

Stellungnahme zur Diskussion der Informationssicherheit im Smart Grid

(Stand 10.2011)

Über den Arbeitskreis „Internet der Energie“ (BDI IdE)

Wir sind ein spartenübergreifend sowie interdisziplinär agierendes Expertengremium der deutschen Industrie und Wissenschaft, das sich seit 2007 mit dem Themenkomplex Internet der Energie („IdE“) beschäftigt. Wir haben fundiertes Wissen und denken ideologiefrei in die Zukunft. Wir sind davon überzeugt, dass die Weiterentwicklung unseres Energiesystems gerade auch nach den politischen Entscheidungen zur zukünftigen Energieerzeugung in Deutschland und im Hinblick auf das Erreichen der Klimaschutzziele eine wesentlich stärkere Vernetzung mit Informations- und Kommunikationstechnologien (IKT) notwendig macht. Unser Auftrag ist das Internet der Energie mit dem Anspruch höchstmöglicher Effizienz zwischen Erzeugung und Verbrauch zu fördern und eine ganzheitliche Wirkungsanalyse (des Internet der Energie) vorzunehmen: Wir definieren Rahmenbedingungen für Smart Grids und erstellen Zeitpläne, leiten daraus Handlungsempfehlungen ab und skizzieren Maßnahmen zur Umsetzung. Wir leisten Aufklärung für Politik, Wirtschaft, Wissenschaft und die interessierte Öffentlichkeit. Als Fachexpertengremium vertreten wir eine unabhängige Position. 2008 veröffentlichten wir unsere erste Broschüre „IKT für die Energiemärkte der Zukunft – Die Energiewirtschaft auf dem Weg ins Internetzeitalter“, abrufbar auf der Homepage www.bdi-ide.de.

1. Hintergrund der Stellungnahme

Am 26. August 2011 hat das Bundesamt für Sicherheit in der Informationstechnik (BSI) das Schutzprofil Version 1.1.1 publiziert. Es beinhaltet den finalen Entwurf für Konformitätsanforderungen für die Kommunikationseinheit eines Messsystems nach Energiewirtschaftsgesetz (EnWG). Zudem hat das BSI die Veröffentlichung einer technischen Richtlinie für den Oktober in Aussicht gestellt.

Bei dieser Publikation handelt es sich um wesentlich mehr als nur einen technischen Vorschlag für eine einzelne Komponente des künftigen Energiesystems. Vielmehr werden hier mit der Public-Key-Infrastruktur und neuen Systemanforderungen entscheidende Weichen für die Architektur, Rollen und auch die Kosten der Smart Grid-/ Metering-Systeme beziehungsweise des Internet der Energie gestellt. Damit werden auch die anstehenden Kosten-Nutzen-Analysen der Politik und der Unternehmen unmittelbar beeinflusst. Etwaige massive Kostenerhöhungen und Einschränkungen in den Systemarchitekturen sowie Geschäftsmo-

dellen könnten die Entwicklung hin zu einem beschleunigten Ausbau des Internets der Energien behindern, wenn nicht sogar verhindern.

Deshalb nehmen wir die BSI-Veröffentlichung zum Schutzprofil zum Anlass, dieses Positionspapier als Beitrag zur Diskussion der Informationssicherheit im künftigen Internet der Energie und zur künftigen Architektur im Smart Grid, insbesondere in Bezug auf Synergien mit dem Smart Metering, zu veröffentlichen.

2. Ziele und Aufgaben des zukünftigen Energiesystems

Unsere Vorschläge ergänzen die im Juni 2011 veröffentlichte Broschüre „Auf dem Weg zum Internet der Energie – Der Wettbewerb allein wird es nicht richten“. Ausgangspunkt für unsere Vorschläge sind die erklärten Ziele der Energiewende:

- (i) **Effizienzsteigerung durch mehr Transparenz**
zeitnahe Anzeige des Stromverbrauchs für Endkunden, häufigere Rechnungsstellung
- (ii) **Intelligente Steuerung der Energieverteilnetze**
Umsetzung dynamischer und preisvariabler Tarife, Steuerungsmöglichkeiten für dezentrale Erzeuger und Speicher, Versorgungssicherheit

Diese Ziele sind ohne die Einführung steuerbarer Betriebsmittel (u.a. Regelbare Ortsstationen, Speicher, Erzeuger) sowie die Ein- beziehungsweise Anbindung von Mess- und Steuerungssystemen über ein Kommunikationsnetz nicht erreichbar. Die Informations- und Kommunikationstechnik auf der Verteilnetzebene und in den Liegenschaften werden damit zur Schlüsseltechnologie für die Weiterentwicklung der Energiesysteme zum Internet der Energie/ Smart Grids. Für die Erreichung dieser Ziele sind die daraus jeweils resultierenden Aufgaben differenziert zu betrachten:

- (i) **Datenerfassung für Abrechnungszwecke (metrologisches Messen)**
zur Abrechnung und für entsprechende Kontrollmöglichkeiten beziehungsweise Verbrauchsanzeigen bei Prosumern und Endkunden
- (ii) **Optimierung der Energieflüsse (Steuern und Regeln)**
im Verteilnetz und in den Liegenschaften mit Blick auf ökonomische, ökologische sowie physikalische Parameter, die Einfluss auf die Versorgungssicherheit beziehungsweise die Netzeffizienz haben

Unter diesen unterschiedlichen Aufgaben ist auch bei der An- und Einbindung der technischen Anlagen und Informationssysteme in den Liegenschaften der Endkunden zwischen zwei Systemen zu unterscheiden: Die metrologischen Informationssysteme und die Systeme, welche die Energieflüsse zur beziehungsweise von der Liegenschaft ins Verteilnetz unmittelbar oder mittelbar steuern.

3. Integration der Smart Grid Aufgaben

Die Arbeitsgruppe erachtet es für außerordentlich wichtig, den Schutz der Privatsphäre angemessen zu behandeln. Die Grundproblematik, wenn Energiekunden per Gesetz verpflichtet werden Daten zu erfassen und weiter zu geben, ist klar. Verständlich ist auch, dass zügig ein erster Ansatzpunkt für die Umsetzung der Datenschutzbemühungen gefunden werden sollte. Ein Schutzprofil für den Smart Meter lag nahe.

Allerdings sieht die Gruppe auch eine ganze Reihe von Herausforderungen, die in den jetzigen Ansätzen nicht adressiert wurden und potentiell zu problematischen Konsequenzen führen. Diese Punkte sollen im Weiteren aufgezeigt werden. Uns ist wichtig, dass diese Kommentare in einem konstruktiven Grundverständnis erfolgen und wir großen Respekt für die Akteure haben, die wegen der beschleunigten Energiewende unter hohem Zeitdruck erste konkrete Impulse setzen möchten. Unsere Anmerkungen verstehen sich als teils kritischer, dabei aber hoffentlich zielführender Beitrag zur Diskussion.

In der Einschätzung der Arbeitsgruppe legt das BSI-Schutzprofil primär Regeln für die Datenerfassung fest und berücksichtigt nur unzureichend die Anforderungen und möglichen Synergien in einem Smart Grid. Insbesondere wird nicht zwischen unterschiedlichen Qualitäten von Smart Meter-Daten unterschieden. Gerade im Hinblick auf die unterschiedlichen Ziele und Aufgaben im Smart Grid kann eine Gleichbehandlung aber das Heben von Synergie- und Effizienzpotentialen behindern.

So sind Verbrauchsinformationen kundenbezogene Daten und müssen deshalb den strengen Anforderungen des Datenschutzes genügen. Neue Tarife sollen den Endkunden helfen, energiebewusster zu werden und energieeffizienter zu handeln. Kundenorientierte Anwendungen (z.B. Informationsportale) mit unterstützender Datenaufbereitung und neuen Diensten sind hierfür ein wichtiger Schlüssel zum Erfolg und zur breiten Akzeptanz.

Dagegen werden für das Netzmonitoring und die Koordination von Steuerungseingriffen in erster Linie anonymisierte technische Informationen und Daten zum Netzzustand ohne direkten Personenbezug benötigt. So können in Smart Grids komplexe Vorgänge in Markt- und Regelprozessen beherrscht und Erzeugung und Verbrauch besser ausbalanciert werden. Zentrale Herausforderung ist das Zugriffsrechte-/Rollenmanagement in den Markt- und Dienstleistungsprozessen und deren regulierungskonforme Abbildung sicher zu stellen um synergetisch die Smart Meter-Infrastruktur sowohl für metrologische als auch für Steuerungsaufgaben nutzbar zu machen.

Hier geht es um ein Gleichgewicht, bei dem das Recht auf informationelle Selbstbestimmung einerseits und der Schutz einer öffentlichen Infrastruktur andererseits berücksichtigt werden muss. Vor diesem Hintergrund sind Architekturen zu entwickeln, die eine Balance zwischen Datenschutz/-sicherheit, der Kosten/Verfügbarkeit der Dienstleistungen und der Energieversorgungssicherheit hervorbringen. Diese sollen zudem für eine Skalierung zukünftiger Smart Grids in der Energieversorgung geeignet sein.

