Sicherheit des Stromzählers

Anforderungen Lastenheft

CONNECTING BUSINESS & TECHNOLOGY

Versionsdatum: Oktober 2012

Version: 0.4

© Devoteam 2012

Devoteam
Consulting • Solutions • Expertise

Inhalt

Vorbemerkungen

Bis Ende 2017 sollen 70% aller Haushalte in Österreich mit intelligenten Messgeräten („Smart Meter“) ausgestattet sein. Ein zentraler Bestandteil der Messsystem-Architektur ist der intelligente Stromzähler, der u.a. Schnittstellen zu weiteren Spartenzählern, Kundenfunktionen und zu den Systemen des Netzbetreibers bereitstellt.

Im Folgenden werden die Anforderungen an die Sicherheit der Schnittstellen sowie an die internen Sicherheitsfunktionen eines solchen Smart Meter Stromzählers („Stromzähler“) für den österreichischen Markt beschrieben.

Diese Sicherheitsfunktionen müssen kryptografische Funktionen bereitstellen, als sicherer Speicher für kryptografische Schlüssel und weitere wichtige Daten des Stromzählers dienen, sowie die Kommunikation des Zählers absichern und Zugriffsregeln durchsetzen.

Die Anforderungen im vorliegenden Lastenheft beschränken sich auf das Thema Sicherheit und sind somit als Ergänzung des funktionalen Lastenhefts für intelligente Stromzähler auf dem österreichischen Markt zu verstehen.

Dieses Dokument basiert auf den Empfehlungen der Projektgruppe „Sicherheit der Smart Meter Schnittstellen“ von Österreichs Energiewirtschaft in Kombination mit folgenden Dokumenten:

- Intelligente Messgeräte-AnforderungsVO 2011 (IMA-VO 2011)
- FNN Lastenheft EDL Elektronische Haushaltszähler
- Dutch Smart Meter Requirements V3.0 (DSMR)
- BSI Protection Profile for the Security Module of a Smart Metering System
- BSI Protection Profile for the Gateway of a Smart Metering System
- Technische Richtlinie BSI TR-03109-1 Anforderungen an die Interoperabilität der Kommunikationseinheit eines intelligenten Messsystems
- Technische Richtlinie BSI TR-03109 - Anhang A: Kryptographische Vorgaben für die Infrastruktur von Messsystemen

1. Schutzfunktionen gegen Manipulation

Der Stromzähler ist möglicherweise ausgefeilten Manipulationsversuchen und physischen Angriffen ausgesetzt und muss diesen durch geeignete Schutzmaßnahmen entgegenwirken können.

Anforderung	Beschreibung	MUSS/ SOLL
1.1.	Gewährleisten eines sicheren Zustands im Fehlerfall Der Stromzähler muss einen sicheren Zustand bewahren auch wenn Fehler und unerwünschte bzw. nicht vorgesehene Betriebszustände auftreten (zufällig oder mutwillig herbeigeführt) Beispiele für solche Fehler sind: ○ Spannungsverlust ○ Integritätsfehler ○ Fehler beim Selbsttest des Stromzählers ○ Fehler beim Ausführen kryptographischer Funktionen ○ Fehler beim Überprüfen der Zugriffsberechtigungen ○ Fehler bei der Dateneingabe (falsche Datenformate, falsche Datenfeldlänge, ungültige Befehle, etc.) ○ Fehler bei der Bedienung der lokalen Eingabetasten (Tastenfolge zu schnell, mehrere Tasten gleichzeitig gedrückt, etc.) Weitere relevante Fehlertypen und die getroffenen Schutzmaßnahmen sind vom Hersteller anzugeben.	MUSS
1.2.	Erkennen von Wiedereinspielungen Der Stromzähler muss die unautorisierte Wiedereinspielung (Replay) von Daten erkennen können und wiedereingespielte Daten ignorieren.	MUSS
1.3.	Selbsttests Der Stromzähler muss eine Reihe von Selbsttests zur Überprüfung der Zählerfunktionen, der Zählerdaten und zur Erkennung von Manipulationen an der Zählersoftware durchführen können. Diese Tests müssen während des Bootvorgangs, sowie regelmäßig selbstständig während des Betriebs erfolgen. Durchgeführte Tests und verfügbare Rückmeldungen im Fehlerfall sind von Hersteller anzugeben und zu beschreiben.	MUSS

