

## SmartMeter PP - Kommentierungsverfahren

Bitte als ODT- oder Word-Datei (bitte kein PDF) senden an: [smartmeter@bsi.bund.de](mailto:smartmeter@bsi.bund.de)

**Dokument** Gateway for Smart Metering Systems Protection Profile  
Schutzprofil für die Kommunikationseinheit eines Messsystems

**Firma/Institution** VATM e. V.

**Name:** Iris Nolte

**E-Mail:** in@vatm.de

**Telefon:**

**Version** 0.73

**Datum** 18.02.2011

**Kürzel**

Ich bin mit einer Veröffentlichung der Kommentare **mit** Namensangabe einverstanden: Ja  Nein

Ich bin mit einer Veröffentlichung der Kommentare **ohne** Namensangabe einverstanden: Ja  Nein

Zu Spalte 4 – Art (Klassifikation) der Kommentare: GE: allgemeiner Kommentar ED: redaktionelle Anmerkung TE: technische Anmerkung

1	2	3	4	5	6
lfd Nr.	Kapitel/ Unterkap./ Anhang	Absatz / Abb./Tab./ Note	Art	Kommentar (Begründung/Hintergrund)	Änderungsvorschlag (bitte so konkret wie möglich)
1.	1.2.1	Zeile 117f	GE	Die Definition, was ein Smart Metering System darstellt, sollte hier aus Gründen der Unabhängigkeit des Gateway PP unterbleiben. Andernfalls sollte eindeutig darauf hingewiesen werden, dass diese Definition nur für das Gateway PP Gültigkeit besitzt.	The following figure provides an overview over the TOE as part of <b>the household's Smart Metering Components.</b>

## SmartMeter PP - Kommentierungsverfahren

Bitte als ODT- oder Word-Datei (bitte kein PDF) senden an: [smartmeter@bsi.bund.de](mailto:smartmeter@bsi.bund.de)

1	2	3	4	5	6
Ild Nr.	Kapitel/ Unterkap./ Anhang	Absatz / Abb./Tab./ Note	Art	Kommentar (Begründung/Hintergrund)	Änderungsvorschlag (bitte so konkret wie möglich)
2.	1.2.1	Zeile 124ff	TE	Beschreibung des Gateways bezieht sich auf eine spezifische Umsetzung des Gateways. Die in diesem Absatz genannten Funktionen (Speicherung und Verarbeitung von Zählerdaten; It collects and stores the records from E-Meter(s) and ensures that only authorised parties have access to them or derivates thereof.) geben eine Implementierung eines Gateways wieder. Andere Ansätze (Gateway als Protokollumsetzer von Ende-zu-Ende-signierten und -verschlüsselten Daten) werden nicht betrachtet.	The Gateway (as defined in this PP) serves as a <b>physical</b> communication component between the components in the network of the consumer and the outside world. It can be seen as a special kind of firewall dedicated to the smart metering functionality. It collects <b>and stores</b> the records from E-Meter(s) and ensures that only authorised parties have access to them or derivates thereof. <b>Any relevant information sent by the gateway will be signed and encrypted.</b>
3.	1.2.1	Zeile 126ff	GE	Die Speicherung und Weiterverarbeitung von personenbezogenen Zählerdaten erfolgt unter der Hoheit des Messtellenbetreibers. Eine verpflichtende Verarbeitung der Daten auf einem Gerät des Messtellenbetreibers im Haushalt des Kunden bringt keinen zusätzlichen Schutz der Daten vor unberechtigter Einsicht gegenüber der Speicherung von Daten auf zentralen Systemen.	
4.	1.2.1	Zeile 136ff	TE	Die feste Vorgabe der Verwendung eines Security Moduls in Form einer Smart Card ist für einfache Gateways (ohne Speicherung, ohne Ver-/Entschlüsselung von Zählerkommunikation) aus Sicherheitssicht überdimensioniert. Die Verwendung des Security Moduls sollte an definierte Funktionen geknüpft werden.	The Gateway and the E-Meter <b>shall</b> each utilise the services of a Security Module (e.g. a smart card) as a cryptographic service provider and as a secure storage for confidential assets <b>based on conditions lined out in this document.</b>
5.	1.2.1	Zeile 155f	GE	„All data transfer between LAN and WAN flows via the Gateway, which makes it an ideal component for placing significant parts of the systems overall security functionality.“ Diese Aussage mag für einzelne Bedrohungsszenarien zutreffen. Für Szenarien der Datenintegrität und des Datenschutzes ist hingegen der Schutz an der Quelle (dem Zähler) vorzuziehen.	Satz streichen oder: „All data transfer between LAN and WAN flows via the Gateway, which makes it an ideal component for placing <b>significant</b> parts of the systems overall security functionality <b>relating to ...</b> “.

