Ein Sicherheitskonzept für Messgeräte im liberalisierten Energiemarkt

Univ.-Prof. Dr. Christoph Ruland

SELMA Workshop 2003

Berlin, 15. Oktober 2003

Liberalisierter Energiemarkt

- Vorher: nur Energieabnehmer
- Jetzt: Energiekunde
- Jeder soll Energie kaufen und verkaufen können
- Trennung von Erzeugung, Vertrieb/Handel, Transport/Verteilung
- Kunde wählt Lieferanten aus, (Verteil-) Netzbetreiber ist fest
- Häufiges Auslesen der Energiezähler erforderlich

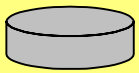
Transaktionsmodell

Messung

Datenakquisition

Zuordnung

Archivierung



Primärwertbildung

Plausibilisierung

Aggregierung

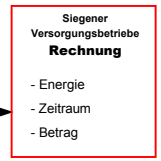
Archivierung

Verteilung

Billing

Bereitstellung im Internet

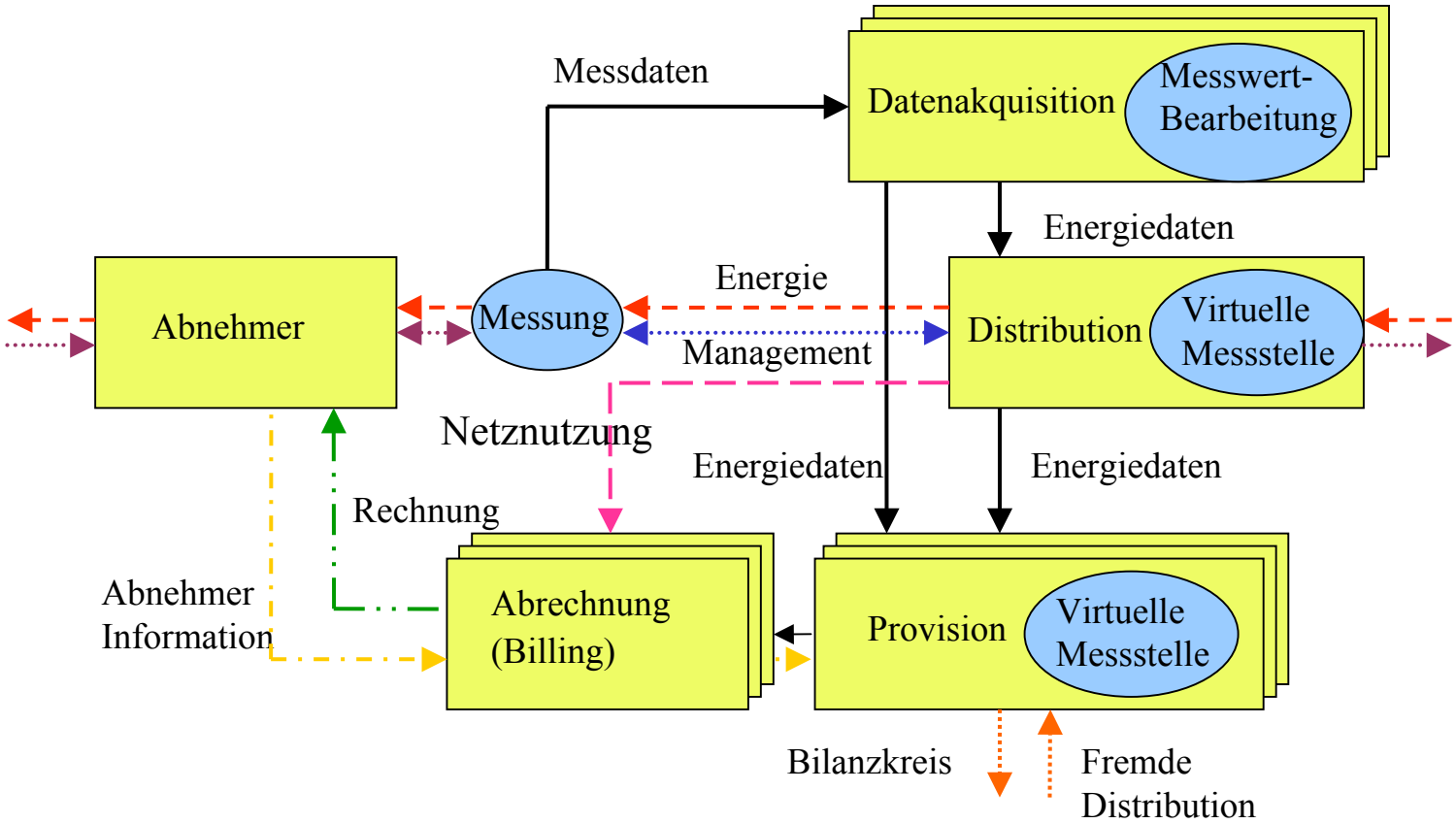
Bilanz-Koodinator



Rechnung an Energiekunden

Abruf durch Berechtigte

Rollen der Marktteilnehmer



Sicherheitsanalyse für Messgeräte

Aktive Angriffe (Auswahl)

- Modifikationen beim Kunden oder während der Übertragung
- Maskerade als anderer Systemteilnehmer
- Leugnen der Messwerte
- Neu: Angriffe von Koalitionen, z.B.
  - **Koalition von Abnehmer und Daten-Akquisitionsstelle**

    Die Daten-Akquisitionsstelle verändert die gemessenen Daten (Messwert oder Uhrzeit) so, dass ein Abnehmer auf Kosten anderer Energie bezieht
  - **Koalition von zwei Abnehmern**

    Ein Abnehmer wählt einen günstigen Tagtarif, ein anderer einen günstigen Nachttarif. Durch Austausch der Messgeräte wird Tag und Nacht Energie zum günstigen Tarif bezogen
- Nicht-autorisierter Managementzugriff

Erforderliche Sicherheitsdienste

- Vertraulichkeit
  - personenbezogene Daten
- Gewährleistung der Datenunversehrtheit
  - Messdaten, Managementdaten
- Verfügbarkeit
  - Messdaten, Abrechnungsdaten
- Authentikation des Ursprungs der Daten
  - Messdaten, Kommandos, Abrechnungsdaten
- Zugangs- und Zugriffskontrolle
  - Datenzugriff, Managementzugriff
- Nicht-Abstreitbarkeit
  - Messwerte, Quittungen