Anforderung	Beschreibung	MUSS/ SOLL
1.4.	Protokollierung Der Stromzähler muss intern folgende Protokolle führen: ○ System-Protokoll mit system- und sicherheitsrelevanten Ereignissen. ○ Verbraucher-Protokoll mit für den Verbraucher relevanten Informationen (wie Zählerstände, Leistungsmittelwerte oder Energieverbrauchswerte, gemäß IMA-VO) ○ Eich-Protokoll, in dem Änderungen in der Kalibrierung des Stromzählers erfasst werden. Dieses Protokoll dient der Umsetzung eichrechtlicher Vorschriften und muss dementsprechend gestaltet sein. In den Protokollen müssen zu jedem Eintrag jeweils die ID des verursachenden Benutzers bzw. Systems, Event-Typ, Zeitpunkt, sowie das Ergebnis der Aktion gespeichert werden.	MUSS
1.5.	Protokoll-Speicher Das Verbraucher-Protokoll für historische Verbrauchswerte muss als konfigurierbarer Ring-Buffer implementiert werden, sodass die maximale Speicherdauer, unabhängig von Intervall und Umfang der Messungen, an die gesetzlichen Vorgaben angepasst werden kann. Der Speicher für das Systemprotokoll muss eine angemessen Größe aufweisen, die sicherstellt, dass System-Protokollmeldungen nicht überschrieben werden, bevor sie durch ein zentrales System ausgelesen werden können. Eine Mindestspeicherdauer von 6 Monaten wird als angemessen erachtet. Das Eich-Protokoll muss alle Einträge der gesamten Lebensdauer des Zählers aufnehmen. Ein Löschen von Einträgen des Eich-Protokolls darf für keinen Benutzer möglich sein.	MUSS
1.6.	Schutz von Protokolleinträgen Die Einträge aller Protokolle müssen vor nicht-autorisierten Veränderungen geschützt sein	MUSS

Anforderung	Beschreibung	MUSS/ SOLL
1.7.	Physischer Manipulationsschutz der Stromzähler Elektronik Die Elektronik (elektronische Bauelemente, interne Datenleitungen) des Stromzählers muss physischer Manipulation (mittels Prüfspitzen o.ä.) durch Angreifer mit hohem Angriffspotentialwiderstehen können. Anstelle des physischen Schutzes von Datenleitungen (z.B. durch eine hochintegrierte Bauweise) können auch kryptografische Maßnahmen treten.	MUSS
1.8.	Schutzmaßnahmen Zählergehäuse Das Zählergehäuse muss angemessenen Schutz gegen unerlaubte Manipulation bieten. Zusätzlich muss die Öffnung des Klemmendeckels und des Gehäuses (separat) mittels geeigneter Maßnahmen (Kontakte, Sensoren) durch die Zählerelektronik erkannt und protokolliert werden.	MUSS
1.9.	Zugangsschutz von Netzwerk-Interfaces Zum Schutz vor unbefugtem Zugriff müssen physische Netzwerkinterfaces zum LMN und WAN durch eine plombierte Abdeckung geschützt sein. Des Weiteren soll es einem Administrator möglich sein, ungenutzte Interfaces in der Konfiguration zu deaktivieren.	MUSS
1.10.	Zeitstempel-Funktion Der Stromzähler muss die interne Systemzeit in regelmäßigen Intervallen mit einer vertrauenswürdigen externen Quelle abgleichen (aktiv oder passiv im Zuge einer Abfrage durch zentrale Systeme). Es soll einem Administrator möglich sein, das Aktualisierungsintervall und die maximale Abweichung zu konfigurieren. Überschreitungen der maximalen Abweichung müssen protokolliert werden.	MUSS

