Zeitschrift: bulletin.ch / Electrosuisse
Herausgeber: Electrosuisse
Band: 95 (2004)
Heft: 10

Artikel: Sicherheit im Zählerumfeld
Autor: Schaub, Thomas
DOI: https://doi.org/10.5169/seals-857948

Sicherheit im Zählerumfeld

Im liberalisierten Energiemarkt bilden die gemessenen Verbrauchsdaten die Basis für alle Verträge zwischen den verschiedenen Marktteilnehmern. In der Vergangenheit war die Messpräzision die kritische Grösse, nach welchen die Messgräte beurteilt wurden. Heute ist die Messpräzision eine Selbstverständlichkeit. Zusätzlich fordert der Markt einen sicheren, rückverfolgbaren Datenaustauschprozess vom Zähler bis zur Rechnung. Im vorliegenden Beitrag wird das Selma[1]-Konzept (sicherer elektronischer Messdatenaustausch) vorgestellt. Das Konzept bietet eine umfassende Sicherheitsarchitektur für die Authentifizierung von Mess-daten, für die Zugriffssicherheit und für die Zertifizierung von Software.

■ Thomas Schaub

Einleitung

Selma steht für «sicheren, elektronischen Messdatenaustausch». Damit wird ein umfassendes Sicherheitskonzept erschaffen, welches die Bedürfnisse des liberalisierten Energiemarktes (Elektrizität, Gas, Wärme, Wasser) abdeckt. Dabei wird der gesamte Messprozess berücksichtigt: von der Messgrätezulassung, Inbetriebsetzung, über die Messung, bis zur Rechnungsstellung.

Die Sicherheitsarchitektur berücksichtigt die folgenden Randbedingungen:

- bestehende, internationale Standards für Kommunikation und Sicherheit;
- ökonomische Gegebenheiten im Messgeräteumfeld (tiefe Lebenszykluskosten, Kommunikationskanäle mit limitierter Kapazität);
- regulatorische Gegebenheiten im Messgeräte-Umfeld (bestehende Zulassungs- und Eichverfahren mit starker nationaler Ausprägung).

Die Selma-Lösung ist modular und skalierbar. Damit lassen sich kosteneffiziente, auf die spezifischen Kundenbedürfnisse abgestimmte, Sicherheitslösungen aufbauen. Durch die konsequente Verwendung von Standards wird eine Lieferantenunabhängigkeit erreicht und die Integration in bestehende Systemumgebungen erleichtert.

Die drei Sicherheitsmodule

In Bild 1 sind die drei Sicherheitsmodule von Selma dargestellt:

Authentifzierung von Messdaten
Klassische Entsprechung: signiertes Dokument.

Die Messdaten werden im Messgerät mit einer digitalen Signatur versehen. Die Signatur begleitet die Messdaten während ihrer gesamten Lebensdauer. Damit kann jederzeit nachgeprüft werden, dass es sich bei den vorhandenen Datensätzen um Originaldaten handelt, welche aus einem bestimmten Gerät stammen und zu einer bestimmten Zeit gemessen wurden. Mit den so signierten Datensätzen können die Rechnungen unter den Marktteilnehmern überprüft werden.

Gesicherte Kanäle:
Klassische Entsprechung: versiegelter Briefumschlag.

Die Kommunikationsdienste werden mit einer digitalen Signatur versehen. Dabei wird sowohl der auf das Messgerät zugreifende Mandant als auch das antwortende Messgerät identifiziert. Das Messgerät gewährt den vorgesehenen Mandanten Zugriffe auf die für sie vorgesehenen Daten. Mit diesem Modul können selbst über «unsichere Kommunikationskanäle» sicherheitskritische Interaktionen (z.B. Zeitstellen, Parametrierungen, Software Download) mit dem Messgerät durchgeführt werden. Dieses Sicherheitsmodul erschliesst die Nutzung des Internets für die Messdatenerfassung und für den Messgeräteunterhalt.