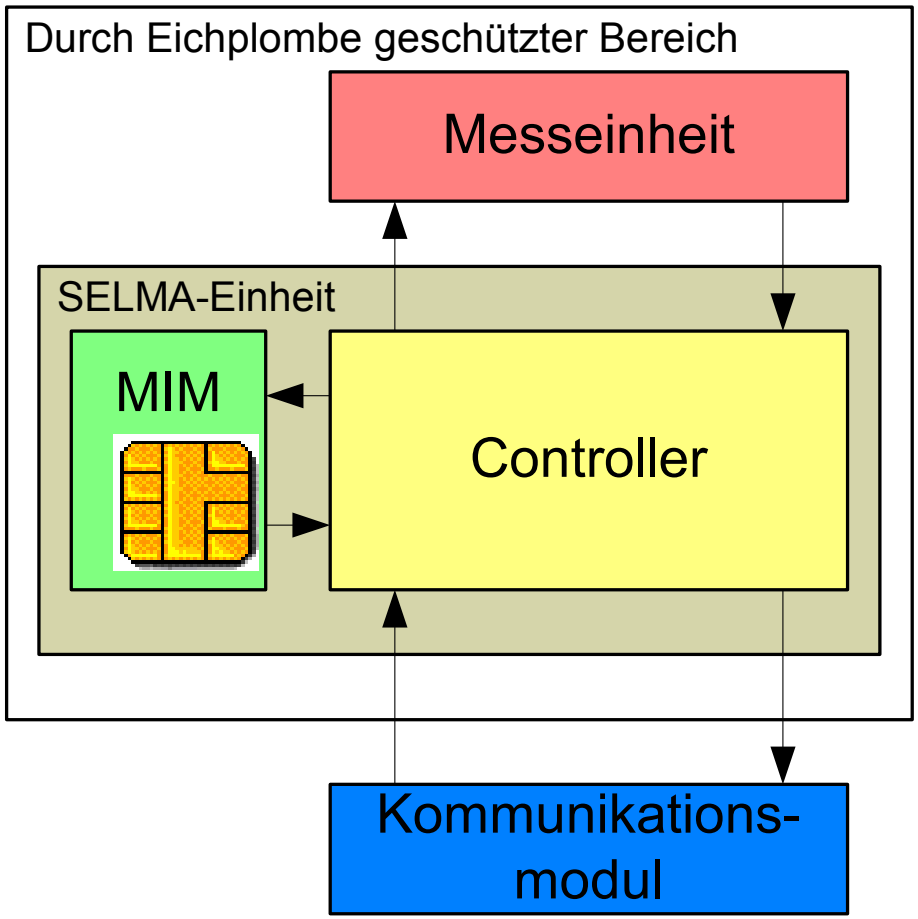
Anforderungen an das Sicherheitskonzept

- Digitale Signaturen der Messwerte sollen technisch *qualifizierten Signaturen* (SigG) entsprechen
- Erweiterungen der Messdatensätze um digitale Signaturen, zeitvariante Parameter, zusätzliche Identifikationen, etc.
- End-to-End Authentikation des Ursprungs der Messwerte von der Generierung bis zur Abrechnung
- Verifikation der Messwerte muss jedem Marktteilnehmer möglich sein
- Transportgebundene Vertraulichkeit bei Übertragung personenbezogener oder sensibler Daten

