



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



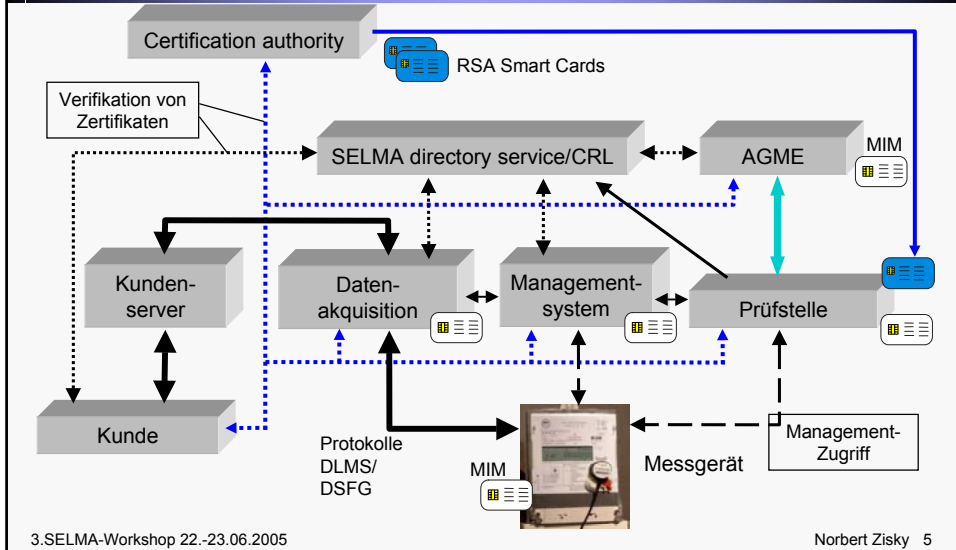
Vielfältiger Einsatz der SELMA-Prüfsoftware

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

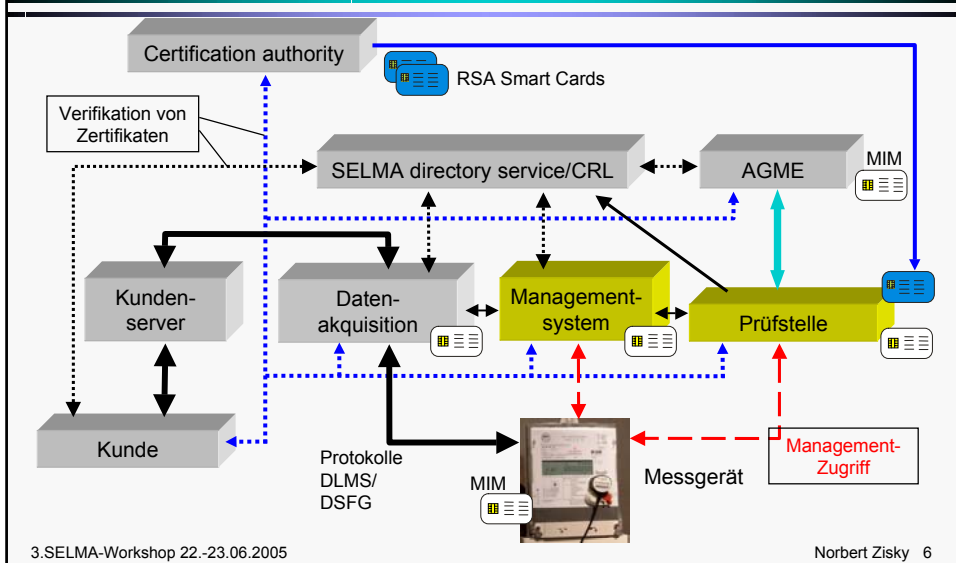
Prüfung der SELMA-Konformität

- 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)

