Übersicht

1 Rückblick
2 Ausblick

martin.kahmann@ptb.de

...wie alles anfing

Marktteilnehmer. Die bislang unbeantwortete Frage, wie die relativ großen Lastgang-Datenmengen authentisch und unverfälscht ökonomisch vom Zähler über offene Netze übertragen werden können, ist ein wesentlicher Hemmschuh für eine breite Markteinführung entsprechender Technik. Die Aussicht auf den Gewinn einer VERNET-Förderung wäre m.E. geeignet, alle Betroffenen (Hersteller, Anwender, Behörden) zur Bildung einer Interessengemeinschaft zu motivieren, deren Ziel z.B. wie folgt für den Wettbewerb formuliert werden könnte:

31.07.2000

Transformation des Konzeptes der gesetzeskonformen Digitalen Signatur auf das Problem der sicheren Übertragung geldwertiger Energiemesswerte

Entwicklung technischer und organisatorischer Voraussetzungen zur Sicherung der Verfügbarkeit, Vertraulichkeit, Unversehrtheit und Verbindlichkeit über offene Netze übertragener Speicherinhalte von Elektrizitätszählern

Externe Interessenten könnten z.B. sein: ZVEI, VDEW, BSI. Sollte die Bildung einer

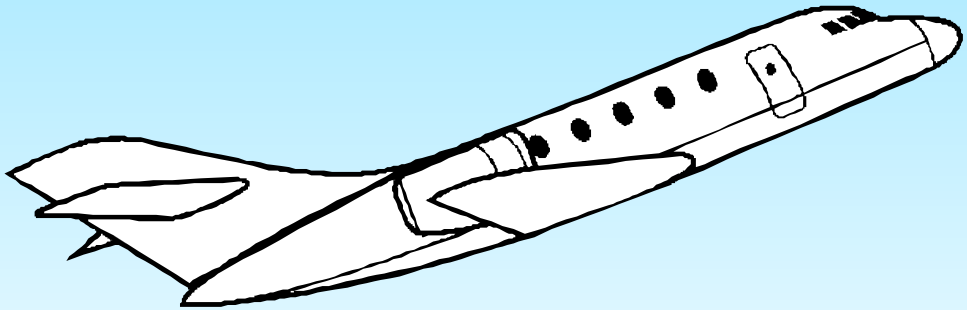
...aus dem Dienstweg-Antrag auf Bewerbung bei VERNET

Vorgeschichte: PTB-Besuche von Siemens/L&G im Mai 2000

Intentionen beim Start

- **Anwendung nur für Auslesung**
- **Anzeige mit Konsumelektronik**

- **Erben etablierter Sicherheits-Technik**



Ehrgeizige Projektleitung durch Herrn A. Sammler

SELMA

27.10.2000

Sicherer **EL**ektronischer **M**essdaten-**A**ustausch

Mit unseren Beitrag **SELMA** zur Vernet-Ausschreibung wollen wir ein Verfahren bereitstellen, das standardisiert ist und es ermöglicht, verrechnungsfähigen Messdaten von einer Messstelle über offene Netze sicher und zuverlässig zu einer Anzeige-/Auswertestelle zu übertragen. Diese Anzeigestelle kann z. B. der Home-PC, der Fernseher oder das Handy sein.

frühe Projektskizze: ... Anzeige auf Fernseher oder Handy

Gefragt: Angemessene Sicherheit

zu Beginn:

- **Sicherheits entsprechend erwarteter Verbreitung von IuK-Technik**
- **Annahme mit Verbreitung wachsende Bedrohung und Schadensrisiken**

Geschaffenes bewahren und nutzen

martin.kahmann@ptb.de

Ein SELMA-schädlicher Webfehler der MID

MID, Anhang 1, 10.5 lässt leider Interpretation zu:

Zähler muss immer integrierte Anzeige aufweisen

martin.kahmann@ptb.de

Leider Vererbung in die neue EO

MEV, Anhang B, Abschnitt 10 Anzeige, Absatz 10.5

Messgeräte zur Messung von Versorgungs-leistungen sind unabhängig davon, ob sie fernabgelesen werden können, auf jeden Fall mit einer den Anforderungen dieser Verordnung unterliegenden Sichtanzeige auszustatten, die für den Verbraucher ohne Hilfsmittel zugänglich ist.
Der Anzeigewert dieser Sichtanzeige gilt als Messergebnis, das die Grundlage für den zu entrichtenden Preis darstellt.