Zertifizierte Gerätekomponenten:
Klassische Entsprechung: Zulassungszeichen

Neue Parametersätze oder neue Softwareversionen werden von den entsprechenden Zulassungsstellen geprüft und signiert (Eichstelle, Zulassungsstelle). Das Messgerät seinerseits prüft die Signatur und akzeptiert die neuen Parameter, bzw. die neue SW-Version nur, falls die Signatur die berechtigte Stelle identifiziert. Damit schafft man die technischen Voraussetzungen für eine Neukonfiguration des Messgerätes «im Feld». Ein kostspieliger Ausbau und eine Neueichung

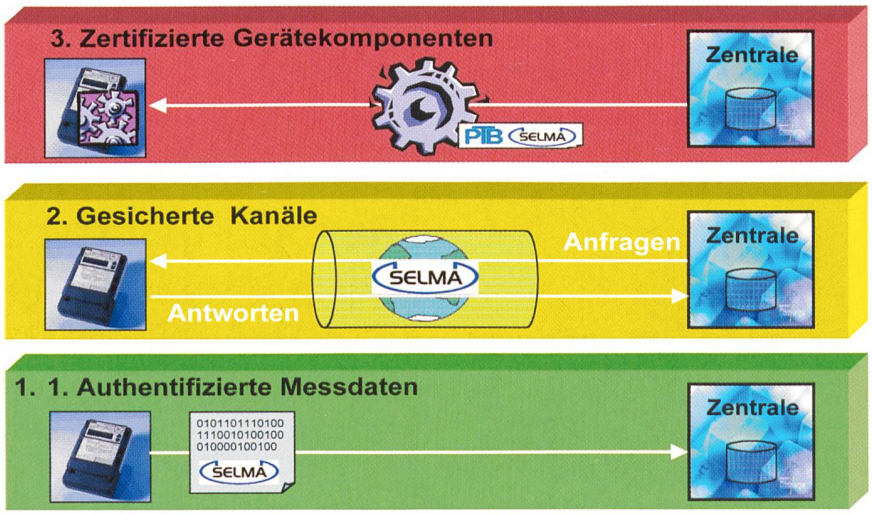

Bild 1 Die drei Anwendungsmodule von Selma.

[1] Das diesem Bericht zu Grunde liegende Vorhaben wird mit Mitteln des deutschen Bundesministeriums für Wirtschaft und Arbeit gefördert: www.selma-project.de

Adresse des Autors
Thomas Schaub
Landis+Gyr AG
Feldstrasse 1
6301 Zug

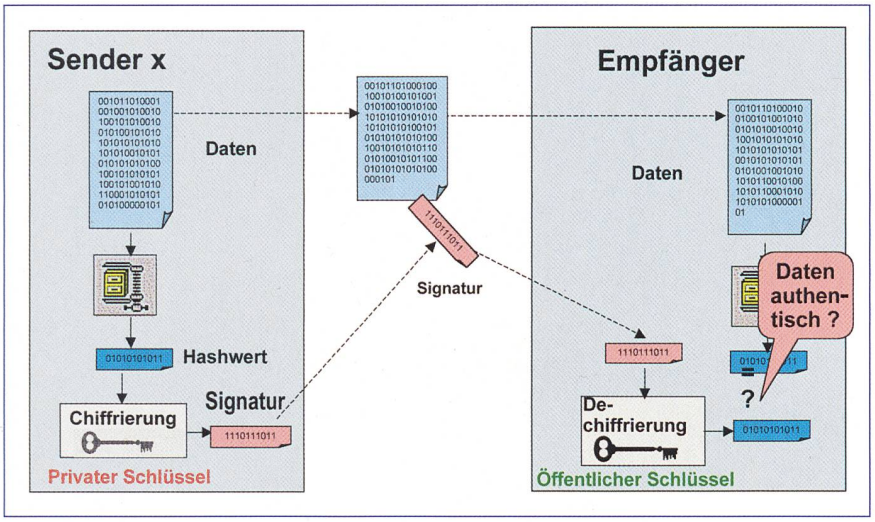

Bild 2 Sicherheit durch Signiertechnologie.

oder sogar eine Neuzulassung können damit vermieden werden. Mit diesem Sicherheitsmodul kann der Messgeräteunterhalt substanziell vereinfacht werden.

