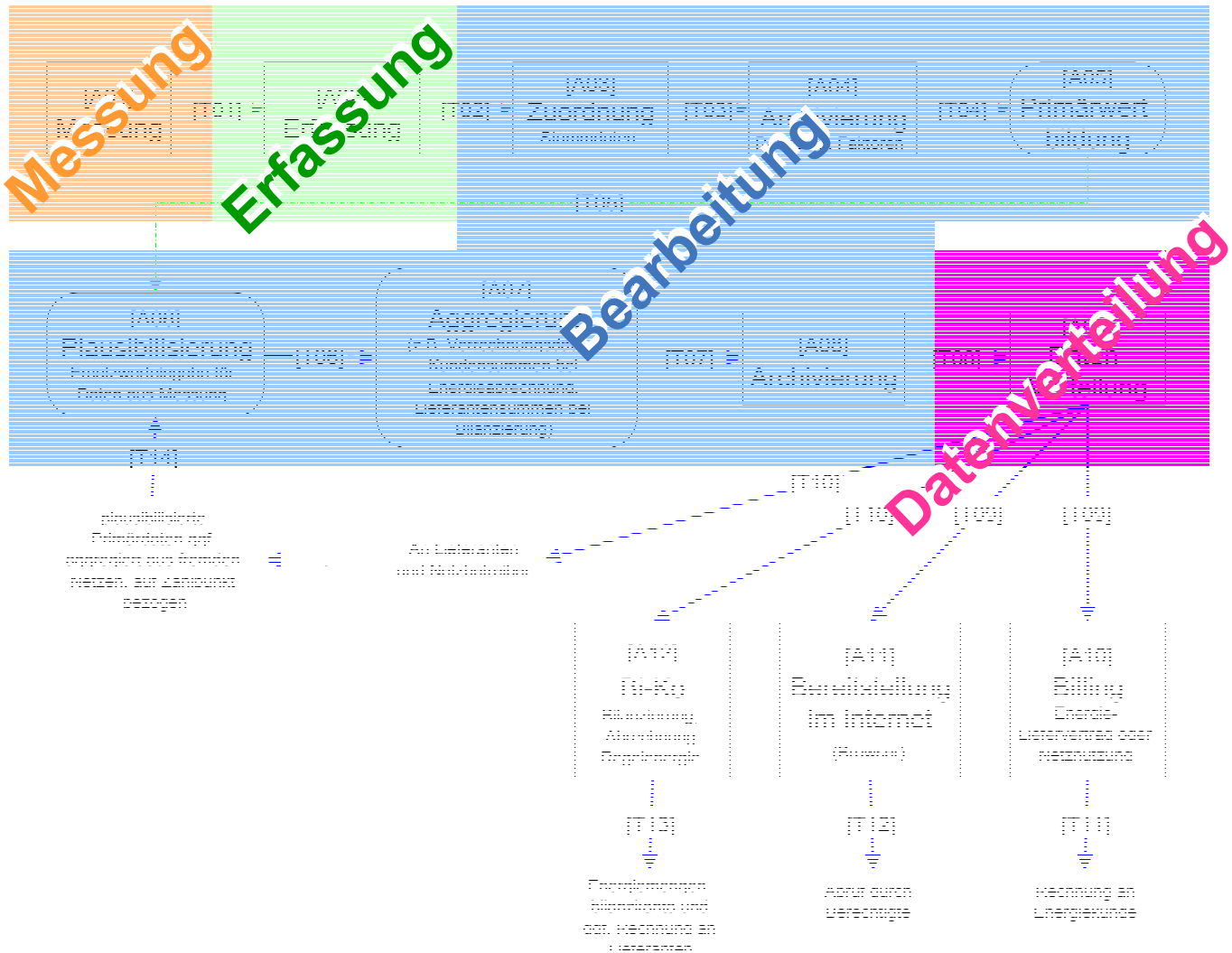
Systemkomponenten II

- Externe nach **Sig**G akreditierte **C**ertification **A**uthority **SigCA**
- Managementsysteme
  - Messgeräte-Management
  - Security-Management
  - Software-Management
- **S**ELMA **D**irectory **S**ervice **SDS**
- **C**ertificate **R**evocation **L**ist **CRL**