Insgesamt sollte bei der Planung der Infrastruktur auf Datenschutz, Datensicherheit und Datensparsamkeit geachtet werden, ohne jedoch durch technische Limitierungen Innovationen und neue Dienste unbillig zu behindern oder die Kosten unnötig zu erhöhen. Synergien im Bereich der IKT sind vom EnWG gefordert und wünschenswert. Sie müssen jedoch auch

den unterschiedlichen Anforderungen im Smart Metering und im Smart Grid gerecht werden. Für die Kommunikationseinheit des Messsystems enthalten das Schutzprofil und die angekündigte technische Richtlinie des BSI gesetzliche Detailvorgaben und Festlegungen. Sie begrenzen somit die mögliche Vielfalt der einsetzbaren Messsystemvarianten sowie deren Kompatibilität zu europäischen Standards. Ebenso werden Synergien im Zusammenspiel mit Smart Grids eingeschränkt.

4. Architekturen im Internet der Energie

Bei der Gestaltung zukunftsfähiger und regulierungskonformer Strukturen sowie bei etwaigen Synergien sind die Wirkungs- und Eigentumsebenen sowie zukünftige Rollen zu beachten. Neben den Aufgaben ist für die Entwicklung einer effizienten Architektur insbesondere die Betrachtung der Akteure und der Prozesse wichtig. Im Gegensatz zur auf Smart Meter fokussierten Betrachtungsweise des BSI-Schutzprofils gehen wir im Folgenden auf die drei Architekturbausteine im Internet der Energie sowie deren Wechselwirkungen und Synergien ein: Smart Building (Energiemanagement bzw. die Automatisierung im Gebäude), Smart Metering und Smart Grid-Lösungen auf der Nieder- und Mittelspannungsebene.

4.1. Smart Building

Die Inhouse-Steuerung der energieverbrauchenden und -erzeugenden Anlagen erfolgt über ein Energie-Management-Gateway (EM-Gateway) in der Hoheit des jeweiligen Kunden. Weder der Verteilnetz (VNB)- noch der Messstellenbetreiber (MSB) werden unmittelbar in die Energie- oder Informationsvernetzung sowie die Steuerung von Anlagen in den Liegenschaften eingreifen wollen, es sein denn, dies ist zum Beispiel im Fall von Erzeugern oder Speichern technisch notwendig, vom Prosumer gewünscht (u.a. virtuelles Kraftwerk) oder durch Gesetz und Betriebsführungsverträge abgedeckt. Daher muss ein EM-Gateway auch in der Lage sein, Steuerungssignale aus dem Netz umzusetzen und so die vom Netz angestrebte stabilisierende Wirkung eigenständig zu gewährleisten. Hier fehlt es jedoch noch an standardisierten Funktionen und Use-Cases.

Lieferanten setzen Tarifierreize, auf die das EM-Gateway selbstständig reagieren kann. Als Input erhält das EM-Gateway Verbrauchsdaten und aktuelle Messwerte aus dem Zählerbereich sowie Tarifdaten vom Stromlieferanten oder anderen Dienstleistern. Es bietet sich hierbei an, dass Markt-/Tarif- und Verbrauchsdaten über das Internet bereitgestellt werden und so der Endkunde unabhängig von lokalen Strukturen bleibt. Dies ist insbesondere in Mehrfamilienhäusern geboten, in denen die Einrichtung einer exklusiven hausinternen Kommunikation vom Gateway zum Kunden nur aufwändig zu realisieren ist. Das lokale Gateway zur Zählerdatenerfassung verfügt nach BSI-Schutzprofil über eine standardisierte Schnittstelle (CLS-Schnittstelle). Über diese kann der Kunde seine Verbrauchsdaten direkt abrufen.

Der komfortable und aufbereitete Zugang über ein Portal dürfte jedoch für viele Endkunden ein wichtiger Erfolgsfaktor für die Akzeptanz von Smart Metering und auch der Chancen zukünftiger Geschäftsmodelle im Smart Grid sein. Das EM-Gateway ist insofern ein wettbewerbles Produkt, dessen Nutzung frei zwischen Endkunden und Dienstleister zu vereinbaren ist. Rechtliche Vorgaben, zum Beispiel nach EEG, sind hierbei durch die Einhaltung von Standards beziehungsweise technischer Richtlinien zu berücksichtigen. Bei der eigen-

ständigen informationstechnischen Anbindung sind die rechtlichen Vorgaben und entsprechenden Anforderungen an die Informationssicherheit zu berücksichtigen.

4.2. Smart Metering

Gemäß EnWG erfolgt das Auslesen der Zähler über ein lokales Gateway, das alle Zählerdaten eines Hauses erfasst. Hierbei sind eichrechtliche und regulatorische Rahmenbedingungen sowie Datenschutzerfordernungen zu beachten. Die nach Vertrag oder Kundenwunsch zu erhebenden Daten sollten je nach Systemansatz lokal oder in dezentralen Systemen (z.B. Aggregation in der Ortsstation) zwischengespeichert und von dort an autorisierte Adressaten weitergeleitet werden. Dies entspricht dem Systemansatz des BSI-Gateways.

