www.selma-project.de

# SELMA-Prüfstellensoftware – Einsatz und Möglichkeiten

Norbert Zisky
Physikalisch-Technische Bundesanstalt



## Inhalt

- SELMA-Prüfungen - Gegenstand, Anforderungen, Prüfkriterien
- Prüfung der SELMA-Konformität
- SELMA-Prüfstelle
- SELMA-Prüfsoftware der PTB
- SELMA-Aufwand für Prüfungen
- Ausblick

## SELMA-Prüfungen - Gegenstand, Anforderungen, Prüfkriterien

Vielfältiger Einsatz der SELMA-Prüfsoftware

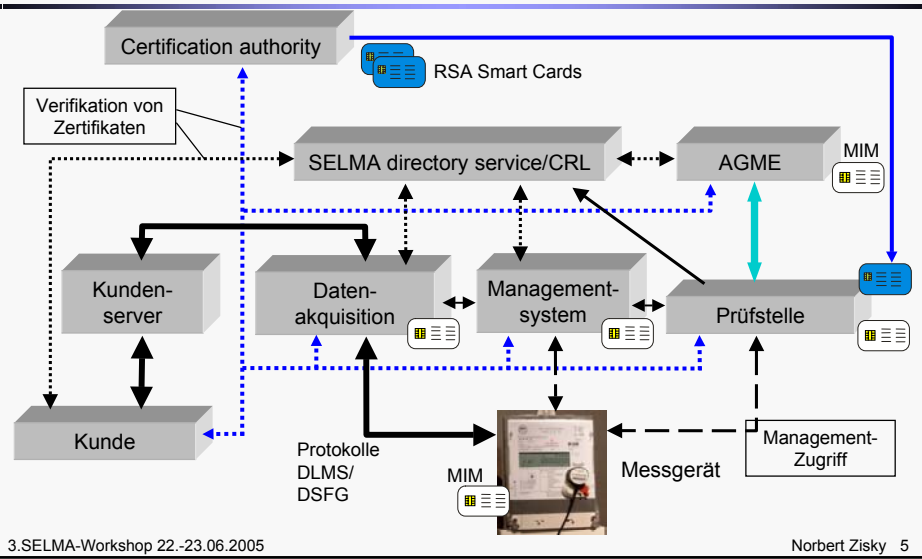
- Prüfung der SELMA-Konformität
- Bauart-Prüfung von SELMA-Geräten
- Prüf- und Managementvorgänge innerhalb einer Prüfstelle
- Prüf- und Managementvorgänge beim Messgerätebetreiber



## Prüfung der SELMA-Konformität

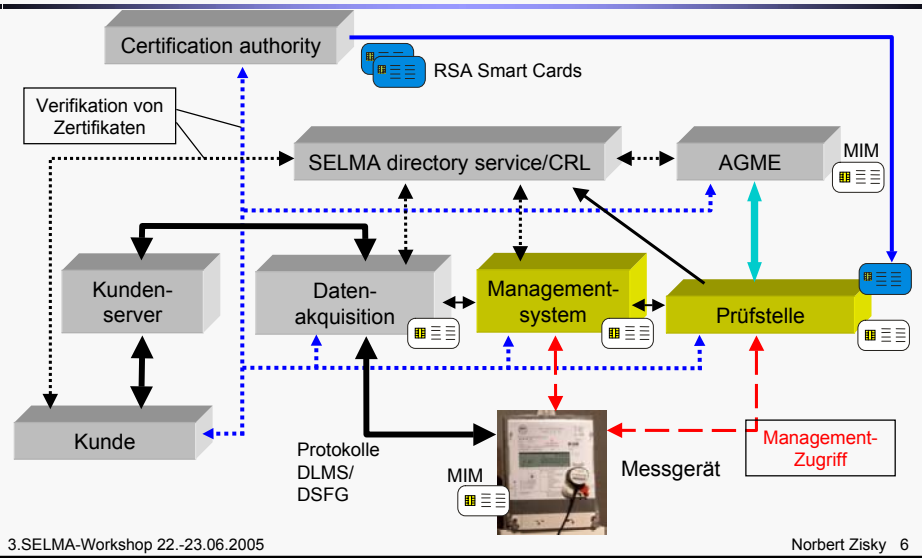
- SELMA-Sicherheitskonzept beschreibt Verfahren
- Untersetzung im SELMA-Datenmodell (Use Cases, Datenstrukturen, Klassenmodell)
  - Schutz von Datensätzen durch digitale Signaturen (SELMA-Grundfunktion)
  - Bidirektionaler Schutz des Kommunikationsweges (SELMA-Erweiterung - Option)
  - SELMA-Rechtemanagement und Logbücher (Download, Parametrierung)