## SmartMeter PP - Kommentierungsverfahren

Bitte als ODT- oder Word-Datei (bitte kein PDF) senden an: [smartmeter@bsi.bund.de](mailto:smartmeter@bsi.bund.de)

1	2	3	4	5	6
Ild Nr.	Kapitel/ Unterkap./ Anhang	Absatz / Abb./Tab./ Note	Art	Kommentar (Begründung/Hintergrund)	Änderungsvorschlag (bitte so konkret wie möglich)
6.	1.2.1	Zeile 160ff	GE	Aus den in Zeile 151ff getroffenen Aussagen lassen sich die hier getroffenen Aussagen nicht zwangsweise ableiten. Ein Ansatz, der das TOE als „Firewall“ für die Zähler und Protokollkonverter sieht, den Zählern aber die Funktionen zur starken Signatur und Verschlüsselung der versendeten Daten gibt, setzt ein Security Module im Zähler voraus. Der Nutzen eines weiteren Security Modules im TOE ist hingegen zweifelhaft. Auch gibt dieser Absatz durch die Annahmen, dass der Zähler nur ein Minimum an Sicherheitsfunktionen besitzt und das Gateway die restlichen Funktionen abbildet, eine Implementierungsrichtung vor, die alternative Ansätze unterbindet.	
7.	1.2.1	Zeile 165f	GE	Diese Aussage kann so nicht getroffen werden. Es werden im folgenden eine Reihe von Annahmen getroffen, die nur für bestimmte Technologien, Systeme und Konzepte (z. B. MUCC) zutreffen.	Absatz streichen
8.	1.2.2	Zeile 170ff	GE	Um das PP für möglichst viele Metering-Konzepte anwendbar zu gestalten, sollte von der Möglichkeit ausgegangen werden, dass nur Teile des PP von einem TOE umgesetzt werden. Auch muss davon ausgegangen werden, dass CLS wie Kühlschränke in größerer räumlicher Entfernung zum Zähler stehen, so dass diese nicht an das Smart Meter Gateway (TOE) angeschlossen werden können. Insofern ist die Formulierung in Zeile 170ff so anzupassen, dass sie diesem Gedanken Rechnung trägt.	„Typically, the Gateway will be placed in the household or premises of the consumer <sup>3</sup> of the utility and enables access to local E-Meter(s) (i.e. the device(s) used for measuring the consumption of electric power, gas, water, heat etc.). Controllable Local Systems (i.e. power generation plants, controllable loads such as air condition and intelligent ... <b>may be accessed through the TOE where applicable.</b>
9.	1.2.2	Zeile 177f	ED/ GE	Die „location“ im Sinne eines Ortes der Unterbringung des Gateways wird durch das Bild 1 nicht erläutert. Das „overall Smart Metering System“ wird durch Bild 1 nicht dargestellt. Es wird das Metering-Kommunikationsnetzwerk nur im Haushalt/beim Kunden betrachtet.	The <b>positioning</b> of the Gateway in the <b>household's</b> Smart Metering <b>communication network</b> and the corresponding interfaces are summarised in Figure 1 above.