- SELMA-Messgeräte
- **M**eter **I**dentification **M**odule **MIM**

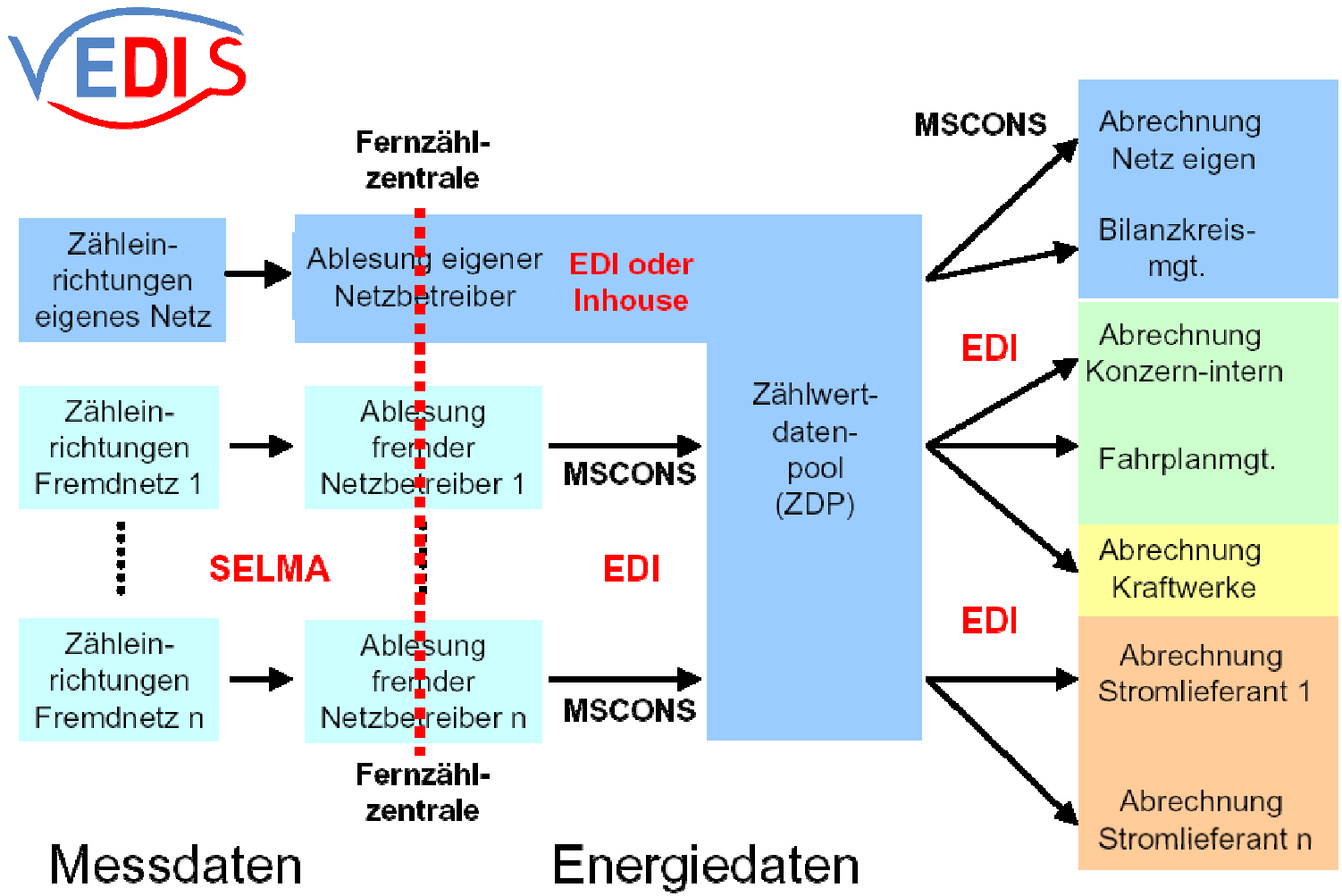
- **D**aten**a**quisitions**s**ystem **DAS**
- Web-Server
- **E**nergiedaten-**V**erfikations-**M**odul **EVM**