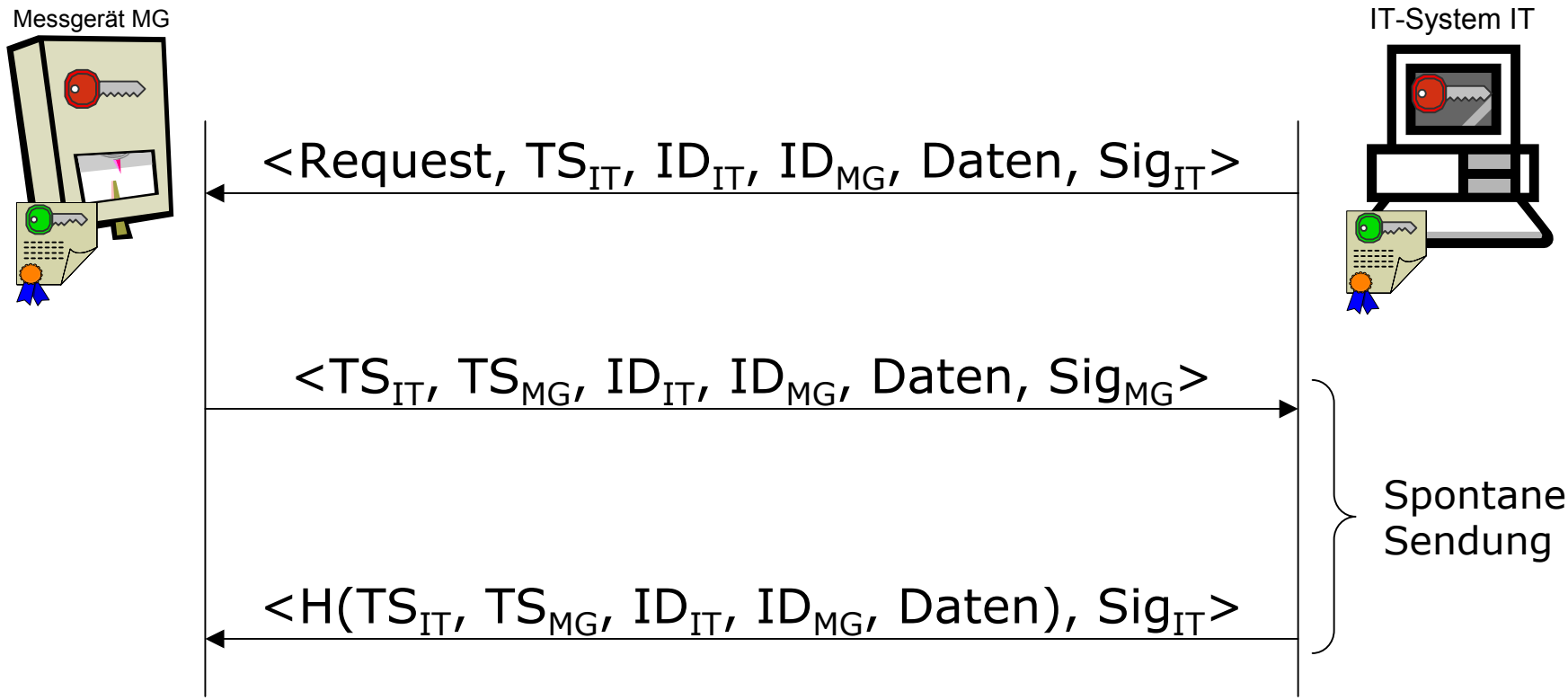
Sicherheitskonzept

- Messgeräte werden um „Signaturerstellungseinheit“ (MIM) erweitert
- Alle Anfragen an das Messgerät werden signiert und über das Rechtemanagement geprüft
- Alle Nachrichten vom Messgerät werden von der MIM signiert
- Jede MIM generiert ihr eigenes Schlüsselsystem
- Messgeräte nutzen Elliptische Kurvenkryptographie (ECC)
- Ein zugelassener Zertifikatsdiensteanbieter (ZDA) liefert RSA-Schlüsselsysteme für die Prüfbehörden (Eichstellen)
- Prüfbehörden zertifizieren die öffentlichen Schlüssel der Messgeräte mit *qualifizierten Signaturen* (SELMA-Zertifikat)