Signiertechnologie

Basis für alle Sicherheitsmodule bildet das Signierverfahren gemäss Bild 2. Die zu sendenden Daten (z.B. Messdaten) werden mit einem Standardverfahren auf eine fixe Anzahl Bytes reduziert, den so genannten Hashwert. Die Signatur wird durch Chiffrierung des Hashwertes mit dem privaten Schlüssel errechnet. Die Signatur wird zusammen mit den Originaldaten übertragen. Dabei ist zu beachten, dass die eigentlichen Daten von der Signatur nicht beeinflusst werden. Es ist auf der Empfängerseite somit immer noch möglich, die Daten mit bestehenden Mitteln auszuwerten, indem die Signatur ignoriert wird. (Diese Tatsache erleichtert die schrittweise Einführung von signierten Daten in einem bestehenden Systemumfeld beträchtlich.)

Auf der Empfängerseite wird die empfangene Signatur dechiffriert und mit dem berechneten Hashwert verglichen. Stimmen die beiden Werte überein, so wird die Signatur als gültig – und dementsprechend die Daten als unverfälscht – erklärt.

Besonders zu beachten ist, dass bei dem verwendeten unsymmetrischen Chiffrierverfahren der Schlüssel für die Dechiffrierung nicht mit dem Schlüssel für die Chiffrierung übereinstimmt. Zudem kann aus der Kenntnis des Dechiffrierschlüssels der Chiffrierschlüssel nicht berechnet werden. Für die Signaturanwendung wird deshalb der Chiffrierschlüssel geheim gehalten (private key), während der Dechiffrierschlüssel öffentlich bekannt gegeben wird (public key). Damit wird die Signatur*erstellung* nur für den Berechtigten möglich, während die Signatur*prüfung* von allen durchgeführt werden kann.

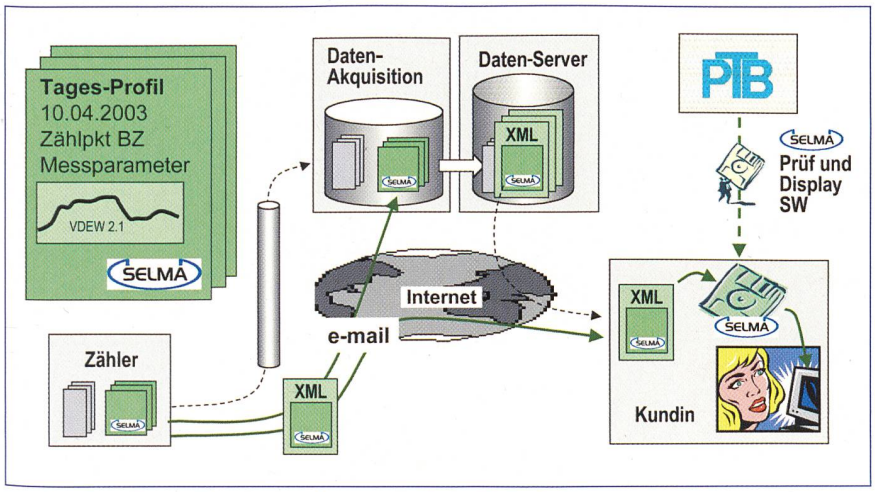

Bild 3 Authentifizierte Messdaten zur Rechnungsprüfung für den Endkunden.

Ein kritischer Punkt bei dem beschrieben Verfahren bildet die Verteilung der öffentlichen Schlüssel. Diese muss durch eine vertrauenswürdige Instanz erfolgen (SigCA, Signature Certification Agency). Der Schlüsselaustausch geschieht mittels von der SigCA signierten Schlüsselzertifikaten. Das Sicherheitskonzept von Selma definiert diese Schlüsselaustauschprozesse im Detail. Dabei wird auf der bestehenden Infrastruktur von Prüfstellen und Zulassungsstellen aufgebaut.

Anwendungen

In den folgenden Abschnitten wird anhand von Beispielen die Anwendung von zwei Selma-Modulen dargestellt.