Reklamation von Logikmangel bislang zurückgewiesen

MEV, Anhang B, Abschnitt 7 Eignung, Absatz 7.6

Ein Messgerät ist so auszulegen, dass die Messvorgänge kontrolliert werden können, nachdem das Messgerät in Verkehr gebracht und in Betrieb genommen wurde.

Erforderlichenfalls muss das Messgerät eine spezielle Ausrüstung oder Software für diese Kontrolle besitzen.

Das Prüfverfahren ist in der Bedienungsanleitung zu beschreiben.

Besonders Ärgerlich

Was wird aus §16, Abs. 3 EO-AV ?

(3) Die Bauart eines Messgeräts, die von den Anforderungen dieser Verordnung oder den anerkannten Regeln der Technik abweicht, wird zur innerstaatlichen Eichung zugelassen, wenn die gleiche Messsicherheit auf andere Weise gewährleistet ist. Die Anforderungen an die Bauart werden bei der Bauartzulassung festgelegt.

Aber immerhin im MEG vorgesehen: Systemsicherheit

innerstaatlich geltend:
im neuen Eichrecht deutlicher als bisher:

Verankerung der Systemsicherheit durch

- **dezidierte Benennung von Verwenderpflichten**
- **Gleichstellung von Messsystemen und Messgeräten**

....die Hoffnung bleibt bis zuletzt

Womöglich Ausgangsprodukt für 50.7-Nachfolge

WELMEC Guide 7.2

allerdings
Uneinigkeit über
Risikoklassen B, C, D

D-Vorschlag für E-Zähler:
Risiko-Klasse abhängig von der Genauigkeit:

A > B
B > C
C > D

Für MID keine eichrechtlich relevante DÜ möglich...

...aber hoffentlich bei uns. Dann relevant: (Anhang T)

T1	Do transmitted data contain all relevant information necessary to present or further process the measurement result in the receiving module?
T2	Are transmitted data **protected against accidental and unintentional changes?**
T3	Are legally relevant transmitted data **protected against intentional changes carried out** by *simple common software tools* (for risk classes B&C) or by ***special sophisticated software tools*** (for risk classes **D**&E)?