Anforderung	Beschreibung	MUSS/ SOLL
1.11.	Alarmierung Der Zähler muss einen Administrator aktiv alarmieren, falls Manipulationsversuche oder kritische Systemzustände erkannt werden (beispielsweise basierend auf bestimmten Einträgen im System-Protokoll, zu starker Abweichung der Systemzeit, bei Öffnen der Geräteabdeckung oder bei Erkennen von starken Magnetfeldern). Die Alarmierung bzw. nicht Alarmierung bei Events muss dabei vom Betreiber über das zentrale System konfigurierbar sein.	MUSS

2. Schutz der Daten im Zähler

Der Stromzähler muss die Integrität lokal gespeicherter Daten sowie den berechtigten Zugriff auf gespeicherte Benutzerdaten über entsprechende Schnittstellen sicherstellen können. Dies soll während des gesamten Lebenszyklus der Daten (von der Erhebung / Import über Verwendung bis zur Löschung / Sperrung) gewährleistet sein. Von besonderer Wichtigkeit ist der Umgang mit personenbezogenen Daten des Verbrauchers.

Anforderung	Beschreibung	MUSS/ SOLL
2.1.	Zugriffskontrolle Der Stromzähler soll eine Policy durchsetzen, die den Zugriff auf gespeicherte Schlüssel, Zertifikate und Nutzerdaten regelt. Dabei soll geregelt sein, auf welche Objekte von welchen Subjekten über welche Schnittstellen zugegriffen werden darf. Der Zählerhersteller ist aufgefordert, die Zugriffskontrollpolicy anzugeben, sowie verfügbare Managementfunktionen, die es Zähleradministratoren erlauben, diese entsprechend zu ändern.	SOLL
2.2.	Verschlüsselung gespeicherter Daten Der Stromzähler soll lokale Daten, die nicht in Gebrauch sind verschlüsselt speichern können.	SOLL
2.3.	Integrität der Zählerdaten Der Zähler soll die Integrität der Zählerdaten (Zählerstand, Lastgang, etc.) durch digitale Signaturen durch geeignete kryptografische Maßnahmen gemäß Kapitel 6 sichern können.	SOLL
2.4.	Überwachung der Integrität gespeicherter Daten Eine unbefugte Änderung der Daten auf dem Stromzähler darf nicht möglich sein. Daher müssen die gespeicherten Daten auf Integritätsfehler hin überwacht werden. Bei Entdecken eines Fehlers muss die Nutzung der Daten, sowie der zugehörige Prozess gestoppt werden und es ist eine Systemmeldung bzw. je nach Konfiguration ein Alarm zu erzeugen. Falls bei Entdeckung von Integritätsverletzungen weitere Maßnahmen umgesetzt werden, sind diese vom Hersteller zu beschreiben.	MUSS

Anforderung	Beschreibung	MUSS/ SOLL
2.5.	Schutz von nicht mehr benötigten Schlüsseln und Daten Es muss sichergestellt sein, dass alle nicht mehr benötigten Informationen (insbesondere temporäre Schlüssel) bei Freigabe des zugehörigen Speicherbereichs komplett unverfügbar gemacht werden. Der Stromzähler muss dazu in der Lage sein, Schlüssel und sonstige Daten mit einem geeigneten Löschverfahren zu entfernen. Das Löschverfahren ist anzugeben.	MUSS
2.6.	Pseudonymität Die im Stromzähler gespeicherten und in Folge zu zentralen Systemen übertragenen Daten sollen keinen direkten Rückschluss auf die Identität des Kunden ermöglich (z.B. über die in Marktprozessen verwendete Zählpunktnummer, Kundennamen oder Anlagenadresse)	SOLL

3. Sicherheit der Zählerkommunikation

Die Kommunikation des Stromzählers mit den Kommunikationspartnern in WAN, LMN und HAN ist hinsichtlich Vertraulichkeit, Integrität und Authentizität abzusichern.