Datenfluss - Transaktionsmodell



Datenfluss – Transaktionsmodell

Abgrenzung SELMA / VEDIS



Sicherheitsverfahren
Verschlüsselung, Signatur

- ***häufig verwendete Algorithmen (Verschlüsselung, Signatur)***
  - data encryption standard ***DES*** zur Verschlüsselung, symmetrisches Verfahren
  - digital signature algorithm ***DAS*** wird als Bestandteil des digital signature standard DSS verwendet, asymmetrisches Verfahren zur Signatur
  - (Rivest, Shamir, Adleman) ***RSA*** asymmetrisches Verfahren zur Verschlüsselung und zur Signatur
  - elliptische Kurven ***EC***, z.B. ECDSA, ECGDSA, ECKDSA kleine Schlüssellängen!

Sicherheitsverfahren
Verschlüsselung, Signatur

- ***Einwegfunktionen***
  - Mathematische Funktionen für kryptographische Verfahren mit öffentlichen Schlüsseln (asymmetrischer Kryptographie) - lassen sich relativ einfach berechnen, die Umkehrung ist aber erheblich schwieriger.

Potenzieren ist einfacher als Wurzel ziehen!

Sicherheitsverfahren

- ***Hashfunktionen***
  - Kompressionsfunktionen, Kontraktionsfunktion, Message-Digest, Fingerabdruck, kryptographische Prüfsumme, ...
  - Die Hashfunktion berechnet aus einem Eingabe-String variabler Länge einen Ausgabe-String fester Länge (Hashwert).
  - Bekannte Hasfunktionen:
    secure hash algorithm ***SHA-1***, 160 bit langer hash Wert
    RIPEMD im Rahmen des Projekts RIPE der EU entwickelt,
    128 bit langer hash Wert

Sicherheitsverfahren
Standards

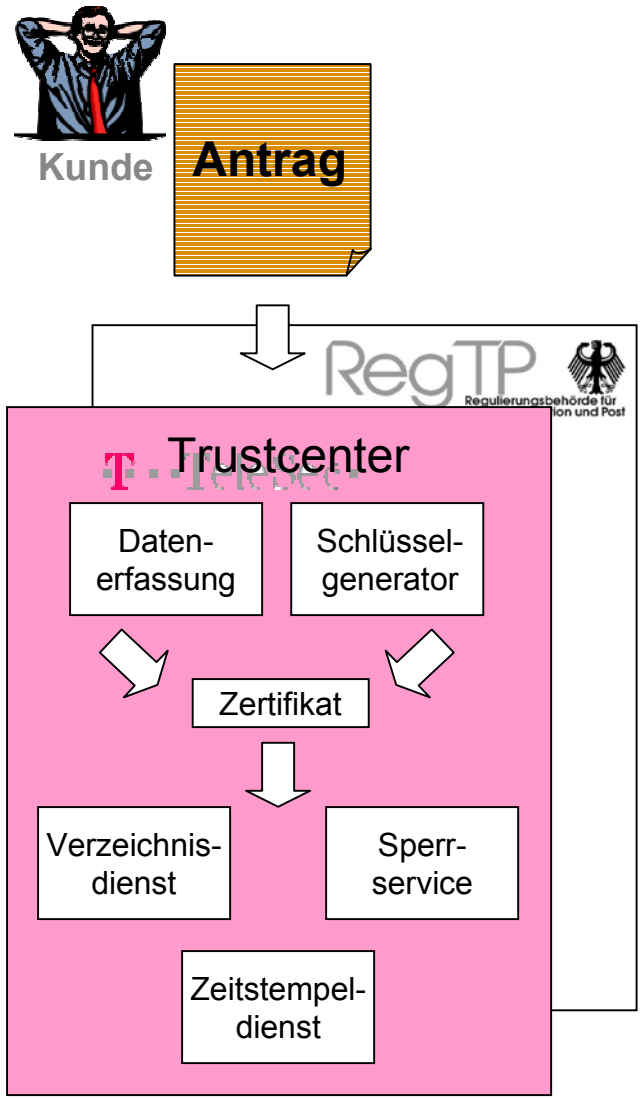
- ***common criteria*** for Information Technology Security Evaluation (1998, internationaler Standard)
- ***ITSec*** Kriterien für die Bewertung der Sicherheit von Systemen der Informationstechnik (1991, Deutschland)