Im dezentralen Ansatz bilden das lokale Gateway und das zum Beispiel in der Ortsstation vorgesehene Modul zur Datenhaltung/-Verarbeitung eine integrierte und IT-seitig abgeschirmte Lösung. Diese wird erst am Datenhaltungsgateway an das WAN angebunden. In der lokalen Variante erfolgt die Datenhaltung dagegen direkt im Haus, so dass hier keine kostensenkenden Synergien wie beim dezentralen Ansatz möglich sind. Der Kunde und die autorisierten Parteien (u.a. Messstellenbetreiber, Lieferant) haben aus dem WAN einen autorisierten, verschlüsselten Zugriff auf das Gateway. Darüber hinaus liefert das Gateway die Daten in einem definierten Rhythmus an den berechnete Empfänger ab.

Der VNB als vertrauenswürdige Stelle beziehungsweise ein MSB, der den VNB oder Dritte mit dieser Aufgabe betraut, erfüllt die Anforderungen des Kunden an einen sicheren Aufstellungsort respektive eine sichere Datenhaltung. Hier sollte dem MSB/VNB mehr Freiheit in der Implementierung eingeräumt werden, um im Sinne einer effizienten Lösung nachhaltige Strukturen im Smart Grid auf zu bauen und Synergien nutzen zu können.

4.3. Smart Grid-System

Im Smart Grid sind primär die zum Netzbetrieb benötigten Systeme auf der Nieder- und Mittelspannungsebene und in Einzelfällen lokale Sensoren und/oder Anlagen (z.B. Einspeiseanlagen) bei Endkunden einzubinden. Ein Smart Grid mit Fokus auf Versorgungssicherheit und Netzstabilität benötigt nicht zwangsläufig Smart Metering und EM-Gateways. Synergien in den Strukturen, zum Beispiel in der IKT, helfen aber die Kosten zu senken. Einerseits setzen viele Geschäftsmodelle auf integrierte Lösungen zum Erreichen einer kritischen Masse, andererseits bauen sie auf Differenzierung und erheben gegebenenfalls sehr divergierende Anforderungen insbesondere an die Leistungsfähigkeit der Kommunikationstechnik. Die Berücksichtigung infrastruktureller Synergien und die regulatorische Abgrenzung von Geschäftsmodellen beziehungsweise Prozessen bilden die Basis für eine nachhaltige Architektur im Smart Grid.

Auf der Niederspannungsebene können Synergien über das lokale Gateway als Interface zum Gebäude gehoben werden. Darüber hinaus können Haushaltszähler auch wichtige anonymisierte Netzdaten für das Smart Grid liefern. In einer kostenoptimierten IKT-Architektur erfolgt der Smart Grid- und der Smart Metering-Zugang zwar bis zum Gebäude auf der physikalisch gleichen IKT, jedoch in logisch getrennten Subnetzen, die den jeweiligen Anforderungen an Protokolle, Datenschutz und Sicherheit gerecht werden. So könnte beispielsweise aus dem Smart Grid eine anonymisierte Information eines Zählers direkt abgefragt werden. Die Smart Grid relevanten Daten haben in vielen Fällen (z.B. Spannungswerte, Phasenwinkel) keine Relevanz für den Messstellenbetreiber und Endkunden, der pri-

mär Verbrauchsdaten erhebt. In diesem Fall ist der Zähler ein lokaler Sensor, auf den der Messstellenbetreiber und der Netzbetreiber mit unterschiedlicher Zielstellung unabhängig, jedoch über die gleiche IKT, zugreifen.

4.4. Synergien zwischen Smart Grid und Smart Metering

Die Architekturbeispiele verdeutlichen, dass Synergien in der IKT-Infrastruktur für Energiesysteme zu heben sind. Hierfür müssen getrennte Marktrollen nicht zwangsläufig zusammengeführt werden müssen. Gleichwohl wird es idealerweise eine bestehende Marktrolle geben müssen, die verbindlich eine gemeinsame IKT für Smart Grid und Smart Metering aufbaut und diese Struktur den anderen Marktrollen diskriminierungsfrei zur Verfügung stellt. Als Betreiber kommen hier grundsätzlich zwei bereits etablierte Marktrollen in Frage: der Messstellenbetreiber und der Verteilnetzbetreiber. Da die Rolle des MSB mit der Zielsetzung für mehr Wettbewerb in diesem Markt geschaffen wurde und somit in einem Verteilnetz mehrere MSB gewünscht sind, scheint es problematisch den Betrieb der Infrastruktur einem einzelnen MSB zu übertragen. Dagegen ist der VNB ohnehin gesetzlich zur diskriminierungsfreien Bereitstellung seiner Infrastruktur verpflichtet. Darüber hinaus kann der VNB durch unmittelbaren und schnellen Zugriff auf alle für den sicheren Netzbetrieb relevanten Informationen eine stabile Energieversorgung gewährleisten.