# SELMA-Prüfumgebung



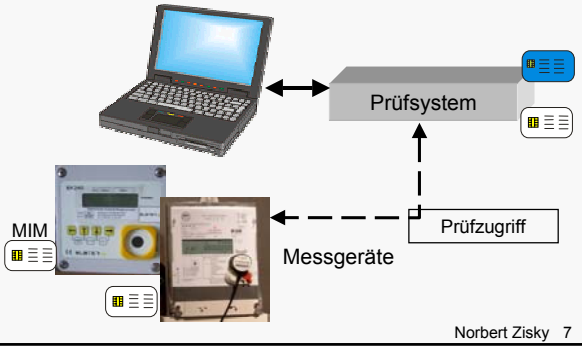



# SELMA-Prüfumgebung



# SELMA-Konformität

- Prüfziel: Nachweis der Erfüllung der Festlegungen entsprechend SELMA-Sicherheitskonzept und -Datenmodel
- Voraussetzung: Konformes Mapping auf Zielprotokoll






# SELMA-Konformität

**Prüfgegenstände**

- Signiereinheit zur Erzeugung der digitalen Signaturen
- Einfluss des Eichschalters im Zusammenhang mit SELMA-Funktionen
- Herstellerspezifische Funktionen mit Einfluss auf SELMA-Funktionen
- Zur Zeit 9 SELMA Interface Klassen Modelle im konkreten Mapping auf ein Standardprotokoll

  Beispiele
  - Tageslastgang - SDP
  - Ereignisgesteuerte Datenaufzeichnung - SCO
  - Meter Key Manager

# SELMA-Konformität

**Prüfung von Interface-Klassen (1)**

SELMA-Signierfunktion (SSF)

- SELMA-Basisfunktionen
  - SELMA-Schlüsselverwaltung - Meter Key Manager
  - Zugriffssteuerung - Access Agent
- Schutz von Datensätzen durch digitale Signaturen
  - Tageslastgänge - Signed Daily Profiles
  - Einfache Einzelmesswerte - Signed General Data
  - Ereignisgesteuerte Datenaufzeichnung - SCO



# SELMA-Konformität

**Prüfung von Interface-Klassen (2)**

Bidirektionaler Schutz Kommunikationsweg (SBSK)

- Verwaltung der Zugriffsrechte - Association Security Setup

SELMA-Rechtemanagement und Logbücher (SRM)

- Anzeige der Zugriffsrechte - Access Rights Viewer
- Metrologisches und Sicherheits - Management Logbuch