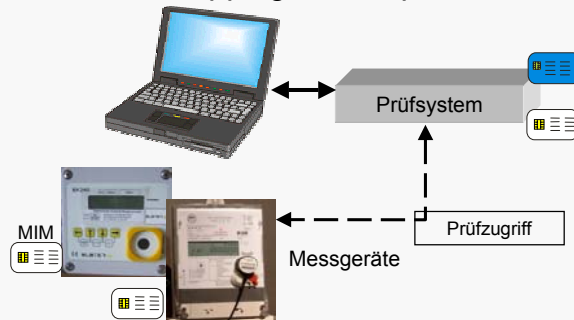
SELMA-Prüfumgebung



SELMA-Prüfumgebung



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



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-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

Bidirektionaler Schutz Kommunikationsweg (SBSK)

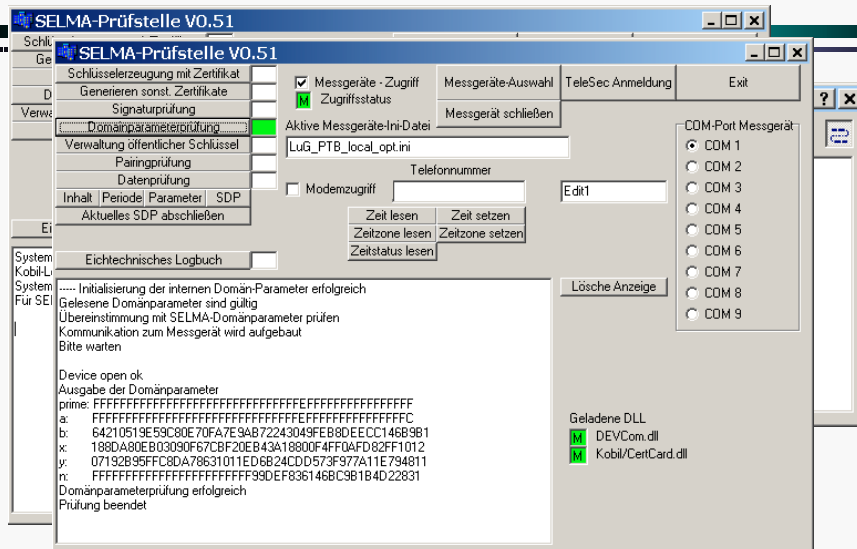
- Verwaltung der Zugriffsrechte - Association Security Setup

SELMA-Rechtemanagement und Logbücher (SRM)

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

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

PTB-SELMA-Prüfsoftware Messgeräteaufruf und Prüfschritte



SELMA-Prüfstelle V0.51

Schlüssel: Schlüsselzerzeugung mit Zertifikat, Generieren sonst. Zertifikate, Signaturprüfung, Domänparameterprüfung, Verwaltung öffentlicher Schlüssel, Pairingprüfung, Datenprüfung, Inhalt / Periode / Parameter / SDP, Aktuelles SDP abschließen, Eichtechnisches Logbuch

Ge: Messgeräte - Zugriff, Zugriffsstatus, Messgeräte-Auswahl, Messgerät schließen, TeleSec Anmeldung, Exit

Verwe: Aktive Messgeräte-Ini-Datei: LuG_PT_B_local_opt.ini, Telefonnummer, Modemzugriff, Edit1

