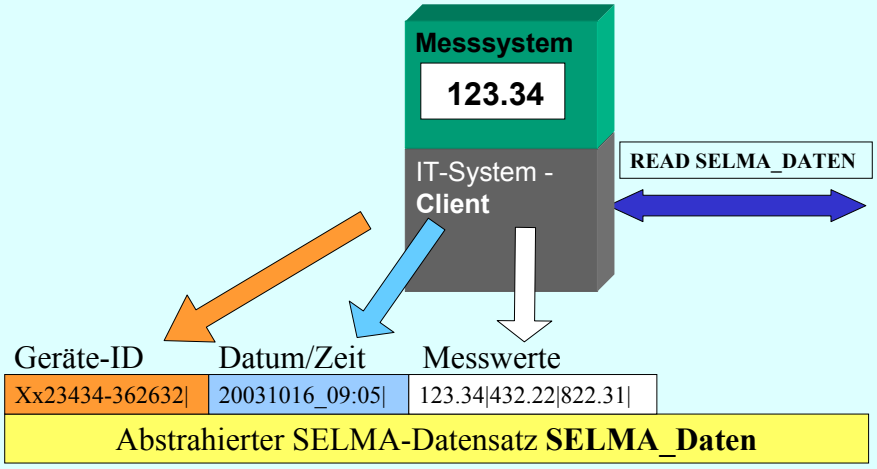
> Durch Setzen von Parametern können Dateien geschützt werden



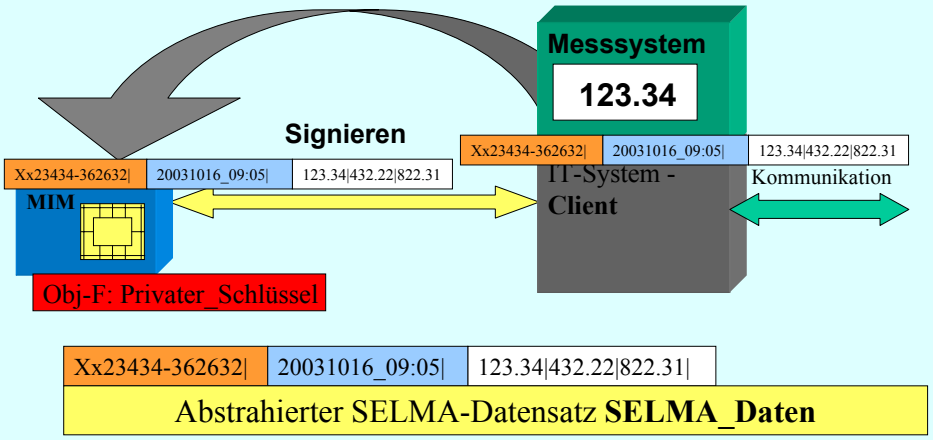
SELMA-Sicherheitsmodul - MIM
Funktion Generiere Schlüsselpaar



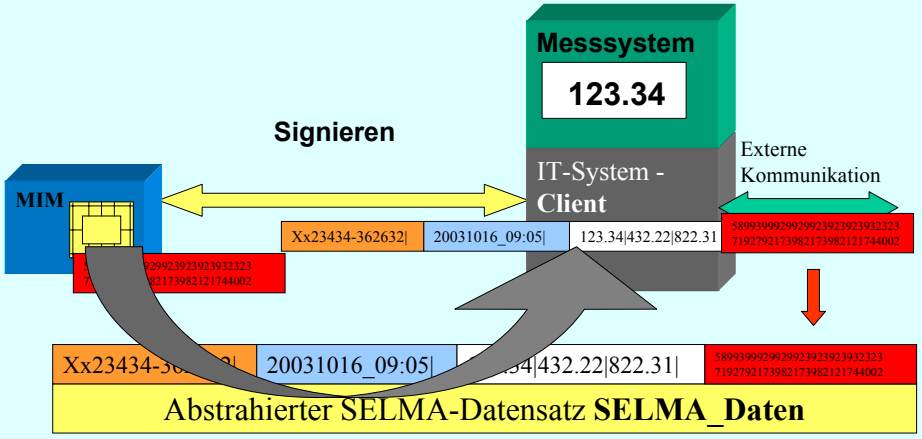
Signieren von Daten
Generieren von SELMA-Datensätzen