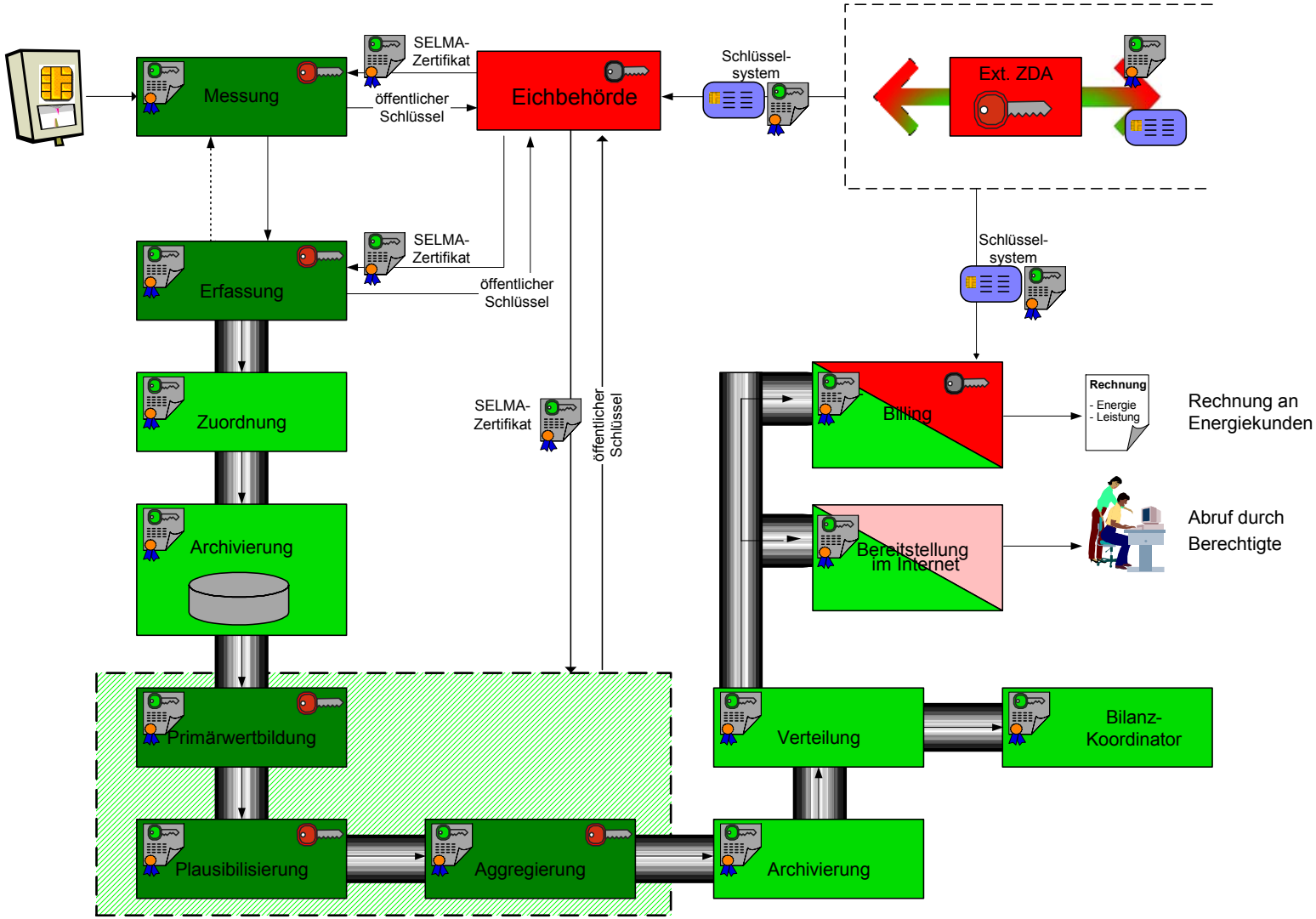
Signaturerstellungseinheit



Signierte Protokolldateneinheiten



Hybridsystem ECC/RSA



Erläuterung zum Hybridsystem ECC/RSA

- Der Zertifizierungsdiensteanbieter (ZDA) erstellt Zertifikate über öffentliche RSA-Schlüssel der Prüfstellen, die mit dem RSA-Verfahren signiert sind
- Die Prüfstellen stellen SELMA-Zertifikate aus, die öffentliche ECC-Schlüssel enthalten und mit einem RSA-Schlüssel signiert sind (s.o.)
- Die Messgeräte, Erfassungsstellen und Systeme, die Messwerte bilden, enthalten eine Signaturerstellungseinheit, z.B. MIM, generieren ECC-Schlüsselsysteme, signieren und verifizieren mit dem ECC-Verfahren. Alle anderen Stellen verifizieren nur mit dem ECC-Verfahren
- Die Rechnungsstelle (Billing) signiert Datensätze, die im Internet hinterlegt werden, mit dem RSA-Verfahren. Alle befugten Internet-Teilnehmer, die auf diese Datensätze zugreifen, verifizieren diese RSA-Signaturen

Schlüssel im SELMA-Messgerät

aktives Schlüsselpaar: Pri_{akt} | Pub_{akt}

inaktives Schlüsselpaar: Pri_{inakt} | Pub_{inakt}