Systemseitig wird eine sichere bidirektionale IKT-Infrastruktur in jedem Verteilnetz benötigt. Hierbei ist nicht die konkrete technische Ausgestaltung (z.B. DSL, UMTS/GSM, Powerline) festzulegen, sondern lediglich das Kommunikationsprotokoll (z.B. TCP/IP und höhere Protokollebenen). Die konkrete Ausgestaltung der Infrastruktur kann so an regionale Gegebenheiten (Stadt, Land) und vorhandene technische Ausstattung angepasst werden. Die technische Umsetzung muss eine, soweit technisch und wirtschaftlich darstellbar, ausreichende Performance und standardisierte Schnittstellen aufweisen. Über standardisierte Datenprotokolle und Kommunikationsschnittstellen kann der Verteilnetzbetreiber so den Berechtigten rollenspezifisch einen abgesicherten Zugang zu Smart Metern und technischen Anlagen ermöglichen.

Die angestrebten Synergien von Smart Metering und Smart Grid sind jedoch nur dann zu erwarten, wenn aufgrund des regulatorischen Rahmens eine hohe Durchdringung mit einer flächendeckenden IKT erzielt wird. Bei einer Beschränkung des Smart Grid/Metering auf punktuelle Anwendungen wird weder die kritische Masse für flächendeckende IKT-Strukturen noch die für viele Geschäftsmodelle erreicht. Auch eine schleppende Markteinführung hätte ähnliche Effekte, da zunächst nur punktuell aufgebaute Strukturen nur mit hohem Aufwand in flächendeckende Strukturen zu überführen sind.

5. Empfehlungen für die Technische Richtlinie

Für die Einführung von Standards und nachhaltigen Strukturen im Internet der Energie ist die vom BSI erfolgte Festlegung von TCP/IP und Layer-Architekturen als Grundlage der Kommunikation zu begrüßen (vgl. Abbildung 1). So kann bei Entwicklungen der Applikationsentwicklung stets auf die für Kommunikationssysteme wesentlichen Layer Ethernet und TCP/IP zurückgegriffen werden. Gleichzeitig können für das Gesamtsystem bewährte Sicherheits- (TLS) und Managementstandards (SNMP) verwendet werden. Darüber hinaus sind die notwendigen Systemaspekte und Prozessketten Smart Metering und Smart Grid zu beachten und prozessorientierte IKT-Architekturen zu entwickeln.

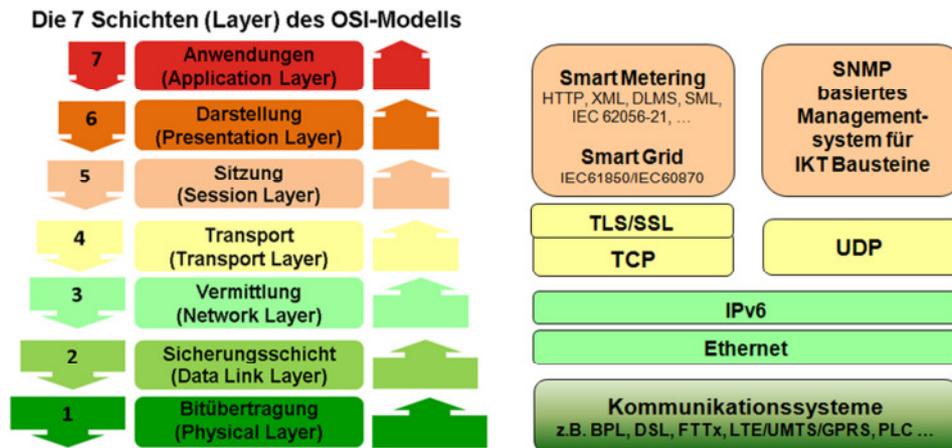


Abbildung 1: Layerarchitektur im Smart Metering, Smart Grid und Systemmanagement

5.1. Schlanker Zertifizierungsansatz

Durch die punktuelle Betrachtung der Kommunikationseinheit des Messsystems dürfen die Freiheiten in der Implementierung nicht in unnötigen Hürden und hohen Kosten für das Smart Meter und Smart Grid-Gesamtsystem resultieren. Smart Grid-Informationssicherheit sollte in einer prozessorientierten Sicht im Smart Grid-Gesamtsystem weiterentwickelt werden. Dabei sollten keine produktorientierten Pflichtzertifizierungen aller technischen Akteure und ihrer aktiven Komponente im Smart Grid notwendig werden, da dies eine Kostenexplosion und Verlust von Innovationsdynamik zur Folge hätte. Der aufwändige Zertifizierungsprozess darf nicht zu einer Hürde für die in der Praxis aufgrund betrieblicher Zwänge und des Lernprozesses stattfindende sukzessive Anpassung der Systeme (z.B. Software, Architekturen) werden. Für etwaige Anpassungen zertifizierter Komponenten muss ein einfacher und preiswerter Prozess zur erneuten Zertifizierung gefunden werden.