## SmartMeter PP - Kommentierungsverfahren

Bitte als ODT- oder Word-Datei (bitte kein PDF) senden an: [smartmeter@bsi.bund.de](mailto:smartmeter@bsi.bund.de)

1	2	3	4	5	6
Ild Nr.	Kapitel/ Unterkap./ Anhang	Absatz / Abb./Tab./ Note	Art	Kommentar (Begründung/Hintergrund)	Änderungsvorschlag (bitte so konkret wie möglich)
10.	1.2.4	Zeile 183f	ED	Die ursprüngliche Formulierung („The TOE shall be the complete Gateway, comprising the hardware and software/firmware running on this hardware.“) ist nicht ganz eindeutig, da mit dem Ausdruck „the complete gateway“ mehrere Sachverhalte beschrieben werden können.	The TOE shall comprise both hardware and software/firmware running on this hardware.
11.	1.2.5.1	Zeile 207	TE	Die Anforderung, dass Daten nur gepollt, d.h. aktiv durch das TOE abgefragt werden dürfen, ist nicht vereinbar mit dem Einsatz von Funktechnik in batteriebetriebenen Zählern (Gas, Wasser, Wärme), da diese aus Gründen der Energieeffizienz nur in bestimmten Intervallen eigenständig Daten an das TOE übertragen. Die Anforderung aus Zeile 207 ist von diesen Zählern nicht zu erbringen, was den Einsatz von drahtgebundenen Auslesetechnologien effektiv vorschreibt. Damit ist diese Vorgabe nicht mehr technologieneutral.	the Gateway shall <del>poll</del> accept data (e.g. metering data) from authorised E-Meters only
12.	1.2.5.1	Zeile 216	TE	Die Anforderung, wie die Zählerdaten signiert sein sollten, ist an den Zähler zu richten. Nur durch die Signatur der Daten im Zähler kann die Integrität von Ende zu Ende sichergestellt werden (siehe Anforderung Teile 220ff).	Streichen und als Anforderung an den Zähler aufnehmen
13.	1.2.5.1	Zeile 217	TE	Die Anforderung, die Daten im TOE zu pseudonymisieren, kollidiert mit der Signaturanforderung aus Zeile 216. Die Signatur ist nur sinnvoll, wenn sie auch eine eindeutige Adresse gebunden ist. Die Pseudonymisierung (Änderung der eindeutigen Adresse) würde die Signatur des Zählers brechen,	Streichen und Pseudonymisierung als Anforderung an den Zähler aufnehmen

## SmartMeter PP - Kommentierungsverfahren

Bitte als ODT- oder Word-Datei (bitte kein PDF) senden an: [smartmeter@bsi.bund.de](mailto:smartmeter@bsi.bund.de)

1	2	3	4	5	6
Ild Nr.	Kapitel/ Unterkap./ Anhang	Absatz / Abb./Tab./ Note	Art	Kommentar (Begründung/Hintergrund)	Änderungsvorschlag (bitte so konkret wie möglich)
14.	1.2.5.1	Zeile 225	TE	<p>Die Feststellung, dass das TOE eine Schnittstelle zum Kunden anbietet, ist nicht für alle Arten von Metering Gateways gegeben. Alternative Ansätze, wie die Implementierung der Kundenschnittstelle in anderen Systemen werden hierbei ignoriert.</p> <p>Auch werden mit dieser Schnittstelle Probleme, wie die räumliche Trennung zwischen Wohnung und Keller (besonders problematisch bei Mehrfamilienhäusern, wo mehrere Stockwerke zwischen Wohnung und Keller liegen können) ignoriert. Ein Anschluss eines oder mehrerer Kunden an diese Schnittstelle birgt neben stark erhöhtem technischen Aufwand weitere Sicherheitsrisiken.</p>	<p>„The TOE <b>may offer</b> an interface to the consumer ...“</p> <p>Betrachtung der Sicherheit eines User-LANs (an IF_GW_U) hinzufügen.</p>
15.	1.2.5.3	Zeile 242ff	TE	<p>Die Überprüfung von Authentizität und Integrität der Zählerdaten muss an der Datensenke, in der die Weiterverarbeitung stattfindet, durchgeführt werden. Eine Prüfung auf dem TOE ersetzt nicht die Prüfung in zentralen Systemen im Sinne einer Ende-zu-Ende-Überprüfung. Eine Prüfung auf dem TOE hat allenfalls Filterfunktionen, die zu einer Reduzierung des Datenverkehrs beitragen, aber nicht zur Sicherheit des Systems.</p>	<p>Satz anfügen: „Alternatively the verification shall be done by the intended data recipient.“</p>
16.	1.2.5.3	Zeile 246ff	TE	<p>Diese Anforderung ist nur für die Verbreitung kryptografisch ungesicherter Daten (keine Signatur) notwendig oder wenn der Empfänger die Sicherung der Daten nicht überprüfen kann (nicht das passende Zertifikat). Bei gesicherten Zählerdaten (siehe Zeile 242ff) kann durch die „external party“ die Integrität der Zählerdaten direkt festgestellt werden.</p>	<p>Satz anfügen: „This provision only applies to data not already protected as described in the section above. Cryptographically signed data (e.g. signed meter data), which can be verified by the intended recipient may be exempted.“</p>
17.	1.2.5.4	Zeile 266f	TE	<p>Die Sicherheit des User Interfaces vor Angriffen durch den Consumer wird nicht betrachtet. Es sollte an dieser Stelle von den gleichen Gefahren durch den Kunden wie durch das WAN ausgegangen werden, da der hinter dem Kunden-Interface hängende PC potenziell von dem gleichen Angreifer wie im WAN bereits kompromittiert wurde.</p>	<p>Sicherheitsbetrachtung User-Interface (IF_GW_U) durchführen</p>