Anforderung	Beschreibung	MUSS/ SOLL
3.1.	Physisch getrennte Schnittstellen Der Stromzähler soll folgende physisch getrennte Schnittstellen aufweisen: ○ Weitverkehrskommunikation (WAN) ○ Lokales Metrologie Netzwerk für Spartenzähler (LMN) ○ Kundenschnittstelle in Home Area Netzwerke (HAN) ○ Lokale Wartungsschnittstelle für den Netzbetreiber	SOLL
3.2.	Firewall-Funktion Der Stromzähler dient als Firewall zwischen den vorhandenen Schnittstellen und muss somit den Informationsfluss zwischen allen angeschlossenen Kommunikationspartnern regeln können.	MUSS
3.3.	Authentifizierung von ausgehenden WAN Verbindungen Es muss sichergestellt werden, dass Informationen vom Zähler nur an authentifizierte externe Kommunikationspartner im WAN gesendet werden.	MUSS
3.4.	Beschränkung der Schnittstellen für Administrationsfunktionen Der Zugriff auf Funktionen zur Zähleradministration muss ausschließlich über dafür berechtigte Schnittstellen möglich sein. Der Zugriff über nicht berechtige Schnittstellen muss geeignet unterbunden werden, sodass der Zugriff auch mit gültigen Authentifizierungsdaten nicht möglich ist.	MUSS
3.5.	Berechtigte Spartenzähler Informationen von nicht-authentifizierten Spartenzählern müssen vom Stromzähler ignoriert werden.	MUSS

Anforderung	Beschreibung	MUSS/ SOLL
3.6.	Sicherung der Kommunikation ins WAN Der Stromzähler muss Ver- und Entschlüsselung sowie Integritätssicherung im verwendeten Protokoll zur Verbindung über die WAN Schnittstelle gemäß den Vorgaben zur Kryptografie aus Kapitel 6 beherrschen.	MUSS
3.7.	Sicherung der Kommunikation ins LMN Der Stromzähler muss Ver- und Entschlüsselung sowie Integritätssicherung im verwendeten Protokoll zur Verbindung über die LMN Schnittstelle gemäß den Vorgaben zur Kryptografie aus Kapitel 6 beherrschen.	MUSS
3.8.	Wake-Up Nachricht Es soll möglich sein, eine Wake-Up Nachricht an den Stromzähler zu senden, woraufhin dieser eine Verbindung zu einer hinterlegten Adresse aufbaut.	SOLL
3.9.	Sichere Kanäle für unterschiedliche Kommunikationspartner Der Stromzähler muss zu verschiedenen vertrauenswürdigen externen Kommunikationspartnern über WAN und LNM Interfaces kryptografisch gesicherte Kanäle aufbauen können, die untereinander logisch getrennt sind.	MUSS
3.10.	Prüfung des Ursprungs der Kommunikation Der Zähler muss durch geeignete kryptografische Maßnahmen gemäß Kapitel 6 dafür sorgen, dass gesendeten Daten einen eindeutigen Beweis des Ursprungs der Kommunikation tragen. Der Zähler muss den Ursprung von empfangenen Daten ebenso eindeutig prüfen können. Die unberechtigte Zwischenschaltung von zusätzlichen Kommunikationspartnern muss verhindert werden.	MUSS

4. Sicherheit im Zählerbetrieb

Administrativen Aufgaben des Netzbetreibers im Zählerbetrieb (Parametrisierung, Updates, Fernschaltungen, etc.) sind überwiegend aus der Ferne durchzuführen, um die Kosten einer Vor-Ort-Bedienung des Stromzählers zu vermeiden. Gleichzeitig ist es erforderlich, dass die Wartungsfunktionen des Zählers entsprechend abgesichert sind, um einen Missbrauch dieser Funktionen zu verhindern.

Anforderung	Beschreibung	MUSS/ SOLL
4.1.	Administrationsfunktionen Der Stromzähler muss mindestens folgende administrative Sicherheitsfunktionen ausführen können: ○ Update von Schlüsseln und Zertifikaten ○ Festlegen der Gültigkeitsdauer von kryptografischen Schlüsseln. ○ Firmware Update ○ Pairing-Funktion zum Anbinden von Spartenzählern ○ Konfiguration der Kommunikationsparameter des Stromzählers ○ Konfiguration der Firewall Funktion ○ Zugriffsmanagement	MUSS
4.2.	Identifikation und Authentifizierung Der Stromzähler darf Informationen erst dann über bidirektionale Schnittstellen an einen Anforderer senden, nachdem dieser erfolgreich identifiziert und authentisiert wurde. Die Authentifizierung muss dabei zählerspezifisch und schnittstellenspezifisch erfolgen (d.h. über individuelle Passwörter pro Zähler und pro Zählerschnittstelle. Der Schlüssel bzw. das Passwort für die lokale Schnittstelle darf nicht für den Fernzugriff über das WAN gültig sein).	MUSS
4.3.	Authentifizierung zum Ausführen von Administrationsfunktionen Administrations-Funktionen (z.B. Parametrierung) dürfen nur nach erfolgreicher Authentifizierung über eine berechtigte Schnittstelle ausgeführt werden.	MUSS