5.2. Vermeidung von Smart Metering-Insellösung

Für Netzsteuerungszwecke werden in Smart Grids technische Daten aus dem Nieder- und Mittelspannungsnetz (u.a. Spannung, Frequenz, $\cos \varphi$) hinzukommen und in den Netzleitständen oder in lokalen Regelkreisen verarbeitet. Für diese komplexeren Regelungsprozesse sowie für die Umsetzung spezieller Protokolle werden leistungsfähige IKT-Strukturen (z.B. transparente Ethernetzugänge) benötigt. Diese Daten müssen in Echtzeit verfügbar sein um gegebenenfalls direkt steuernd eingreifen zu können. So beruht ein Smart Grid gemäß ENTSO-E oder ACER zum Beispiel auf lokalen Echtzeitdaten zum Netzzustand und einem Zugang zu jedem Erzeuger. In diesen Fällen werden technische Daten von Smart Meter ohne jeden Personenbezug in Aspekte der Netzsteuerung eingebunden. BSI-Gateways

unterstützen gegebenenfalls diese Belange der Versorgungssicherheit nur unzureichend oder aus dem Schutzprofil resultierende Einschränkungen beeinträchtigen die Smart Grid-Fähigkeit der IKT.

Anforderungen an Smart Grid und Smart Metering sind auch bei gemeinsamen IKT-Strukturen getrennt zu betrachten und geeignete, gegebenenfalls logisch getrennte Strukturen/Dienste, sind zu implementieren. Dies ermöglicht auch den Einsatz der unterschiedlichen standardisierten Protokolle für Metering-Systeme und Smart Grid-Systeme. Offen ist in diesem Zusammenhang auch die zukünftige Beziehung zwischen Anschlussnehmer und Anschlussnutzer auf der einen und dem Netzbetreiber und Messstellenbetreiber auf der anderen Seite. Anforderungen des Netzbetreibers an den Anschlussnehmer können zum Beispiel bei Demand Response nur vom Anschlussnutzer oder der von ihm beauftragten Dienstleister bedient werden.

5.3. Flexibilität im Datenhaltungsansatz

Die Erhebung von Verbrauchsdaten durch Smart Meter unterliegen dem Selbstbestimmungsrecht des Kunden und werden dezentral bei den jeweiligen Vertragspartnern (z.B. MSB, Kunde, Anschlussnutzer) gespeichert. Das bedeutet jedoch nicht, dass diese persönlichen Daten nur ausschließlich im Haus datenschutzkonform abgelegt werden können. Der MSB beziehungsweise im Auftrag der VNB als „Datentreuhänder“ könnte aus Effizienzgründen Daten auch an geeigneten dezentralen Orten sicher speichern und so dezentrale Gebiete kosteneffizient ohne Einschränkung des Datenschutzes auf ein BSI-Gateway bündeln. Darüber hinaus können dem Endkunden so die Daten kostengünstiger und leichter über leistungsfähige Portale verfügbar gemacht werden. Ein zusätzlicher hausinterner Zugang (über CLS) sollte zwar möglich sein, wird aufgrund der Zusatzkosten und Restriktionen jedoch eher die Ausnahme sein. Kundenfreundliche Portallösungen mit Zusatzangeboten (Benchmarks, Analysen, Visualisierung) würden auch die Akzeptanz erhöhen. Hier müssen die technischen Richtlinien zum BSI-Schutzprofil Implementierungsvarianten offen und den Kundennutzen im Fokus halten. Smart Metering ist kein Selbstzweck. Als ein Hilfsmittel muss es effizient und komfortabel nutzbar sein und dem nachhaltigen Internetservices-Trend gerecht werden.