## SmartMeter PP - Kommentierungsverfahren

Bitte als ODT- oder Word-Datei (bitte kein PDF) senden an: [smartmeter@bsi.bund.de](mailto:smartmeter@bsi.bund.de)

1	2	3	4	5	6
Ild Nr.	Kapitel/ Unterkap./ Anhang	Absatz / Abb./Tab./ Note	Art	Kommentar (Begründung/Hintergrund)	Änderungsvorschlag (bitte so konkret wie möglich)
18.	1.2.5.4	Zeile 266f	TE	Diese Anforderung ist nicht technologie-neutral gestaltet. Es gibt eine Reihe von Gründen, den Verbindungsaufbau mit dem Gateway vorzusehen, z. B. manuelle Zählerablesung durch den Kunden, externe Steuerung von/Einwirkung auf Dezentrale Energieerzeugungsanlagen und Großverbraucher (Nachtspeicheröfen, Klimaanlage, Erdwärmepumpe, ...), Übertragung von kurzfristigen Energieangeboten, lokale Optimierung in der Niederspannungszelle. Ein Smart Grid Gateway muss diese Funktionen anbieten können.	Absatz streichen
19.	1.2.5.4	Zeile 269f	TE	Der Einsatz von verschlüsselten Verbindungen im LAN bzw. WAN (link encryption) für die Datenübertragung verschlüsselter Information (z. B. verschlüsselter Zählerdaten; end-to-end encryption) bringt keine oder nur eine sehr geringe Erhöhung der Sicherheit.	„only cryptographically-protected (...) <b>data shall be transmitted.</b> “
20.	1.2.5.4	Zeile 269f	TE	Die Gegenseitige Authentifizierung ist im LAN bei Zählern mit Funk-schnittstelle (z. B. Wireless M-Bus) nicht möglich (Energieeffizienz bei batteriebetriebenen Zählern). Die Anforderung der gegenseitigen Authentifizierung ist daher nicht technologie-neutral umzusetzen.	„only cryptographically-protected (i.e. encrypted and <b>mutually</b> authenticated) <b>data shall be transmitted.</b> “
21.	1.2.5.4	Zeile 269f	GE	Zur Zeit sind keine geeigneten Zählerprotokolle für gegenseitige Authentifizierung und Signierung von Zählerdaten vorhanden. Eine verpflichtende Zertifizierung nach CC ohne ein sicheres Zählerprotokoll führt zu herstellerspezifischen, inkompatiblen Lösungen. Der Einsatz von Zählern verschiedener Hersteller und damit offenen Lösungen wird damit unterbunden.	Schutzprofil Zähler erstellen.
22.	1.2.6	Zeile 290 Table 1	TE	Diese Tabelle erscheint auch als nicht vollständig. So ist z. B. die geschützte Kommunikation mit dem E-Meter nicht erwähnt.	Genauer spezifizieren, welche Schlüssel gespeichert werden: z. B. Kpub-e-meter

## SmartMeter PP - Kommentierungsverfahren

Bitte als ODT- oder Word-Datei (bitte kein PDF) senden an: [smartmeter@bsi.bund.de](mailto:smartmeter@bsi.bund.de)