Master

Master-Backup

0	AGME (DN, Pub_{AGME0})	1
1	AGME (DN, Pub_{AGME1})	0
2	PTB (DN, Pub_{PTB})	0,1
3	Prüfstelle #1 (DN, Pub_{PS1})	0,1
4	Prüfstelle #2 (DN, Pub_{PS2})	0,1
5	VNB (DN, Pub_{VNB})	3,4

Struktur fest vorgegeben

Schlüssel-position

M-Zertifikat überprüfen mit öffentlichem Schlüssel auf Position ...

Schlüsselhierarchie im Messgerät

- Zwei Signatur-Schlüsselsysteme (ein aktives, ein inaktives), generiert im Messgerät
- Zwei öffentliche Schlüssel der AGME (Arbeitsgemeinschaft Mess- und Eichwesen)
- Zwei öffentliche Schlüssel von zugelassenen Prüfstellen, zertifiziert durch die AGME. Der VNB (Verteilnetzbetreiber) wählt selbst seine Prüfstellen aus.
- Öffentlicher Schlüssel des VNB, zertifiziert durch eine der eingetragenen Prüfstellen
- Öffentliche Schlüssel der Datenerfassungsstellen, zertifiziert durch eine der eingetragenen Prüfstellen, eingetragen durch den VNB
- Öffentliche Schlüssel der Managementsysteme, zertifiziert durch eine der eingetragenen Prüfstellen, eingetragen durch den VNB