Anforderung	Beschreibung	MUSS/ SOLL
4.4.	Sicherung der Ausführung von kritischen Befehlen Vor der Ausführung von als kritisch eingestuften Befehlen (z.B. Connect/Disconnect, Firmware Update, Änderung von zulassungsrelevanten Parametern) soll die Gültigkeit des Befehls über zusätzliche Sicherheitsmerkmale geprüft werden, die über die Authentifizierung der regulären Kommunikationsverbindung hinausgeht. Die Ausführung darf erst nach positiver Prüfung durch den Zähler erfolgen. Zulässige Implementierungsvarianten sind die Prüfung von zusätzlichen Schlüsseln oder die Validierung einer sicheren Signatur für die Ausführung des Befehls.	SOLL
4.5.	Absicherung von Software-Updates Ein Update der Firmware darf erst erfolgen, nachdem die Authentizität des Update-Befehls, sowie der Firmware selbst mittels kryptographisch sicherer digitaler Signaturen geprüft wurde und falls die Version der neuen Firmware höher als die der aktuellen ist. Der Zähler muss, falls diese aus betrieblichen Gründen erforderlich ist,einen sicheren Rückstieg auf eine ältere Firmware Version ermöglichen. Die Zählerdaten (gespeicherte Messdaten und Konfiguration) dürfen durch ein Update der Firmware nicht verändert oder gelöscht werden. Im Zuge des Up- oder Downgrades müssen zwingend notwendige Änderungen an der Konfiguration von neuen oder geänderten Funktionen automatisch vorgenommen werden.	MUSS
4.6.	Beschränkung der Fähigkeiten von Funktionen Die hier beschriebenen Sicherheitsfunktionen dürfen nicht durch weitere Features ausgehebelt werden. Daher sind vom Stromzähler-Hersteller zusätzlich implementierte Funktionen (andere als die hier beschriebenen) so zu gestalten (klare Trennung), dass die hier beschriebenen Sicherheitsmaßnahmen nicht beeinträchtigt werden.	MUSS

Anforderung	Beschreibung	MUSS/ SOLL
4.7.	• Deaktivierung von internen Herstellerfunktionen Funktionen, die nur bei der Entwicklung und Herstellung des Stromzählers verwendet werden, müssen im operativen Betrieb zuverlässig deaktiviert sein. Dies sind beispielsweise Funktionen zum Testen, Debuggen oder zur Initialisierung im Rahmen des Produktionsprozesses. Diese Funktionen dürfen weder über nicht dokumentierte Funktionen noch über nicht undefinierte bzw. fehlerhafte Betriebszustände ansprechbar sein.	MUSS
4.8.	Benutzer-Attribute Der Stromzähler soll für die einzelnen Benutzer mindestens folgende Attribute speichern: ○ Benutzer-ID bzw. System-ID ○ Berechtigungsgruppe ○ Erlaubte Verbindungs-Schnittstelle Werden weitere Attribute gespeichert, so sind diese anzugeben. Der Zähler soll zudem für Administratoren die Möglichkeit bereitstellen, Benutzer-Attribute zu ändern.	SOLL
4.9.	Überwachen fehlgeschlagener Authentifizierungen Der Zähler soll die Anzahl der fehlgeschlagenen Anmeldeversuche speichern und bei Überschreiten eines Schwellwertes entsprechende Aktionen (z.B. Zeitsperren, Alarme) ergreifen. Der Schwellwert soll von einem Administrator definiert werden können.	SOLL
4.10.	Ablaufen der Identifikation und Authentifizierung Der Zähler soll das zugreifende System nach Ablauf einer Frist (Zeitraum vom Zähleradministrator festlegbar) auffordern, sich erneut zu authentifizieren.	SOLL

5. Sicherheit in der Zählernutzung durch den Verbraucher

Die Nutzung betrifft z.B. das Abfragen der eigenen Verbrauchsdaten über das lokale Display und die HAN Schnittstelle durch den Verbraucher. Die operative Nutzung des Stromzählers durch den Verbraucher muss durch entsprechende Sicherheitsfunktionen abgesichert werden.