1	2	3	4	5	6
Ild Nr.	Kapitel/ Unterkap./ Anhang	Absatz / Abb./Tab./ Note	Art	Kommentar (Begründung/Hintergrund)	Änderungsvorschlag (bitte so konkret wie möglich)
23.	3.1	Zeile 308f	GE	Die Beschreibung des Systems als E-Meter und Gateway beschreibt eine Lösung für Smart Metering. Alternative Lösungen (z. B. Kunden-Web-Portal) werden in dieser Systembeschreibung nicht betrachtet. Folglich ist auch die Auflistung der „external parties“ auf die betrachtete Systemlösung zugeschnitten.	„The following external parties <b>may</b> interact with the <b>system consisting of</b> E-Meter and Gateway .“
24.	3.1	Zeile 311 Local Attacker	TE	Der Angreifer über das User-Interface wird in dieser Auflistung nicht betrachtet. Das User-Interface ist ebenso wie die anderen Schnittstellen zu betrachten. Es ist u. U. (je nach Angreiferbild und Systemimplementierung) die einfachste Möglichkeit des Angriffs auf das TOE.	Attacker having physical access to E-Meter, <b>User</b> , Gateway or a connection between these components, trying to disclose or alter metering data or configuration data (including software updates) downloaded by E-Meter or Gateway.
25.	3.5	Zeile 332 OSP.Log	TE	Die Anforderungen an das TOE im Bezug auf die Aufzeichnung von Ereignissen, Informationsflüssen, Zählerdaten und die Anzeige dieser Daten für den Kunden geben erneut eine Implementierung des Smart-Metering-Systems vor.  Die Speicherung und Anzeige der Zählerdaten und Loginformationen zur Kontrolle durch den Kunden setzt eine Kundenschnittstelle (IF_GW_U) am TOE voraus.  Zusätzlich werden mit der OSP.Log die Funktionen der Kontrolle der ordnungsgemäßen Funktion des Geräts mit der Überwachung der Abrechnung vermengt. Hier sollte eine deutliche Trennung dieser Funktionen erfolgen. Die Abrechnungskontrolle kann durch die signierten Zählerdaten auch an anderer Stelle (z. B. Webportal) erfolgen.	Trennung zwischen Administrator und Consumer  Letzten Absatz streichen oder umformulieren (nicht technologieneutral)
26.	3.6	Zeile 335 O.Conceal	GE	O.Conceal ist im Kontext des PP nicht notwendig. Das TOE sendet regelmäßig (per Policy) Daten nach außen. Die übertragenen Daten sind Zählerstände und damit keine Daten, die eine variable Länge haben. Auch wird bei kryptografischen Verfahren mit Blockarbeitsweise, (wie z. B. AES) ein Datenpaket durch Padding auf die benötigte Blockgröße aufgebläht.	O.Conceal löschen

## SmartMeter PP - Kommentierungsverfahren

Bitte als ODT- oder Word-Datei (bitte kein PDF) senden an: [smartmeter@bsi.bund.de](mailto:smartmeter@bsi.bund.de)