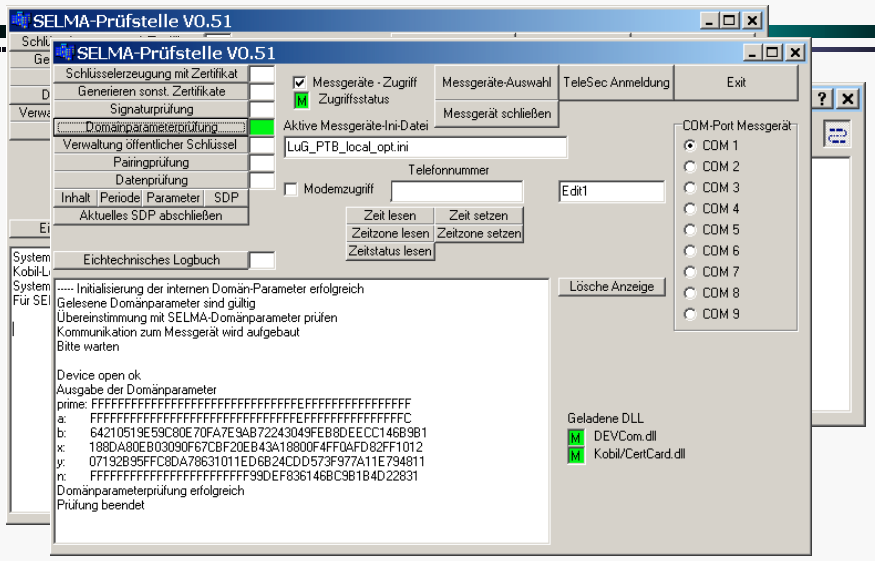
# SELMA-Konformität

- Prüfungen entsprechend SELMA-Sicherheitskonzept und -Datenmodell
- Prüfschritte sind Gegenstand des SELMA-Prüfkonzepts
- Prüfergebnis Prüfbericht

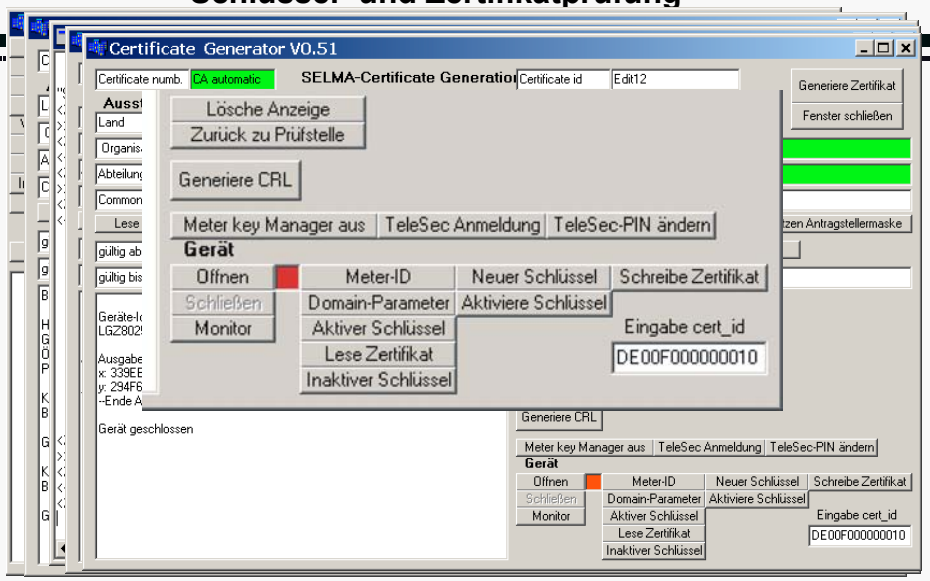


# PTB-SELMA-Prüfsoftware

## Messgeräteaufruf und Prüfschritte



# PTB-SELMA-Prüfsoftware
## Schlüssel- und Zertifikatprüfung






# SELMA-Konformität
Ergebnisse des Feldversuchs

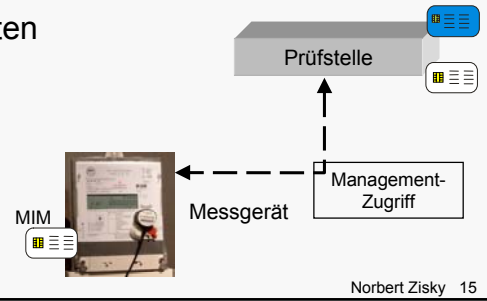
Es wurden insgesamt 5 Messgerätebauarten geprüft