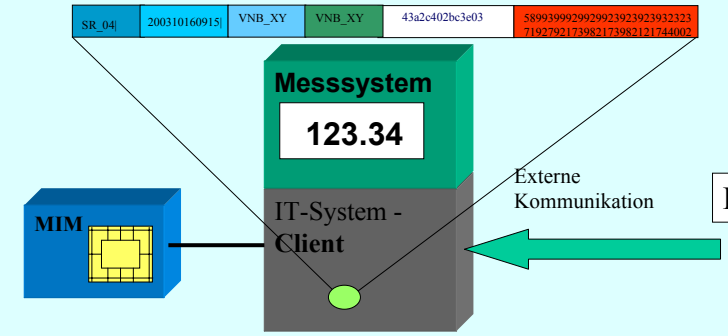
Signieren von Daten
Signatur berechnen



Signieren von Daten
Signatur übergeben



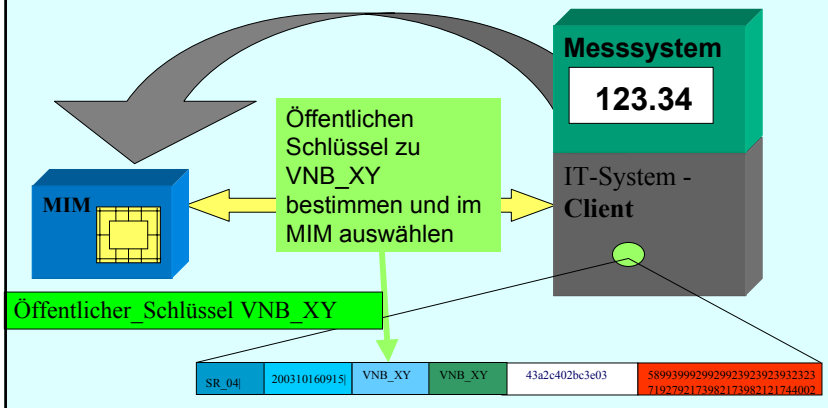
Verifizieren von Daten
Empfang des Datensatzes



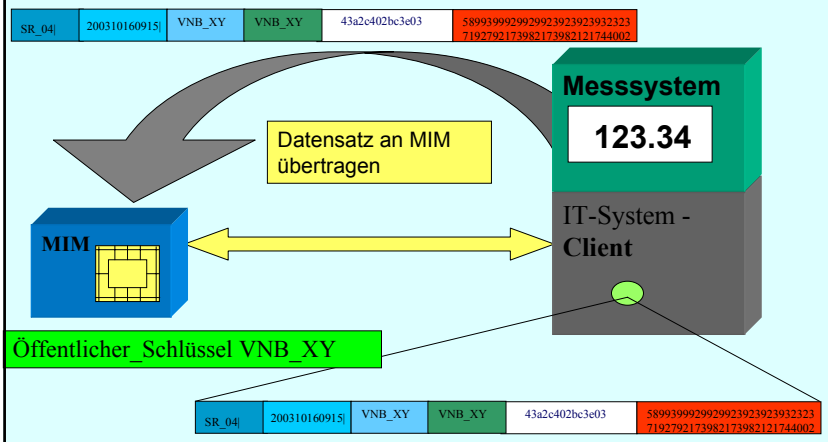
Request	Zeit $_{IT}$	Ident $_{IT}$	Ident $_{MG}$	Daten	Signatur
SR_04|	200310160915|	VNB_XY	VNB_XY	43a2c402bc3e03	589939992992992392392393232371927921739821739821217440002

Abstrahierter SELMA-Datensatz **SELMA_Anfrage**

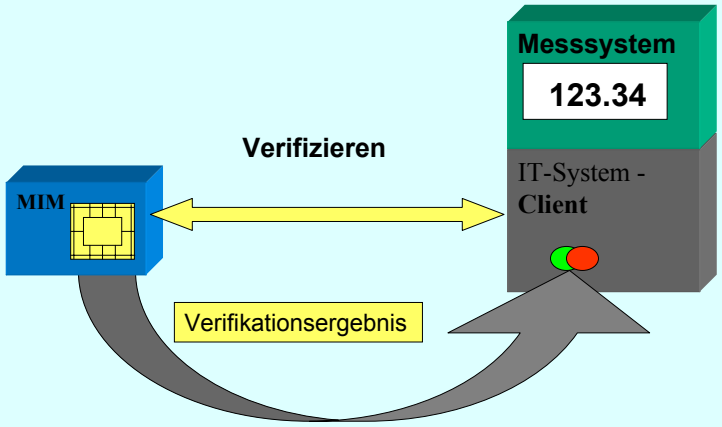
Verifizieren von Daten
Verifizieren des Datensatzes



Verifizieren von Daten
Verifizieren des Datensatzes



Verifizieren von Daten
Rückgabe der Verifikationsergebnis

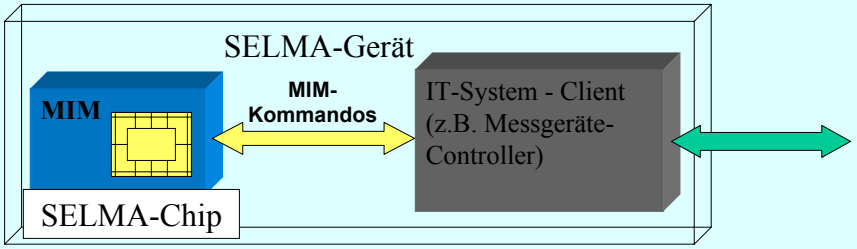


Weitere SELMA-Sicherheits-Funktionen

- Generiere neues Schlüsselpaar
- Führe Schlüsselwechsel durch
- Lesen von MIM-Parametern
- Lade zertifizierten öffentlichen Schlüssel

→ Die detaillierte Beschreibung dieser Funktionen erfolgt in den SELMA-Unterlagen

SELMA-Sicherheitsmodul - MIM Ausblick



Entwicklung eines speziellen SELMA-Kryptochips, der in der Lage ist, die SELMA-MIM-Kommandos zu verarbeiten

Vielen Dank für Ihre Aufmerksamkeit