5.4. Effiziente Lösungen für Mehrfamilienhaushalte

Die Verwendung der BSI konformen Kommunikationseinheit des Messsystems im Mehrfamilienhaus ist aufgrund der Anforderungen an die liegenschaftsinterne Vernetzung und an das Management des Gateways sehr komplex. Weiterhin kann diese Einheit nicht sinnvoll für die Steuerung von Geräten und Anlagen in den Unterstrukturen der Liegenschaften (Einsatz als singuläres Energiemanagement Gateway für alle Privatbereiche) eingesetzt werden, da es außerhalb des Hoheitsgebietes des einzelnen Endkunden liegt. So müsste es für mehrere Parteien im Haus in deren private Anlagen eingreifen. Hier wären Eigentums-/Hoheitssphären eines Gateways, der Indoor-Kommunikation und die Wohnungshoheit des Kunden nicht mehr sinnvoll zusammenzubringen. Darüber hinaus wären Betreiberaufgaben (z.B. Intra-Netz) nur schwer abzugrenzen. Es ist deshalb zu erwarten, dass die Vielzahl der EM-Gateways unabhängig von der Kommunikationseinheit der Messsysteme standardmäßig in der Hoheit des Endkunden der einzelnen Privatbereiche innerhalb der Liegenschaften betrieben werden und diese die Kommunikation direkt mit den verschiedenen Marktakteuren (z.B. MSB, Energiedienstleister/Lieferant) über das WAN/Internet betreiben.

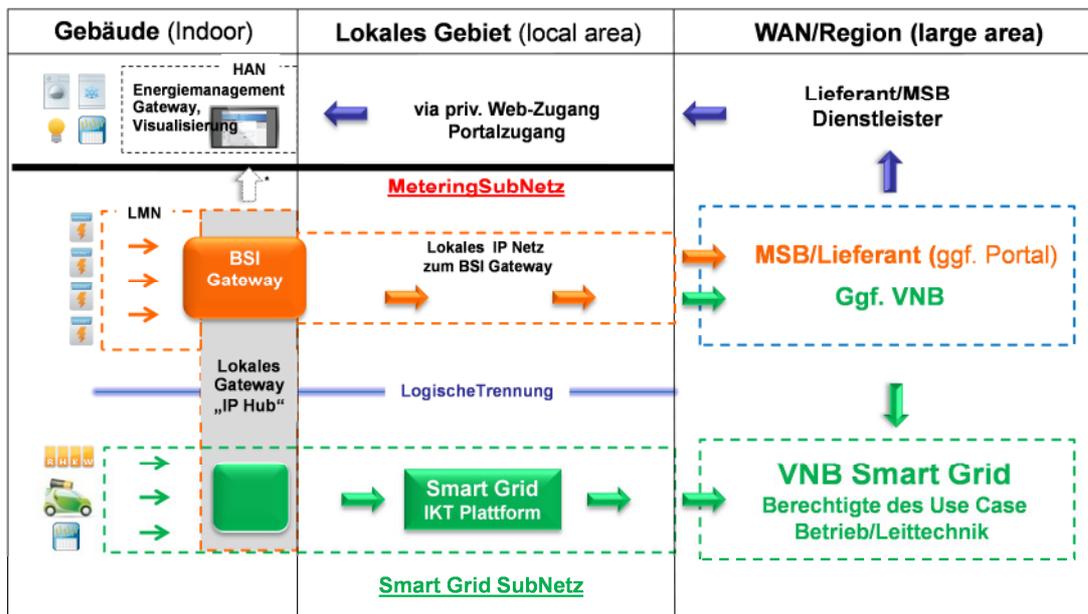
5.5. Vorschläge für eine effiziente Architekturausgestaltung

Im BSI-Schutzprofil werden diese unterschiedlichen Anforderungen und die Wechselwirkungen der Systembereiche nicht ausreichend berücksichtigt sowie mögliche Implementierungsvarianten zu stark eingeschränkt. Dabei bieten moderne IKT-Lösungen durchaus Optionen für datenschutzkonforme und gleichzeitig effiziente Architekturen, die auch den Anforderungen eines Smart Grid gerecht werden. Als Beispiel ist in Abbildung 2, Seite 10, eine IKT-Plattform dargestellt, bei der eine integrierte IKT-Struktur sowohl die Belange des BSI-Schutzprofils erfüllt als auch den Zugang für Smart Grids ermöglicht. Durch konsequente Anwendung der IP-Layerstrukturen können auf einer physikalischen IKT-Infrastruktur logisch getrennte Subnetze abgebildet sowie die Protokolle und Anforderungen der jeweiligen Anwendung optimal bedient werden. Das Energie-Management-Gateway erhält seine Daten aus dem WAN (Internet) und der Endkunde kann als autorisierte Person den „Wake-up-Service“ des BSI-Gateways nutzen, um in Echtzeit aktuelle Verbrauchsdaten abzurufen. Durch Verlagerung des BSI-Gateways über eine „External Communication“ in das lokale Gebiet können die Kosten hierfür gesenkt und die Sicherheit erhöht werden. Das lokale Gateway muss als „IP-Brücke“ nur wenige Anforderungen und keine Datenverarbeitungsvorgänge erfüllen und die IKT-Struktur vom lokalen Gateway zum BSI-Gateway kann gut abgesichert und gehärtet werden. Eine Verlagerung des BSI-Gateways in das Gebäude ist ebenfalls möglich, jedoch deutlich teurer und weniger flexibel als eine dezentrale Lösung. In diesem Fall dient die lokale IKT-Struktur bis zum Gebäude als Verlängerung (BSI-Schutzprofil: „External Communication“) des WAN, im Smart Grid-Bereich ändert sich nichts.