Anforderung	Beschreibung	MUSS/ SOLL
5.1.	Unidirektionale Kundenschnittstelle Die Kundenschnittstelle ist, unabhängig von der physischen Ausprägung der Schnittstelle, unidirektional im Sinne der IMA-VO zu implementieren. Als Kundenschnittstelle wird dabei jene Schnittstelle gewertet, die dem Kunden physisch oder über Funk zur Verwendung gemäß IMA-VO zugänglich gemacht wird. Die Kundenschnittstelle muss bei Bedarf abschaltbar sein.	MUSS
5.2.	Vertraulichkeit der Informationen für den Verbraucher Ein unberechtigtes Mitlesen von Daten und Informationen, die über die HAN Schnittstelle übermittelt werden, darf nicht möglich sein. Dazu sind die in Kapitel 6 beschriebenen Verfahren zur symmetrischen Verschlüsselung einzusetzen. Das Passwort muss durch den Netzbetreiber konfigurierbar sein.	MUSS
5.3.	Schutz des lokalen Displays Die Anzeigen auf dem integrierten Verbrauchsdisplay des Zählers müssen – je nach Kundenwunsch - durch den Netzbetreiber beschränkt werden können. Folgende Varianten des Display-Schutzes müssen konfiguriert werden können: ○ Beschränkung der Anzeige auf aktuelle Messwerte (ohne historische Daten) ○ Keine Beschränkung der Anzeige Bei Öffnen des Klemmendeckels muss eine etwaige Anzeigebeschränkung aufgehoben werden.	MUSS

6. Kryptographische Funktionen

Der Stromzähler muss verschiedene kryptographische Funktionen beinhalten, die von den Sicherheitsfunktionen des Zählers genutzt werden müssen.

Anforderung	Beschreibung	MUSS/ SOLL
5.4.	Nutzungsdauer von Schlüsseln Da der gesicherte und vertrauenswürdige Schlüsselaustausch einen hohen Overhead verursachen kann, soll es möglich sein, vereinbarte Schlüssel in späteren Verbindungen zum gleichen Kommunikationspartner erneut zu verwenden. Die Nutzungsdauer der verwendeten Schlüssel soll parametrisierbar sein..	SOLL
5.5.	Ver- und Entschlüsselung von Inhaltsdaten Der Stromzähler muss Ver- und Entschlüsselung sowie Integritätssicherung der Datenkommunikation über alle Schnittstellen beherrschen. Die Verschlüsselung muss dabei vom Betreiber pro Schnittstelle ein- und ausschaltbar sein. Die Verschlüsselung muss unabhängig vom eingesetzten Transportprotokoll auf höheren Netzwerkschichten implementiert sein, sodass der gesicherte Ende-zu-Ende Transport der Daten gewährleistet ist.	MUSS
5.6.	Kompression von Daten Da für das Versenden von Smart Metering Daten oft nur sehr begrenzte Bandbreiten zur Verfügung stehen, müssen zu versendende Daten vor der Verschlüsselung mittels DEFLATE oder vergleichbar auf der Applikationsebene (Ende zu Ende) komprimiert werden können. Die Kompression muss bei Bedarf abschaltbar sein.	MUSS
5.7.	Erzeugung und Update von Schlüssel und Zertifikaten Für Schlüssel und Zertifikate kann eine begrenzte Verwendungsdauer vorgesehen sein. Die maximale Verwendungsdauer muss daher konfigurierbar sein. Der Stromzähler muss dazu seine kryptographischen Schlüssel auf Kommando selbst erzeugen können.	MUSS