Common critera	ITSec
EAL4	E3
EAL 3+	E2

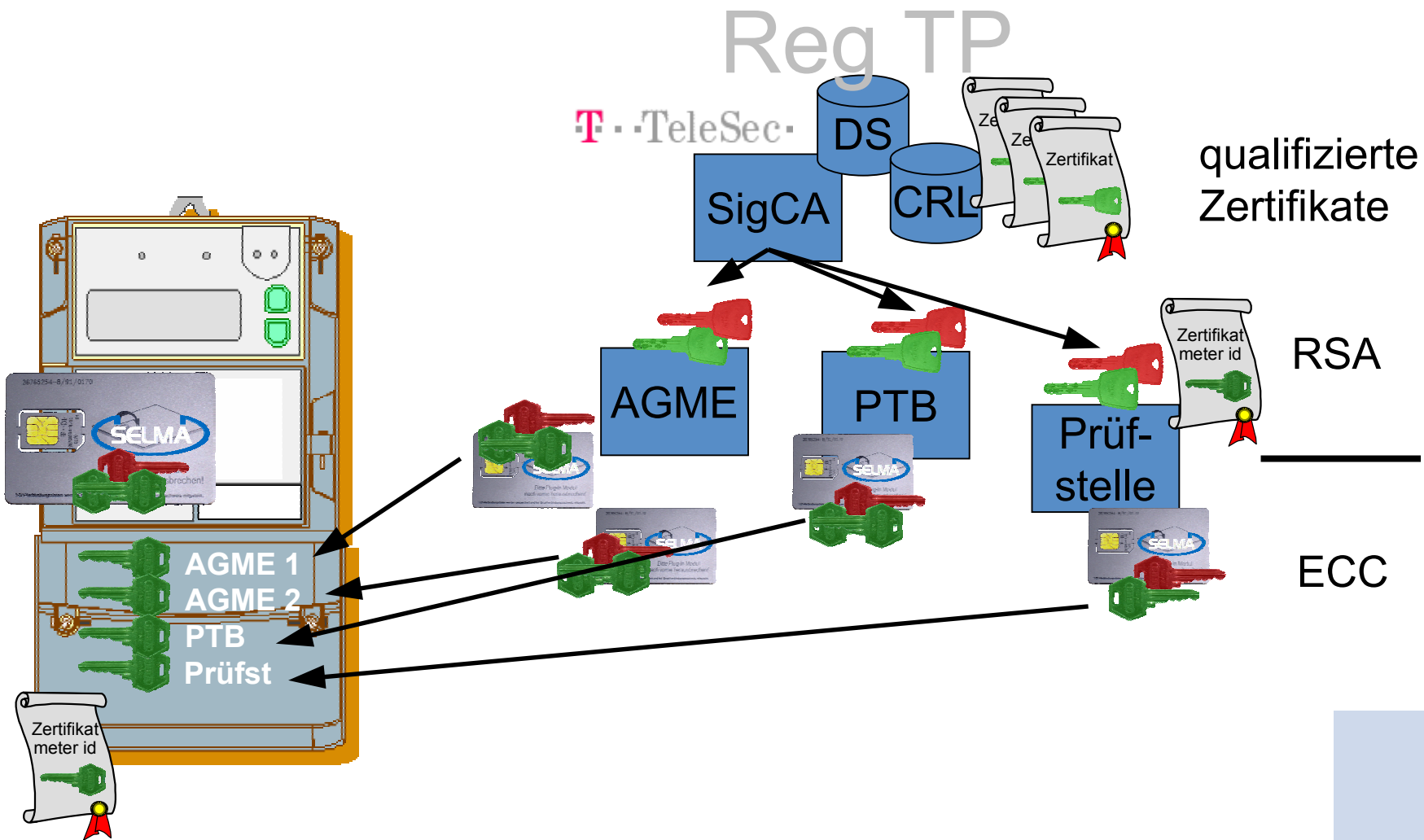
Sicherheitsverfahren

PKI

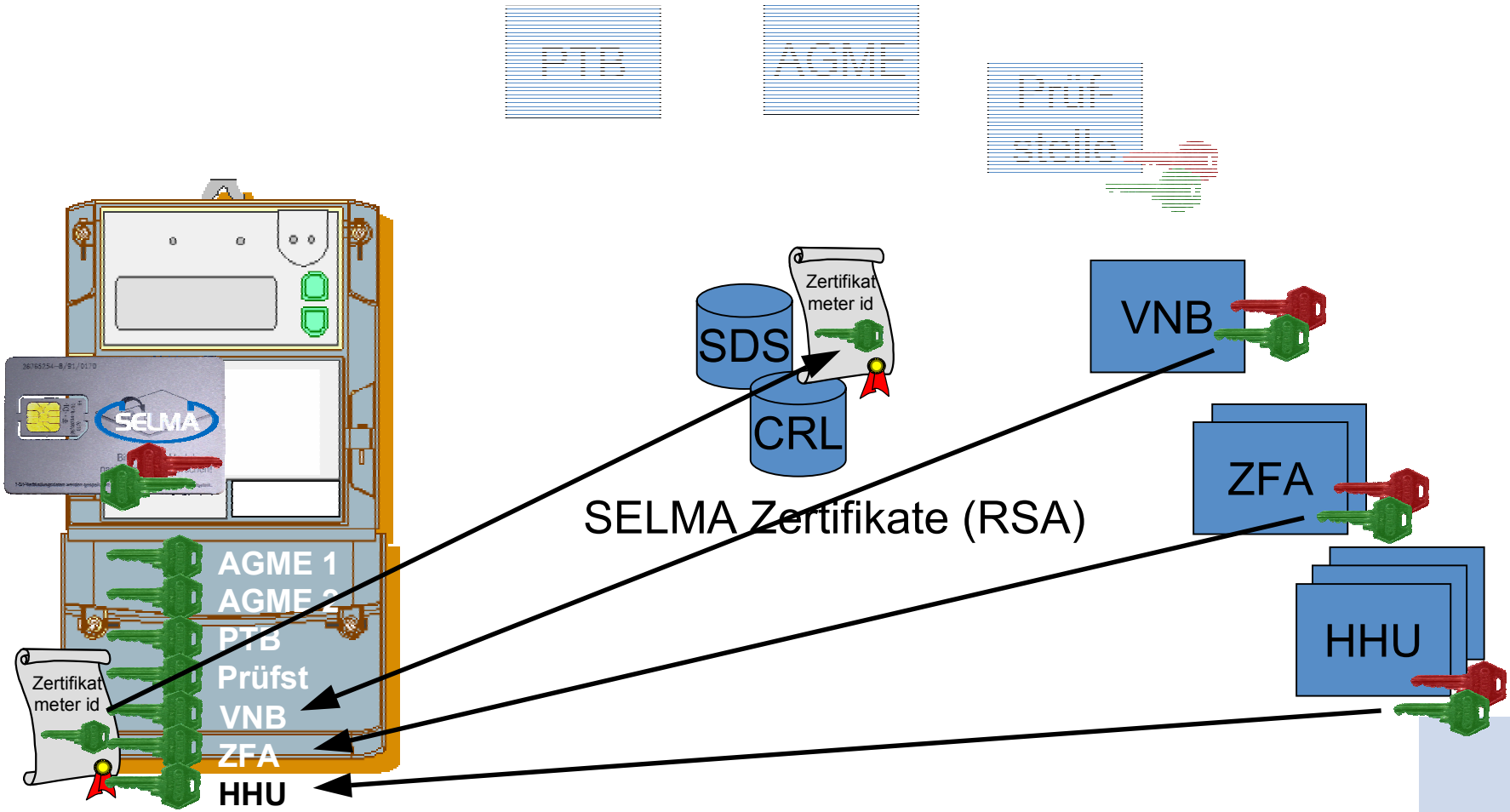
