Universal Metering Interface UMI

Offener Schnittstellenstandard mit Fokus auf batteriebetriebene Kommunikation im Bereich Smart Metering

Anwendungsgebiete

Schnittstellen von Metrologie-Platinen und Kommunikationsmodulen für elektronische Zählwerke der themis-Reihe

Kurzinformation

Im Zuge der EU-Richtlinien 2009/73/EG (Gas) und 2009/72/EG (Strom) werden flächendeckende Markteinführungen von intelligenten Zählern für die Bereiche Gas und Strom vorgestellt. Bei der 2009/73/EG und 2009/72/EG handelt es sich lediglich um Richtlinien, die von den jeweiligen EU-Ländern teils sehr unterschiedlich interpretiert werden. Dies führt dazu, dass einige Länder bereits spezifische Anforderungen definiert haben, welche unter Umständen erheblich von den Forderungen anderer Länder abweichen können. Hier hilft der offene Schnittstellenstandard bei der Entwicklung einer einzigen MID-konformen Metrologie-Platine, die sich mithilfe von modularen und leicht anpassbaren Kommunikationslösungen erweitern und auf die jeweiligen Bedürfnisse zuschneiden lässt. Zähler können somit auch als Smart-Ready-Zähler installiert und erst später durch Hinzufügen eines entsprechenden Kommunikationsmoduls in das Smart Grid integriert werden.

Datensicherheitskonzept

Datensicherheit ist ein zentraler Punkt im Bereich Smart Metering. Nachfolgend sollen kurz die wichtigsten Begriffe erläutert werden, die sich mittels skalierbarer Sicherheitsarten (UMI Schemes) realisieren lassen. Einsetzbar sind hier symmetrische wie auch kombinierte, hybride Verschlüsselungsverfahren.

Authentifizierung: Wer spricht da?
Unter einer Authentifizierung versteht man den Nachweis der Echtheit einer Identität. Im Bereich Smart Metering ist dies beispielsweise bei der Kommunikation mit dem Zähler, aber auch bei der Kommunikation der Komponenten (z. B. Metrologie-Platine und Kommunikationsmodul) untereinander wichtig. Die Authentifizierung hilft dabei sicherzustellen, dass der Kommunikationspartner wirklich berechtigt ist, mit dem Gerät zu interagieren.

Autorisierung: Wer darf was?
Um sicherzustellen, dass der Kommunikationspartner lediglich die für ihn bestimmten Daten beeinflussen kann, wird eine rollenbasierte Autorisierung verwendet. Hierüber lassen sich Zugriffsrechte spezifisch zuweisen und unbefugte wie auch versehentliche fehlerhafte Eingriffe vermeiden. UMI kennt 16 verschiedene Rollen, z. B. Hersteller, Service und Administrator, welchen sich über eine Matrix verschiedene Zugriffsrechte einräumen lassen.

Integrität: Wer garantiert die Echtheit?
Um die Echtheit der Daten zu garantieren, wird das Prinzip der digitalen Signatur angewendet. Es handelt sich hierbei um eine Art Siegel. Die Signatur kann nur verifiziert werden, wenn die Nachricht vollkommen unverändert vorliegt. Die Änderung von lediglich einem Bit lässt die Signatur ungültig werden und alarmiert das Head-End-System. Das Siegel ist folglich von höchster Wichtigkeit und wird daher nur von vertrauenswürdigen Stellen erteilt. Bereits während der Produktion erhält der Zähler ein Zertifikat, welches Auskunft über die zugewiesene vertrauenswürdige Stelle gibt.

Hauptmerkmale

- UMI ist ein frei zugänglicher offener Schnittstellenstandard mit klarer Ausrichtung auf Smart Metering
- Unterstützt modulare Konzepte durch definierte und interoperable Schnittstellen
- Entwickelt für batteriebetriebene Niedrigenergie-Anwendungen (15 µA bei 3 V)
- Unterstützt verschiedene Sicherheitsstufen und Verschlüsselungsverfahren sowie die rollenbasierte Autorisierung von Nutzern (z. B. Hersteller, Service, Administrator etc.)
- UMI-Kommunikationsmodule haben einen identischen Formfaktor und sind interoperabel einsetzbar
- UMI-Kommunikationsmodule lassen sich für verschiedenste Kommunikationsarten auslegen und entsprechend einbinden, z. B.
  - GSM, GPRS, SMS
  - ZigBee, Wireless M-Bus, Z-Wave, Wavenis, Bluetooth, WiFi
  - Kabelgebundener M-Bus, KNX, PLC
- UMI-Elemente lassen sich einfach in andere Datentypen umwandeln

elster
Instromet

UMI Scheme 1
Symmetrische Verschlüsselung

UMI Scheme 1 nutzt ein symmetrisches Verschlüsselungsverfahren. Zum Verschlüsseln und Entschlüsseln wird folglich derselbe Schlüssel verwendet. Dieser Schlüssel muss beiden Kommunikationspartnern bekannt sein.