Messdaten Authentifizierung im Systemumfeld

Die Messdaten werden in so genannte Tagesprofilen aufgeteilt. Dabei handelt es sich um Lastgänge gemäss VDEW2.1 [1], aufgeteilt auf einzelne Tage. Die Tageseinheiten werden vom Messgerät einzeln signiert. Damit diese Tagesprofile jederzeit eindeutig interpretierbar sind, werden ihnen die nötigen Zusatzinformationen wie Zählernummer, Zählpunktsbezeichnung, Messdatum und Messparameter beigefügt. Selma liefert eine detaillierte Spezifikation der Tagesprofile [3] und anderer Datenmodelle. Dabei bedient man sich einer standardisierten Beschreibungssprache, wie sie auch im DLMS Standard [2] eingesetzt wird. Damit können die Selma-Modelle einfach in die internationale Standarisierung übernommen werden.

Gemäss Bild 3 werden die signierten Tagesprofile über die bestehenden Kommunikationskanäle ins Datenakquisitionssystem übertragen und archiviert. Zusätzlich werden die Daten in eine internettaugliche XML-Datei verpackt und über einen bestehenden Internetserver dem Endkunden zur Verfügung gestellt. Der Endkunde kann seine Messdaten mit einem Prüfprogramm auf ihre Authentizität prüfen und mit der Rechnung vergleichen.

Das Selma-Konzept lässt einerseits die Nutzung von bestehenden Infrastrukturen zu, andererseits können aber auch neue Technologien verwendet werden. Insbesondere eignet es sich für die Nutzung von Internettechnologien.

Softwarezertifizierung

Die Architektur des Messgerätes muss den neuen Möglichkeiten, welche die elektronische Zertifizierung von Soft-

ware bietet, angepasst werden. In Bild 4 wird gezeigt, wie die Software – entsprechend der üblichen Zulassungspraxis – in eine «zugelassene SW» (durch die Zulassungsstelle signiert) und in eine «geeichte SW» (durch die Prüfstelle signiert) unterteilt wird. Der «Download Handler» klassifiziert die SW und initiiert die entsprechende Signaturprüfung. In einer Erstzulassung wird sichergestellt, dass der Download Handler die Klassifizierung und die Signaturprüfung einwandfrei durchführt und dass die richtigen Signaturprüfverfahren zum Einsatz kommen.

Die Signiereinheit als Standardkomponente

Der in «Signiertechnologie» beschriebene Signierprozess basiert auf standardisierten Verfahren gemäss [4] und [5]. Damit erreicht man einerseits eine von internationalen Sicherheitsgremien akzeptierte Sicherheit, andererseits wird damit aber auch Unabhängigkeit vom Lieferanten garantiert.

Selma geht bei der Normung noch einen Schritt weiter. Um die Messgeräte-Bauartzulassung von zusätzlichen Prüfungen der Sicherheitsmechanismen zu entlasten, wird für Selma ein zertifiziertes Sicherheitsmodul eingesetzt. Es handelt sich dabei, wie in Bild 5 links unten ersichtlich, um eine Chipkarte, die unter der Eichplombe eingebaut wird. Solange der Messgerätehersteller für die Signaturbildung/-prüfung das zertifizierte Selma-Modul einsetzt, sind für die Bauartzulassung keine zusätzlichen, Prüfungen notwendig.