Anforderung	Beschreibung	MUSS/ SOLL
5.8.	Unterschiedliche einsatzspezifische Zertifikate und Schlüssel Der Stromzähler muss verschiedene Schlüssel(paare) und Zertifikate je nach Kommunikationspartner und Einsatzzweck in ausreichender Zahl vorhalten können. Beispiele für Einsatzzwecke sind: – Signieren und Verifizieren von Messdaten – Verbindungsverschlüsselung im WAN – Passwort für den lokalen Zugriff auf Wartungsfunktionen – Zum Austausch von Schlüsseln für administrative Kommandos – Öffentlicher Schlüssel zum Verifizieren digital signierter Daten – Symmetrischer Schlüssel zur Verschlüsselung des Zählerspeichers.	MUSS
5.9.	Authentisierungsverfahren Der Stromzähler muss folgende Authentisierungsverfahren unterstützen: – Passwort Authentifizierung – Challenge Response Authentifizierung – Signaturbasierte Authentifizierung	MUSS

Anforderung	Beschreibung	MUSS/ SOLL
5.10.	Kryptografische Algorithmen und Schlüssellängen Folgende Algorithmen müssen für die verschiedenen kryptografischen Funktionen des Zählers unterstützt werden: – Erzeugung und Verifikation digitaler Signaturen: ECDSA (siehe ANSI X9.62:2005) – Schlüsseleinigung: ECKA-DH – Schlüsseltransport: ECKA-EG – Symmetrische Verschlüsselung: AES-128 im CBC oder CTR-Modus – Hash-Algorithmus: SHA-256 oder AES-CMAC (siehe ISO/IEC 10116:2006 und RFC4493) – Elliptische Kurven nach NIST P-256 (siehe RFC5114). Die Implementierung von Algorithmen mit gleichwertiger oder besserer kryptografischer Stärke ist zulässig. Etwaige Schwachstellen in der Implementierung von kryptografische Algorithmen müssen über Software Updates behoben werden können.	MUSS
5.11.	Update weiterer kryptografischer Algorithmen Folgende kryptografische Algorithmen sollen in Zukunft per Software Update unterstützt werden: – Symmetrische Verschlüsselung: AES-256 – Hash-Algorithmus: SHA-384 – Elliptische Kurven nach NIST P 384 oder besser	SOLL
5.12.	Erzeugung kryptographischer Zufallszahlen Der Stromzähler benötigt Zufallszahlen zur Schlüsselerzeugung und zur Verhinderung von Replay-Angriffen. Daher müssen kryptographisch sichere Zufallszahlen erzeugt werden können. Der Zufallszahlengenerator soll mindestens den Ansprüchen eines deterministischen Zufallszahlengenerators mit zusätzlich erweiterter Folgenlosigkeit genügen (aufbauend auf ISO18031). Es ist anzugeben, auf welchen Standards der Zufallszahlengenerator aufbaut und welche Gütekriterien er aufweist.	MUSS