Bekannte aus 50.7, Anhang 2

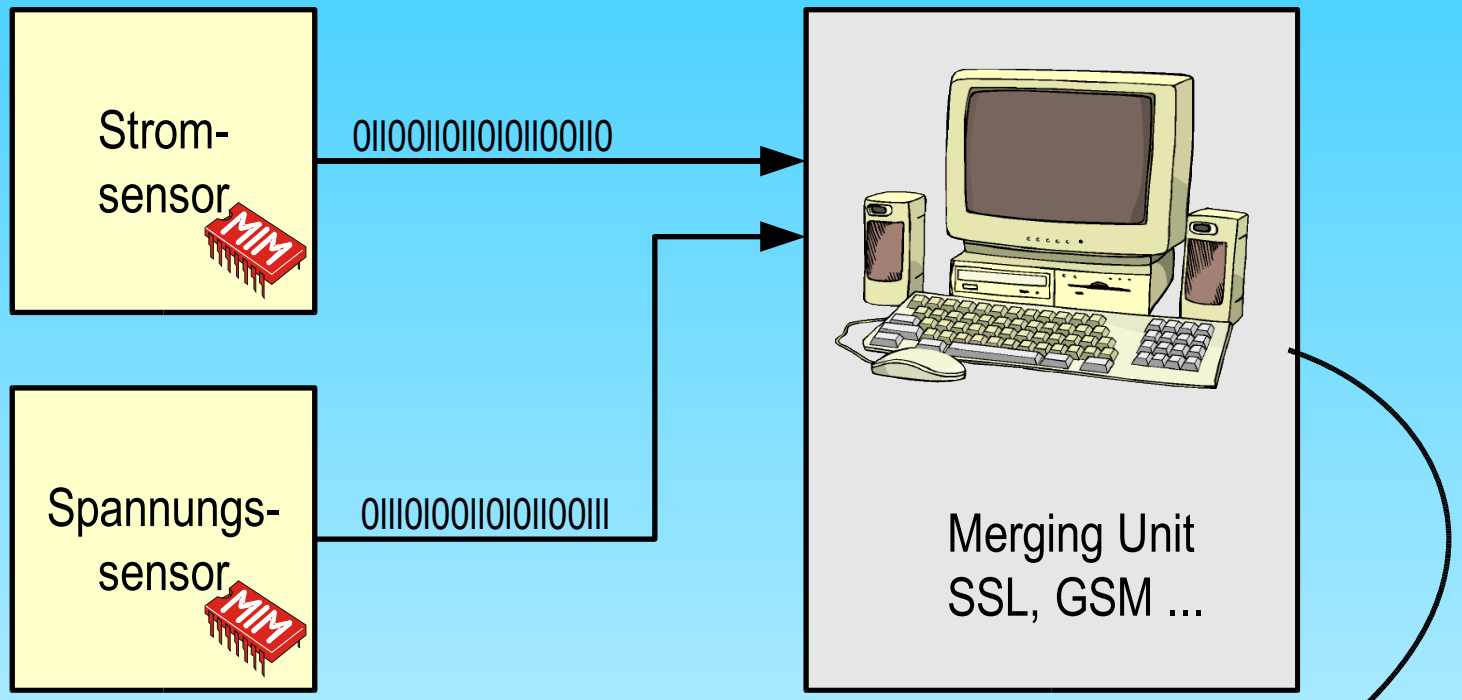
T4	Is it possible for the program that receives transmitted relevant data to verify their authenticity and to assign the measurement values to a particular measurement?
T5	B&C) Are keys treated as legally relevant data and kept secret and protected against compromise by *simple software tools*?
	D&E) Are keys and accompanying data treated as legally relevant data and kept secret and protected against compromise by sophisticated software tools? Are Appropriate methods equivalent to electronic payment used? Is user able to verify the authenticity of the public key?
T6	Are data that have been detected as having been corrupted, prevented from being used?
T7	Is it ensured that the measurement is not inadmissibly influenced by a transmission delay?
T8	Is it ensured that no measurement data get lost if network services become unavailable?

...auch für Down-Load gemäß Guide 7.2 ist SELMA gut

(Anhang D)

D1	Is downloading and the subsequent installation of software automatic? Is it ensured that the software protection environment is at the approved level on completion?
D2	Are **means** employed **to guarantee that the downloaded software is authentic,** and to indicate that the downloaded software has been approved by an NB?
D3	Are means employed to **guarantee that the downloaded software has not been inadmissibly changed** during download?
D4	Is it guaranteed by appropriate technical means that downloads of legally relevant software are adequately traceable within the instrument for subsequent controls?
D5	Is it guaranteed by technical means that software may only be loaded with the explicit consent of the user or owner of the measuring instrument, as appropriate?

Maximal komplizierte Lösung mit SELMA



Stromkunden

„U-Type-Lösung“

SELMAs wesentliche Vorzüge anders nutzen

Rosel

Selmas kleine Schwester
Read-Only-Selma

martin.kahmann@ptb.de

Vereinfachte Authentifizierung: „Direct Trust“

… öffentlichen Schlüssel auf das Produkt drucken !