Initialisierung der SELMA-Messgeräte

Lade AGME-Schlüssel

Lade Prüfstellen-Schlüssel

Generiere initiales Schlüsselpaar

Öffentlicher Schlüssel

SELMA-Zertifikat

Laden weiterer öffentl. Schlüssel

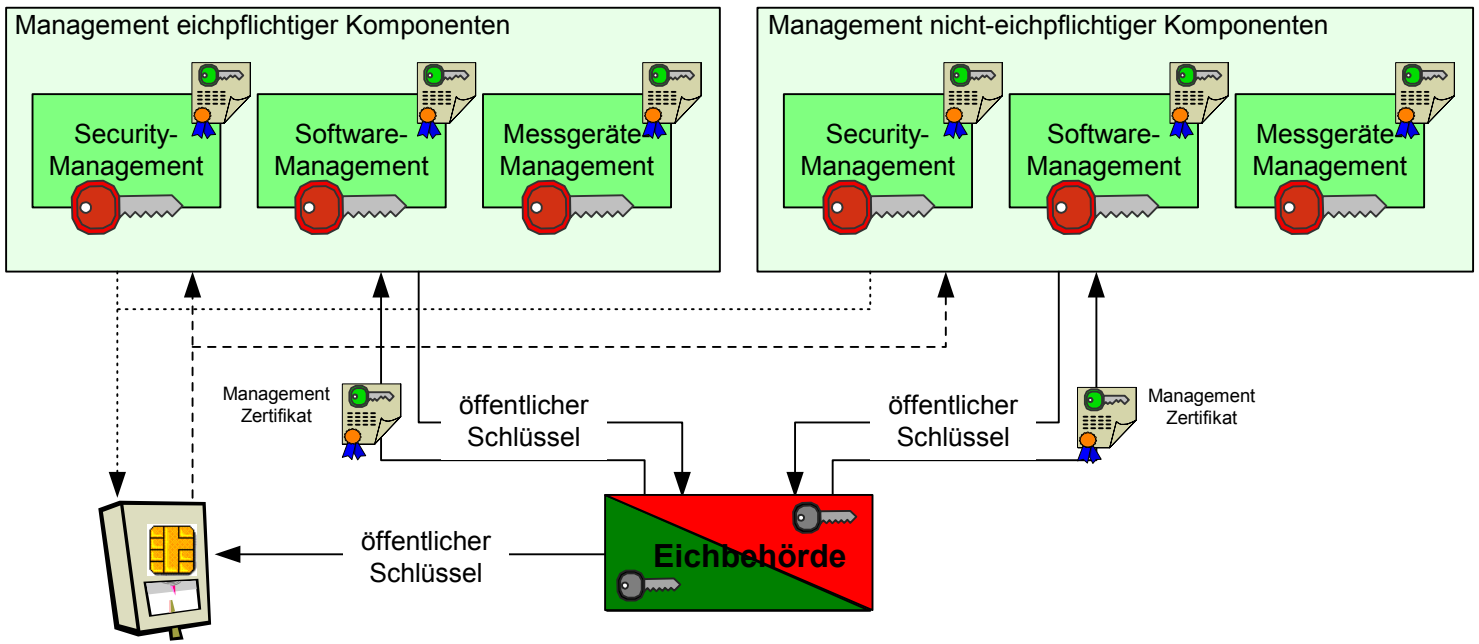
Setzen von Zugriffsrechten

Eichbehörde

Prüfstelle

Management-Systeme

- M-(Management)-Zertifikate beinhalten öffentliche ECC-Schlüssel der zugreifenden Instanzen und wurden von Prüfstellen mit dem ECC-Verfahren signiert
- M-Zertifikate können von Messgeräten verifiziert werden



Zusammenfassung

- Die Messgeräte und alle Instanzen, die Messwerte produzieren, werden um eine MIM erweitert. Die MIM erstellt Signaturen, die dem Niveau von qualifizierten Signaturen nach dem Signaturgesetz entsprechen
- Alle Protokolleinheiten, die zwischen Messgerät und Datenerfassungsstelle oder Managementsystemen ausgetauscht werden, enthalten Zeitstempel und Signaturen
- Intern arbeitet SELMA mit ECC-Verfahren, nach außen hin mit dem RSA-Verfahren
- Bei der Eichung generiert das Messgerät sein Schlüssel-system, und die öffentlichen Schlüssel der AGME werden geladen
- Alle weiteren Initialisierungsschritte können online erfolgen

Ergebnis

- Das Sicherheitskonzept erfüllt alle Anforderungen der Sicherheitsanalyse und betroffenen Interessensgruppen
- Das Sicherheitssystem benötigt nur wenige Zertifikate eines zugelassenen ZDA, arbeitet sonst autonom
- Es gibt eine Schlüsselhierarchie, die ein flexibles, dynamisches und online Schlüssel- und Rechtemanagement erlauben

Mit diesem Sicherheitskonzept sind die Messgeräte für den liberalisierten Energiemarkt gerüstet