Vorteile

- Es wird ein anerkannter, sicherer Verschlüsselungsstandard verwendet (AES-128).
- Einfache Skalierung über die Schlüssellänge möglich.
- Es handelt sich um ein schnelles Kodierverfahren.
- Einfache Integritätsprüfung über Hash-Wert-Bildung möglich.

Nachteile

- Die Schlüssel sind sicherheitsrelevant und müssen geschützt werden.
- Beim Transfer des Schlüssels über einen unsicheren Kanal ergibt sich ein Problem beim Schlüsseltausch.

UMI Scheme 2
Hybride Verschlüsselung

Zum Ver- und Entschlüsseln werden bei der asymmetrischen, zertifikatsbasierten Verschlüsselung unterschiedliche Schlüssel verwendet (privater und öffentlicher Schlüssel).

UMI Scheme 2 nutzt ein hybrides Verschlüsselungsverfahren. Es generiert einen selbst erzeugten, zufälligen symmetrischen Sitzungsschlüssel durch das Diffie-Hellman-Verfahren. Alle anschließenden Nachrichten werden mit dem schnellen und ressourcenschonenden symmetrischen Schlüssel ver- und entschlüsselt.

Vorteile

- Es werden anerkannte sichere Verschlüsselungsstandards verwendet (ECC-256, AES-128).
- Kein Problem beim Schlüsseltausch durch den asymmetrisch verschlüsselten Transfer der Diffie-Hellman-Komponenten.
- Durch die Verwendung des symmetrischen Sitzungsschlüssels wird der Vorteil der schnellen und ressourcensparenden Kodierung genutzt.
- Nur der private Schlüssel ist sicherheitsrelevant. Der öffentliche Schlüssel kann in Form eines Zertifikats frei verteilt werden.
- Einfache Integritätsprüfung über Hash-Wert-Bildung möglich.

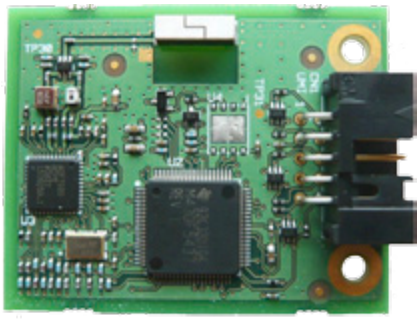
Nachteile

- Beide Kommunikationspartner benötigen eine gemeinsame vertrauenswürdige Zertifizierungsstelle (Certificate Authority (CA)), die ihre Zertifikate signiert und somit die Vertrauenswürdigkeit bestätigt.

Verwaltung rollenbasierter Zugriffsrechte

UMI verfügt über 16 verschiedene Rollen, um den Zugriff auf Daten zu steuern. Hierzu lassen sich über eine Matrix für jede Rolle individuelle Schreib- und Leserechte für alle Datenfelder definieren. Mögliche Rollen wären z. B. Service, Hersteller, Administrator etc.

UMI-ZigBee-Kommunikationsmodul von Telegesis



Kabelloses M-Bus-UMI-Kommunikationsmodul von Elster

UMI wurde von Cambridge Consultants entwickelt und kann dort erworben werden.

UMI und das UMI-Logo sind Warenzeichen von Cambridge Consultants Ltd.

Cambridge Consultants
www.CambridgeConsultants.com/umi

Ihre Ansprechpartner

elster
Vital Connections

Deutschland
Elster GmbH
Strotheweg 1
49504 Lotte-Büren
T +49 541 1214 0
F +49 541 1214 370
info@elster-instromet.com
www.elster-instromet.com

Vereinigtes Königreich
Elster Metering Ltd
Paton Drive, Tollgate Business Park,
Beaconside, Stafford, Staffs. ST16 3EF
T +44 1785 275200
F +44 1785 275305
enquiries@gb.elster.com
www.elster.com

Niederlande
Elster-Instromet B.V.
Munstermanstraat 6
7064 KA Silvolde
T +31 315 338911
F +31 315 338679
Jeroen.vonAlken@elster.com
www.elster-instromet.com

Italien
Elster S.r.l.
Via Cava Trombetta 5
20090 Segrate (MI)
T +39 02269 26272
F +39 02269 26278
mgas-metering-it@elster.com
www.elster.it

Universal Metering Interface UMI DE01
01.2014