Ei: Zeit lesen, Zeit setzen, Zeitzone lesen, Zeitzone setzen, Zeitstatus lesen

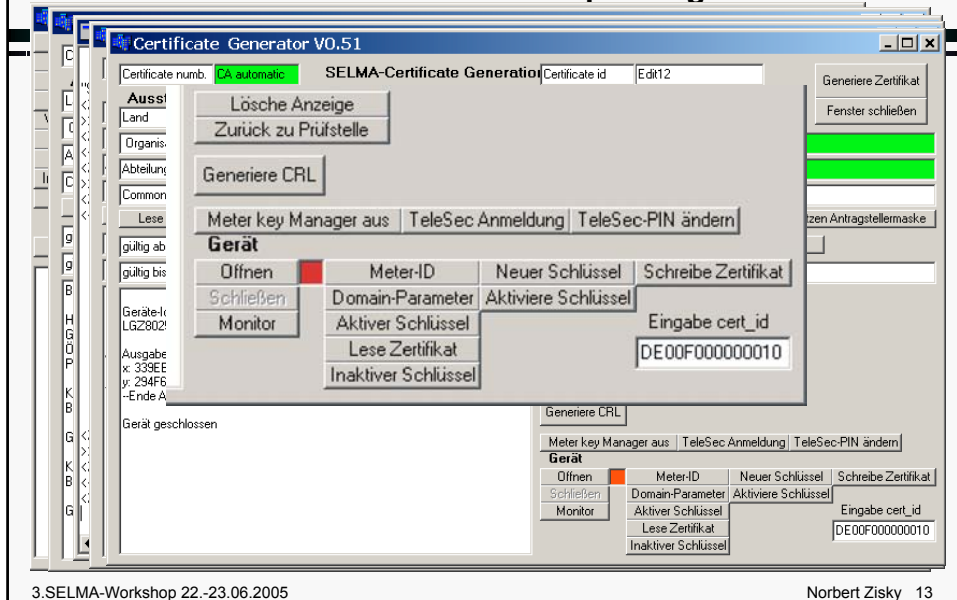
System: COM-Port Messgerät: COM 1, COM 2, COM 3, COM 4, COM 5, COM 6, COM 7, COM 8, COM 9

System: ----- Initialisierung der internen Domän-Parameter erfolgreich
Gelesene Domänparameter sind gültig
Übereinstimmung mit SELMA-Domänparameter prüfen
Kommunikation zum Messgerät wird aufgebaut
Bitte warten
Device open ok
Ausgabe der Domänparameter
prime: FF
a: FF
b: 64210519E59C80E70FA7E9AB72243049EB8DECC146B9B1
x: 188DA80EB03090F67CBF20EB43A18800F4FF04FD82FF1012
y: 07192B95FFC8DA78631011ED6824CDD573F977A11E794811
n: FFFFFFFFFFFFFFFFFFFFFFFFF99DEF836146BC9B1B4D22831
Domänparameterprüfung erfolgreich
Prüfung beendet

Llösche Anzeige

Geladene DLL: DEVCom.dll, Kobil/CertCard.dll

PTB-SELMA-Prüfsoftware Schlüssel- und Zertifikatprüfung



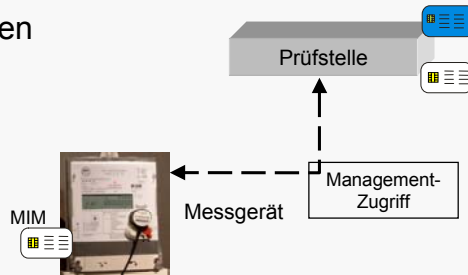
SELMA-Konformität Ergebnisse des Feldversuchs



- 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

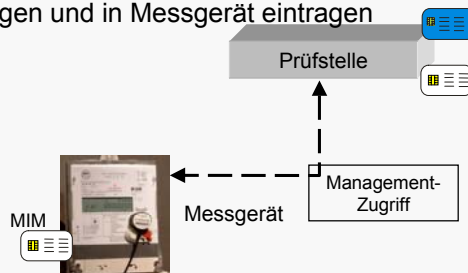
- Prüf- und Managementvorgänge innerhalb einer Prüfstelle entsprechend SELMA-Betriebskonzept
- SELMA-Aufwand ergibt sich aus der Anzahl implementierter SELMA-Funktionen
- Initialisierung der Prüfstelle
- Eichung von Messgeräten
- Befundprüfung
- Annahmeprüfung
- Stichprobenprüfung



SELMA-Prüfstelle

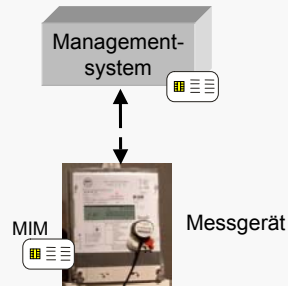
Ablauf während der Eichung

- 1a Prüfen der kryptographischen Parameter
- 1b Eintragen von SELMA-Prüfchlüsseln 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

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

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