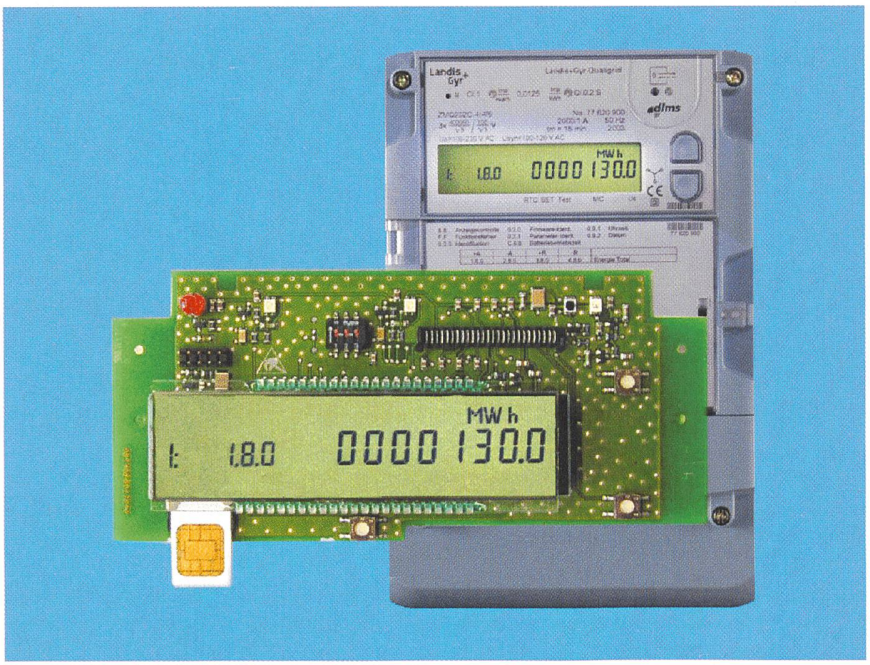

Bild 5 Cryptochip als Standardlösung.

Ausblick

Selma liefert ein Sicherheitskonzept, das auf die Geschäftsprozesse rund um die Energieverbrauchsmessung abgestimmt ist. Die Signatur der Messdaten ermöglicht an allen Stellen des Prozesses (bis zur Rechnungsstellung) eine vereinfachte Validierung der gemessenen Verbrauchsdaten. Damit können Rückfragen und Nacherfassungen weit gehend vermieden werden. Zudem schafft Selma die Möglichkeit durch Herunterladen von validierten und zertifizierten Software-Paketen den Unterhaltsprozess für die Messgeräte zu automatisieren und damit die Unterhaltskosten beträchtlich zu senken. Das Konzept basiert auf bewährten, internationalen Standards und lässt sich deshalb einfach in die bestehende IT-Infrastruktur integrieren. Die Sicherheitsarchitektur ist skalierbar und kann schrittweise eingeführt werden. Das Investitionsrisiko wird mit dem Selma-Konzept klein gehalten.

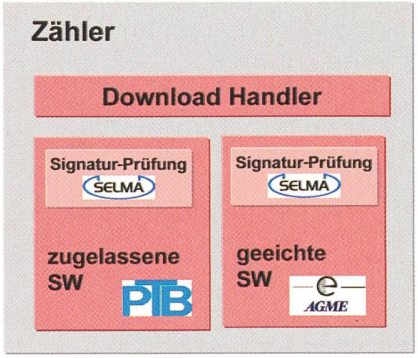

Bild 4 Softwarezertifizierung.

Referenzen

[1] Lastenheft Elektronische Elektrizitätszähler, Erweiterte Version 2.1, VDN, Okt. 2002.
[2] EN62056-62 Zählerstandsübertragung, Tarif- und Laststeuerung, Teil 62: Interface-Klassen.
[3] SELMA, 1.7 Datenmodelle, V1.7, 19.11.03
[4] National Institute of Standards and Technology: NIST: FIPS Publication 180-1: Secure Hash Standard (SHS-1), May 1995.
[5] American National Standards Institute: Public Key Cryptography for the Financial Services Industry: The Elliptic Curve Digital Signature Algorithm (ECDSA), ANSI X9.62-1998, 1998.

La sécurité dans le domaine des compteurs

Sur le marché libéralisé de l'énergie, ce sont les résultats des mesures de consommation qui servent de base à tous les contrats passés entre les différents acteurs du marché. Autrefois, les appareils de mesure étaient principalement jugés d'après leur précision. Aujourd'hui, cette précision va de soi. Le marché exige en plus que le processus d'échange des données soit sûr et puisse être reconstitué, du compteur à la facture. Le concept Selma (échange électronique sûr des données mesurées) est présenté dans le présent article. Ce concept comprend une architecture de sécurité complète pour l'authentification des données mesurées, la sécurité des accès et la certification de logiciels.