Public Key Infrastructure



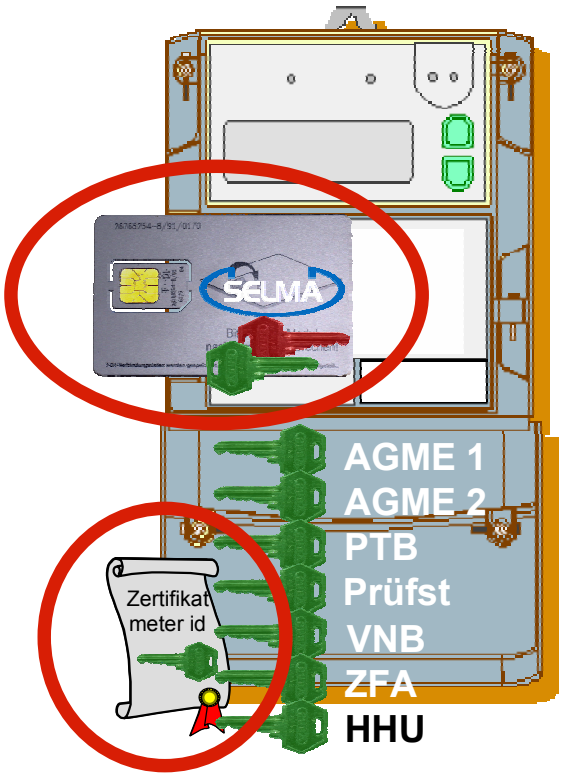
Schlüsselmanagement I



Schlüsselmanagement II



Schlüsselmanagement III