7. Begriffsbestimmungen

AES	Der Advanced Encryption Standard ist ein symmetrisches Blockchiffrierverfahren, der vom NIST als Standard bekannt gegeben wurde.
Asymmetrische Kryptographie	Bei asymmetrischen kryptographischen Verfahren erstellt jeder Empfänger ein Schlüsselpaar, das aus einem öffentlichen und einem privaten Schlüssel besteht. Der öffentliche Schlüssel dient der Verschlüsselung von Nachrichten, die nur mit dem zugehörigen privaten Schlüssel wieder entschlüsselt werden können.
Breaker	Elektronische Absperrvorrichtung am Stromzähler.
CBC-Modus	Cypher Block Chainining. Betriebsmodus um eine Blockchiffre auf einen Datenstrom anzuwenden. Dabei wird ein Chiffreblock mit dem jeweils vorherigen Chiffreblock verknüpft um sich wiederholende Muster zu verhindern.
CMAC	Cipher-base MAC. Methode zur Nachrichtenauthentisierung, die auf einer Blockchiffre basiert.
CTR-Modus	Counter Mode. Betriebsmodus um eine Blockchiffre auf einem Datenstrom anzuwenden.
Debuggen	Prozess des Diagnostizierens und Lokalisierens von Fehlern in IT-Systemen.
Diffie-Hellman-Protokoll	Protokoll zum Schlüsselaustausch eines symmetrischen Schlüssels über einen unsicheren Kanal.
Digitale Signatur	Kryptographisches Verfahren, welches eine Prüfsumme zu einer Nachricht berechnet. Anhand dieser Prüfsumme kann der Urheber der Nachricht eindeutig verifiziert werden.
ElGamal	Ein asymmetrisches Krypoverfahren.
Elliptische Kurve	Elliptische Kurven werden in der Kryptographie eingesetzt, um durch die damit bei gleicher Sicherheit kürzeren Schlüssellängen Speicherplatz zu sparen.
Firewall	System zum Überwachen und Beschränken von Netzwerkverkehr.
Firmware	Software, die in elektronische Geräte eingebettet ist.
Folgenlosigkeit	Ein Zufallszahlengenerator wird dann als folgenlos bezeichnet, wenn durch Kenntnis einer Zufallszahl nicht auf die vorhergehend oder nachfolgend generierten Zahlen geschlossen werden kann.
Hash	Ergebnis einer mathematischen Einwegfunktion (Hash-Funktion). Eine Hash-Funktion ist nicht umkehrbar, d.h. es ist nicht ohne weiteres möglich vom Ergebnis der Funktion auf die Eingabedaten zu schließen.
HAN	Im Home Area Network können Verbrauchsgeräte des Kunden und Stromzähler verbunden werden.
Hybride Ver-/Entschlüsselung	Kombination aus symmetrischer und asymmetrischer Kryptographie. Dabei wird ein symmetrischer Schlüssel mittels eines asymmetrischen Verfahrens ausgetauscht, der für eine gewisse Zeit oder eine gewisse Anzahl von Nachrichten gültig ist. Dies kombiniert den Vorteil des einfachen Austauschs in asymmetrischen Kryptoverfahren mit dem geringeren Overhead der symmetrischen Verfahren.

Integrität	Bezeichnet die Unversehrtheit einer Information. Die Integrität ist gewährleistet, falls die Daten/Informationen in dem Zustand sind in dem sie der letzte berechtigte Benutzer hinterlassen hat.
LMN	Im Local Metrological Network sind Stromzähler und Spartenzähler verbunden.
Overhead	Zusätzlich zum eigentlichen Zweck benötigtes Datenvolumen oder Speicherplatz.
Parametrisierung	Einbringen der Zählerkonfiguration und Aktivierung bzw. Deaktivierung von Zählerfunktionen.
Pairing	Verheiraten zweier elektronischer Geräte. Dies kann u.a. über einen Austausch von kryptographischen Schlüsseln erfolgen, sodass nur noch die beiden Geräte die Kommunikation entschlüsseln können.
Replay	Replay bezeichnet das Wiedereinspielen von bereits gesendeten Nachrichten in einem Netzwerk. Ein Angreifer kann so bspw. versuchen eine Aktion nochmals anzustoßen.
Ring-Buffer	Ein Ring-Buffer oder Ringspeicher ist eine Datenstruktur die auf einem Speicher mit fixer Größe basiert. Sobald das Ende des Speichers beschrieben ist, wird mit dem Schreiben am Speicheranfang fortgefahren als ob die Enden verbunden wären.
Symmetrische Kryptographie	Bei symmetrischen kryptographischen Verfahren müssen Kommunikationspartner einen gemeinsamen Schlüssel austauschen, mit dem ihre Nachrichten ver- und entschlüsselt werden.
TLS-Protokoll	Transport Layer Security ist ein hybrides kryptographisches Protokoll zur Verbindungsverschlüsselung.
WAN	Über das Wide Area Network kommuniziert der Stromzähler mit den Systemen des Netzbetreibers.
Zeitstempel	Wert, der einem Ereignis einen eindeutigen Zeitpunkt zuordnet.

Palais der Schönen Künste, Löwengasse 74, A-1030 Vienna, AUSTRIA
Tel. : +43 (0) 1715 0000-0 – E-Mail : info@devoteam.com
www.devoteam.at