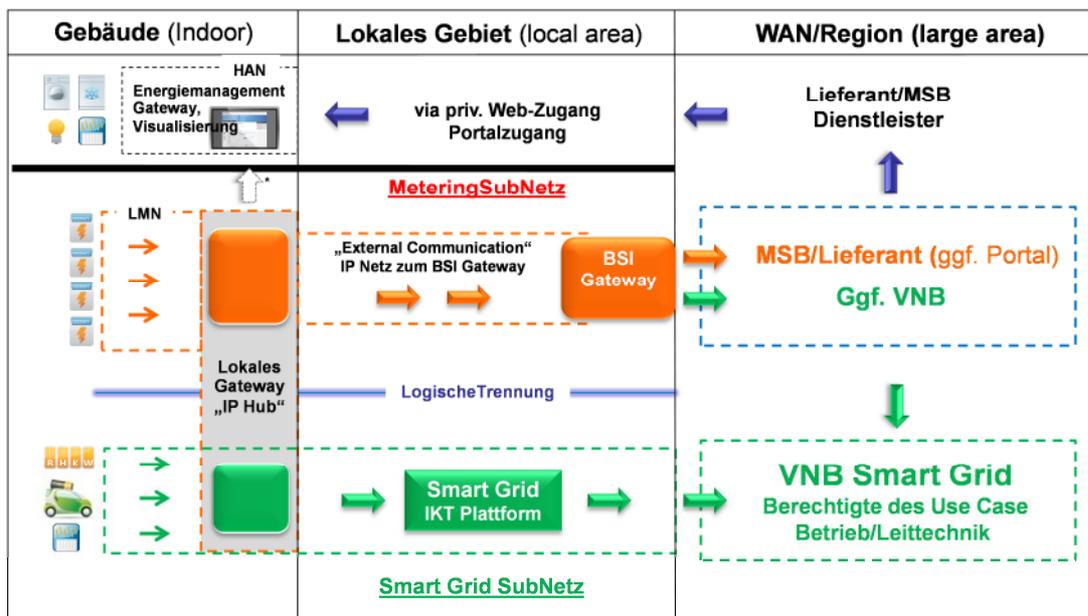
5.6. Methodische Anmerkungen

Das BSI-Schutzprofil spezifiziert Anforderungen an eine Komponente des zukünftigen Energiesystems. Die Sicherheit einer solchen Komponente muss aber in Beziehung gesetzt werden zu den Kernprozessen, die über diese Komponente abgewickelt werden. In welchem Maß das vorgeschlagene Profil tatsächlich zum Schutz der Privatsphäre führt, kann erst beurteilt werden, wenn es im Kontext kritischer Geschäftsprozesse gesehen wird. Wir schlagen vor, drei Kernprozesse als „Nagelprobe“ genauer zu betrachten: den Lieferantenwechsel, einen technischen Schaltprozess zur Stabilisierung eines Netzbereichs und den Software-Update-Prozess. Es würde über den Umfang und das Ziel dieses Papiers hinausgehen, dies hier im Detail auszuführen, wir regen an, diese Analyse ausführlich durchzuführen und zu prüfen, ob es bei diesen Prozessen nicht noch größere datenschutzrechtliche Risiken gibt. Weiterhin ist es methodisch wichtig, Angriffsszenarien systematisch zu beschreiben und das Gesamtsystem daraufhin zu überprüfen. Das System ist nicht sicherer als sein schwächstes Glied; ein „Over-Engineering“ einzelner Komponenten führt gegebenenfalls nur zu hohen Kosten und Barrieren, ohne den Schutz der Daten nachhaltig zu gewährleisten.

Abbildung 2: Exemplarische Implementierungen: Eine IKT-Infrastruktur mit Hausanschluss über ein lokales Gateway „Haus-IP-Hub“, auf der logisch getrennt Subnetze für Metering [(a) mit bzw. (b) ohne „External Communication“ zum BSI-Gateway] und Smart Grid betrieben werden.



a) Ohne „External Communication“ zum BSI-Gateway



b) Mit „External Communication“ zum BSI Gateway