Übertragungsprotokolle

Elektrizität

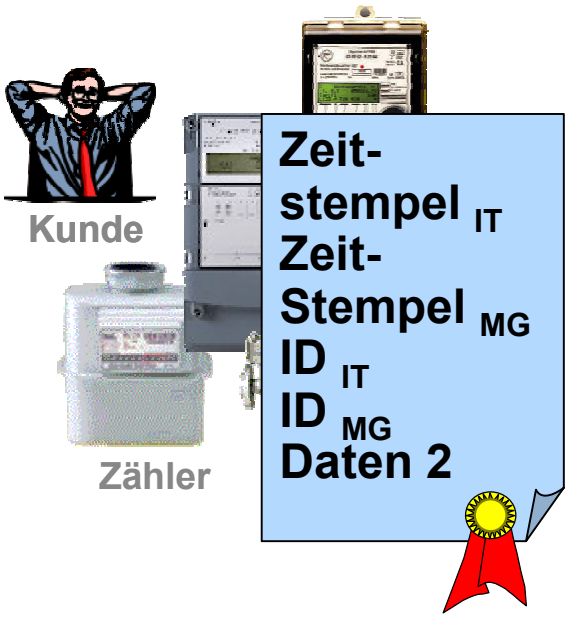
- EN62056-21 (IEC1107)
- DLMS ***Realisierung im Rahmen des Projektes!***