… bekannt und bewährt
im Fall anderer IT-Lösungen

1 Medienbruch-Freiheit wird nicht gefordert !

2 Wahrscheinlichkeit für Notwendigkeit des Schlüsseltausches während der Eichgültigkeit akzeptabel niedrig

Beispiel-Lastgang-Sidecar

Lastgangspeicher Sidecar mit Wiederholzählwerk (Remote-Anzeige auf Kunden-PC)

Messwert-Übertragung z.B. per GSM

bei der Eichung aufgeklebter PK

Arbeitszähler, geeicht, bereits in Betrieb

S0-Impulse

PTB-A 50.7, Anhang 2

SELMA®

Stromkunden

Transparenz der Tarifierung mit CONFER

PTB-A 50.7, Anhang 2
und PTB-A 50.7, 3.1.1.3 B)

SELMA®

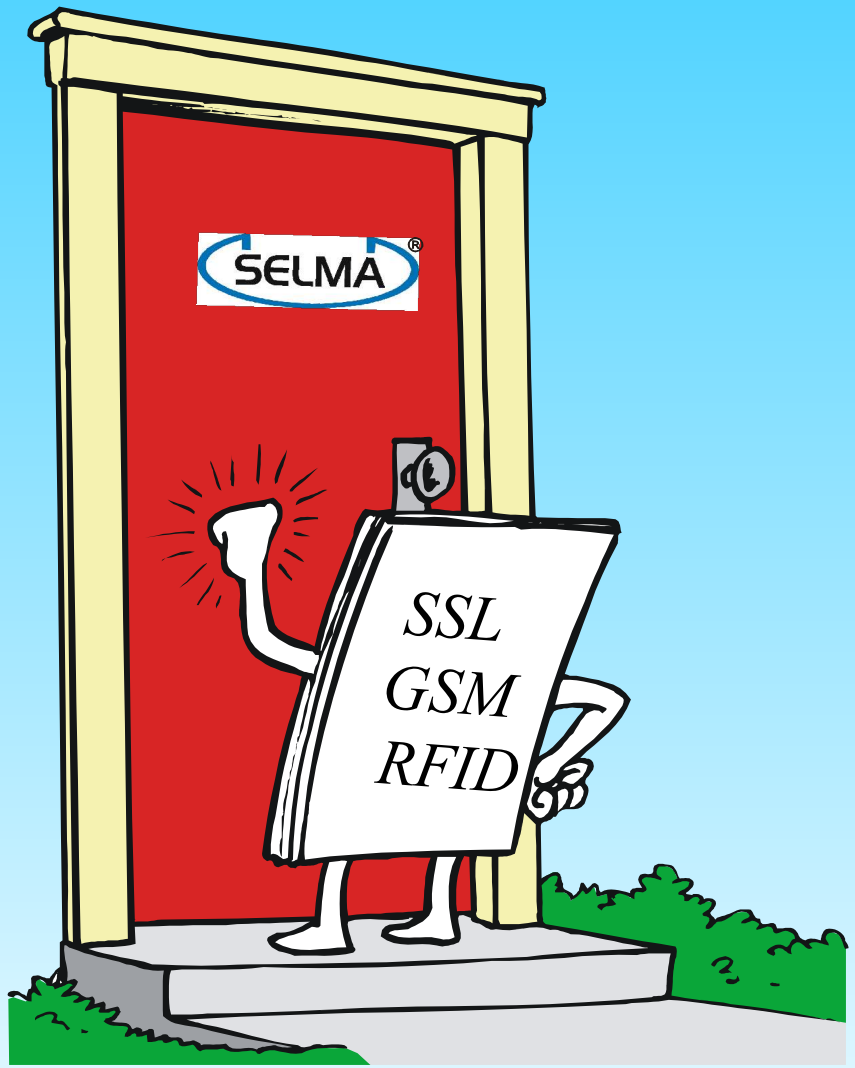
Tarifierung

Zahlungsbeträge

CONFER

Stromkunden

Angebot für Forschungszulassung bis Mitte 2006



Offen sein für Standard-Security Lösungen