1	2	3	4	5	6
Ild Nr.	Kapitel/ Unterkap./ Anhang	Absatz / Abb./Tab./ Note	Art	Kommentar (Begründung/Hintergrund)	Änderungsvorschlag (bitte so konkret wie möglich)
27.	3.6	Zeile 335 O.Firewall	GE	Kryptografische Verfahren werden in IT-Systemen nicht durch Firewalls realisiert. Firewalls kommen in der Regel auch komplett ohne Kryptografie aus. Der Sinn dieser Forderung erschließt sich nicht.	Punkt löschen
28.	3.6	Zeile 335 O.Meter	TE	Zu Punkt 4: Die Kumulierung von Daten im Gateway gibt bereits eine Lösung vor, die unter anderem die Verarbeitung der Daten im Gateway vorsieht. Die datenschutzrechtliche Argumentation, dass die Verarbeitung der Daten im Haus erfolgen soll, erscheint in Anbetracht der Tatsache, dass das TOE unter der Kontrolle des Messtellenbetreibers steht, als „privacy theatre“, bei dem dem Kunden suggeriert wird, seine Daten wären im Haus sicherer. Die Annahmen in Bezug auf den Messtellenbetreiber (A.TrustedAdmins) können so auch an ein zentrales System im Einflussbereich des Messtellenbetreibers gestellt werden	<ul style="list-style-type: none"> <li>the TOE shall deliver the <b>cumulated</b> data to the authorised external parties as defined in the corresponding access control profiles,</li> </ul>
1.	3.7	Zeile 332 OSP.SM	TE	Der zwingende Einsatz eines Security Modules (z. B. Smart Card) im TOE für Gateways ohne Bedarf an starker Kryptographie (alternative Implementierung) als überdimensioniert und unwirtschaftlich betrachtet.	z. B. Satz anfügen: „This OSP only applies to TOE storing with the following properties: storage, management and generation of cryptographic keys; generation and/or verification of digital signatures for metering data; storage and cumulation of metering data; ...“
2.	3.7	Zeile 332 OSP.SM	GE	Die zwingende Voraussetzung eines Security Modules in Form einer Smart Card setzt einen weiteren Entwicklungszyklus bei den Herstellern voraus. Neben den erhöhten Kosten, die den Einsatz von Smart Metering unrentabel machen, bedeutet der Einsatz von HW-Security-Modules voraussichtlich ein Verschiebung der Verfügbarkeit erster zertifizierter TOE und damit den Ausbau von Smart Metering Systemen um mehrere Jahre.	Sicherheitsgewinn durch Security Modules überdenken, Übergangszeit für TOE ohne Smart Card schaffen

## SmartMeter PP - Kommentierungsverfahren

Bitte als ODT- oder Word-Datei (bitte kein PDF) senden an: [smartmeter@bsi.bund.de](mailto:smartmeter@bsi.bund.de)

1	2	3	4	5	6
Ild Nr.	Kapitel/ Unterkap./ Anhang	Absatz / Abb./Tab./ Note	Art	Kommentar (Begründung/Hintergrund)	Änderungsvorschlag (bitte so konkret wie möglich)
3.	3.8.2.1	Zeile 352ff	TE	<p>Grundsätzlich bietet Verschlüsselung keinen Schutz der Datenintegrität. Diese wird nur durch integritätssichernde Massnahmen wie Signaturen sichergestellt.</p> <p>Das Gateway hat bei Funkschnittstellen aus Energieeffizienzgründen keinen Einfluss auf die Verbindung und kann damit auch keine Verschlüsselung durchsetzen. Auch ist es nicht zwingend notwendig, die Integritätssicherung nur zwischen TOE und E-Meter stattfinden zu lassen. Eine Ende-zu-Ende-Signatur bietet Schutz vor Datenveränderungen sowohl lokal (T.DataModificationLocal) als auch im WAN (T.DataModificationWAN).</p>	Signierung von Zählerdaten als Anforderung an Zähler (Meter PP) aufnehmen
4.	3.8.2.2	Zeile 363ff	TE	<p>Grundsätzlich bietet Verschlüsselung keinen Schutz der Datenintegrität. Diese wird nur durch integritätssichernde Maßnahmen wie Signaturen sichergestellt.</p> <p>Nur eine Ende-zu-Ende-Signatur bietet Schutz vor Datenveränderungen sowohl lokal (T.DataModificationLocal ) als auch im WAN (T.DataModificationWAN).</p>	
5.	3.8.2.5	Zeile 393ff	TE	<p>Bei einfachen, energieeffizienten Funktechnologien aus dem Metering-Bereich besteht kein Einfluss auf die Verbindung und deren Sicherheit, da kein verbindungsorientiertes Protokoll verwendet wird.</p> <p>Auch für die Verschlüsselung von Zählerdaten muss festgestellt werden, dass eine Ende-zu-Ende-Verschlüsselung vor beiden Bedrohungsszenarien T.DisclosureWAN und T.DisclosureLocal schützt. Anders als bei der Signatur kann hierbei allerdings keine Verarbeitung der Daten auf dem TOE erfolgen.</p>	<p>Verschlüsselung von Zählerdaten als Anforderung an Zähler aufnehmen</p> <p>Absatz aufnehmen: „Alternatively, the handling and buffering of encrypted data received through one of the LAN interfaces (IF_GW_CLS, IF_M_GW) without decryption counters this threat.</p>