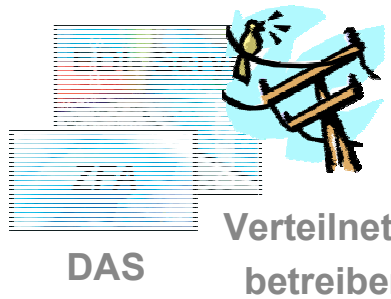
Gas

- DSFG ***Realisierung im Rahmen des Projektes!***

Übertragungsprotokolle

Kommunikationsablauf, gesicherte Kanäle





Übertragungsprotokolle / Datenmodell
signed dailyprofile SDP

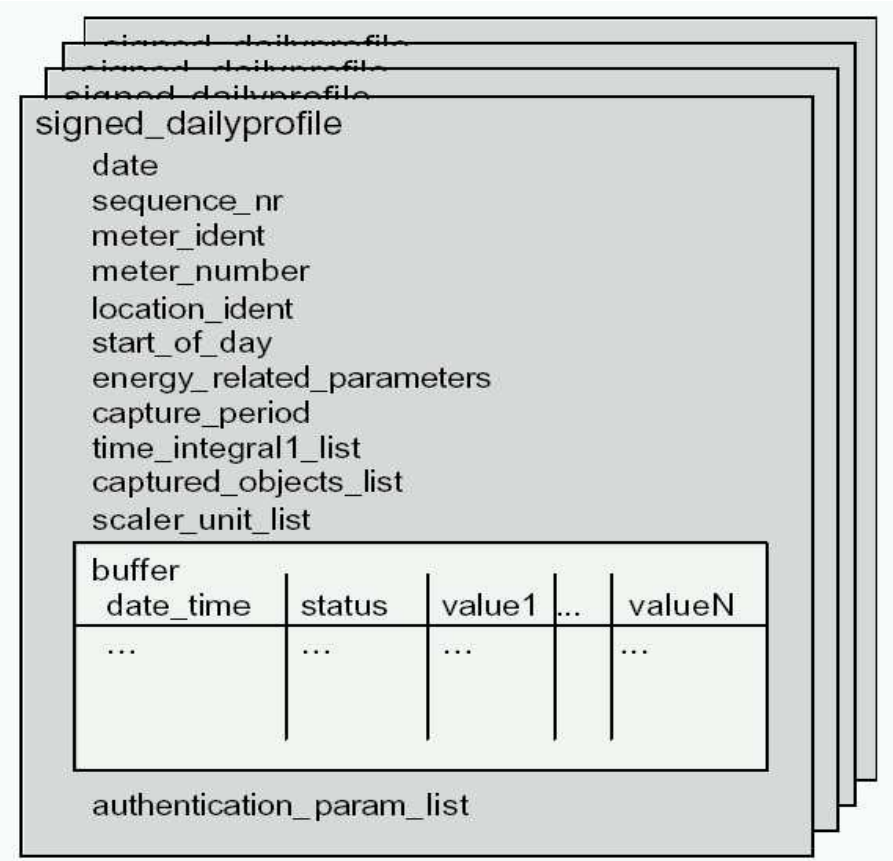


Abbildung 5: IC Signed Daily Profiles

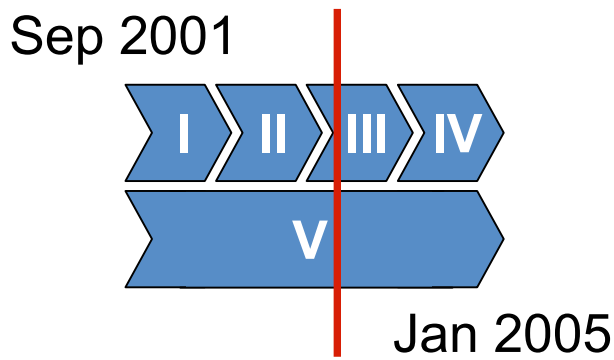
aktueller Projektstand

Phase III Funktionsmodellentwicklung

- Pflichtenhefte der Geräte- und Leitstellenhersteller sind abgenommen
- MIM, Initialisierung, Interface (Makrobefehle)

- Vorbereitung Feldversuch
- Funktionsumfang

- SELMA Dienstgüte
- Messgeräte mit / ohne Uhr



Zusammenfassung

- Projektziel
- Konsortium
- Zeitplan
- Projektphasen / Dokumente
- Systemkomponenten
- Datenfluss / Transaktionsmodell
- Sicherheitsverfahren
- Schlüsselmanagement
- Übertragungsprotokolle
- aktueller Projektstand

Messgeräte mit Qualitätssiegel

Vielen Dank für Ihre Aufmerksamkeit

Andreas Wolff
RWE Rhein-Ruhr Netzservice GmbH
Zählermanagement