- Elster, EMH, Görlitz, LuG, Wieser
- Alle Geräte haben SSF-Prüfung bestanden
- Wieser-Gerät hat SBSK „Bidirektionaler Schutz des Kommunikationswegs“ bestanden

- Für alle 5 Geräte kann im Prinzip ein positiver SELMA-Konformitäts-Prüfbericht ausgestellt werden und die Geräte sind berechtigt die Marke SELMA zu tragen

# SELMA-Prüfstelle

- Prüf- und Managementvorgänge innerhalb einer Prüfstelle entsprechend SELMA-Betriebskonzept
- SELMA-Aufwand ergibt sich aus der Anzahl implementierter SELMA-Funktionen
- Initialisierung der Prüfstelle
- Eichung von Messgeräten
- Befundprüfung
- Annahmeprüfung
- Stichprobenpüfung

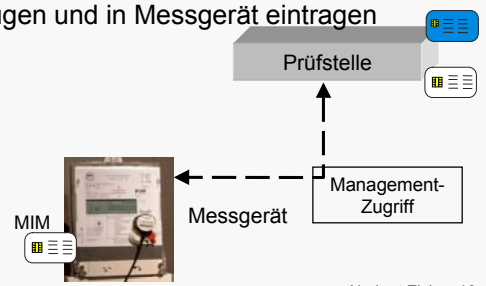





# SELMA-Prüfstelle

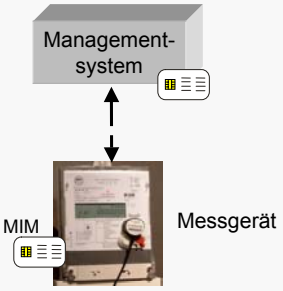
Ablauf während der Eichung

- 1a Prüfen der kryptographischen Parameter
- 1b Eintragen von SELMA-Prüfschlüsseln in das Messgerät
- 1c Messgeräte-ID lesen
- 1d Signierschlüssel erzeugen
- 1e Auslesen des öffentlichen Schlüssels des Messgerätes
- 1f SELMA-Zertifikat erzeugen und in Messgerät eintragen



# SELMA-Prüfungen durch VNB

- Prüf- und Managementvorgänge beim VNB entsprechend SELMA-Betriebskonzept
- Initialisierung des Messgeräts
- Zuweisung von Zugriffsrechten






# SELMA-Aufwand für Prüfungen

**Fehlerfreier Fall**

- SELMA-Konformitätsprüfung mit Prüfsoftware
  SSF 30 Minuten
  SBSK 30 Minuten
- SELMA-Prüfstelle (Handbetrieb)
  Schlüssel- und Zertifikate 10 Minuten
  Testfunktionen 10 Minuten

Anwenderschulung für Prüfstellenpersonal ist erforderlich

# Ausblick

- Weiterentwicklung der SELMA-Test- und Prüfverfahren entsprechend Entscheidungen des SELMA-AK
- Präzisierung und Konkretisierung der Prüfanforderungen
- Automatisierung der Prüfabläufe



# Weiterführende Literatur

www.selma-project.de

Informationstechnik
PTB-IT-11
Braunschweig und Berlin, Oktober 2004
Norbert Zisky (Hrsg.)
**Sichere Übertragung von Messdaten über offene Kommunikationsnetze**
Vorträge des 2. SELMA-Workshops, Berlin 2003

ISSN 0942-1785
ISBN 3-86509-234-9

**PTB-Bericht IT-12**

**Das SELMA-Projekt**
**Arbeitsberichte**
Norbert Zisky (Hrsg.)

ISSN 0942-1785
ISBN 3-86509-257-8

Geplanter Drucktermin März 2005