Nachweisbarkeit in Smart Grids auf Basis von XML-Signaturen

Jochen Saßmannshausen[1] · Christoph Ruland[2]

Universität Siegen
[1]Jochen.Sassmannshausen@student.uni-siegen.de
[2]Christoph.Ruland@uni-siegen.de

Zusammenfassung

Als Smart Grids, bzw. intelligente Energienetze werden Energienetze bezeichnet, in denen verschiedene Vorgänge automatisiert werden, und die Komponenten des Systems in der Lage sind, miteinander zu kommunizieren und Daten auszutauschen. Darüber hinaus können Vorgänge aus der Ferne von verschiedenen Instanzen gesteuert werden. In diesem Beitrag wird der Fokus auf die Sicherheit in der Kommunikation gelegt. Es werden verschiedene Standards vorgestellt, wobei der Standard IEC 61850 im Mittelpunkt steht. Ursprünglich für die Automatisierung von einzelnen Schaltanlagen konzipiert, soll der Standard aufgrund der Flexibilität seiner Protokolle und Konzepte in weiteren Szenarien eingesetzt werden. Durch die neuen Anwendungsgebiete entstehen neue Sicherheitsanforderungen, welche nicht mit den bestehenden Sicherheitsmaßnahmen erfüllt werden können. Wichtige Anforderungen sind dabei die Nachweisbarkeit von Handlungen und Authentizität des Ursprungs von Daten. In diesem Beitrag wird ein Konzept basierend auf XML-Signaturen vorgestellt, mit dem die weiteren Sicherheitsanforderungen erfüllt werden können.

1 Einleitung

Hauptmerkmale der bisherigen Energieversorgung sind eine zentrale Bereitstellung der Energie durch leistungsstarke Kraftwerke, ein Hochspannungsnetz, über welches die Energie verteilt wird, und eine zentralisierte und damit vergleichsweise einfache Steuerung des Systems. Die Verbraucher spielen in dem System nur eine passive Rolle. Durch den Trend zur dezentralen Energieversorgung ändern sich die Struktur der Energienetze und die Anforderungen an diese; so gibt es nun eine Vielzahl kleinerer und eventuell inhomogener Stromerzeuger, die den erzeugten Strom auch direkt in die Niederspannungsnetze einspeisen, z.B. Windkraftanlagen, Photovoltaikanlagen oder Blockheizkraftwerke. Diese Komponenten müssen optimal in das Netz eingebunden werden, sodass einerseits die Energieversorgung gesichert ist, andererseits jedoch das Netz gleichmäßig ausgelastet ist. Im Optimalfall sollte genau so viel Strom erzeugt werden, wie auch tatsächlich verbraucht wird. Ein „Smart Grid“ (intelligentes Stromnetz) kann diesen Anforderungen gerecht werden. In einem Smart Grid sind die einzelnen Komponenten des Systems, also Verbraucher, Verteilnetze, Transformatoren, Stromerzeuger, Energiespeicher, etc. in der Lage, miteinander zu kommunizieren. Auf diese Weise können verschiedene Vorgänge automatisiert werden. In Smart Grids können auch schwankende Energiepreise (in Abhängigkeit des aktuellen Angebots und der Nachfrage) realisiert werden, was letztendlich einen intelligenten Stromverbrauch, Umweltfreundlichkeit und Kostenersparnis ermöglicht.

P. Schartner · K. Lemke-Rust · M. Ullmann (Hrsg.) · D•A•CH Security 2015 · syssec (2015) 98-109.

Durch die dezentrale und automatisierte Steuerung der Netze entstehen neue Anforderungen an die Sicherheit des Systems. Smart Grids sind Teil der kritischen Infrastruktur und müssen aus diesem Grund besonders gegen Angriffe und Ausfälle geschützt werden. Um den schnellen Ausbau von Smart Grids zu ermöglichen und voranzutreiben, haben die Regierungen verschiedener Länder Initiativen gestartet, welche unter anderem die Standardisierung der Kommunikation in den Netzen beinhalten. Zu diesem Zweck werden bereits bestehende Standards geprüft und gegebenenfalls durch neue Teile ergänzt oder angepasst, sodass weitere Anwendungsszenarien adressiert werden können. Im Zuge der Erweiterung der Kommunikationsstrukturen und der Anwendungsbereiche der Standards entstehen neue Anforderungen an die Sicherheit in der Kommunikation, welche ebenfalls erfüllt sein müssen.

2 Überblick

2.1 IEC 61850

Wie der Titel *„Communication Networks and Systems in Substations“* des Standards IEC 61850 bereits aussagt, behandelt der Standard die Kommunikation und Mechanismen für die Automatisierung von Umspannwerken [IEC61850-1]. Umspannwerke sind Teil des Übertragungs- und Verteilnetze von elektrischer Energie. Der Standard IEC 61850 definiert einheitliche Datenmodelle, Kommunikationsstrukturen und Schnittstellen, welche von den verwendeten Systemkomponenten unabhängig sind. Darüber hinaus definiert der Standard IEC 61850 die sogenannte „Substation Configuration Language“ (SCL), welche auf XML basiert und eine Beschreibung von einzelnen Komponenten, aber auch eines kompletten Systems enthalten kann.

Der Standard definiert auch das sogenannte „Abstract Communication Service Interface“ (ACSI). Das ACSI beschreibt die Dienste, welche von einem Server bereitgestellt werden und zur Kommunikation von einem Client genutzt werden können. Der Standard legt ebenfalls fest, welche Elemente die einzelnen Anfragen an den Server enthalten müssen, und welche Elemente in den zugehörigen Antworten des Servers enthalten sein müssen. Diese abstrakte Kommunikationsschnittstelle ist unabhängig von bestimmten Protokollen definiert, was eine hohe Flexibilität erlaubt. Es können verschiedene Protokolle eingesetzt werden, um mit dem Server zu kommunizieren [IEC61850-7]. Der Standard IEC 61850 beschreibt im Teil 8-1 eine Abbildung der ACSI-Funktionen auf das MMS-Protokoll.

Durch die hohe Flexibilität der Protokolle und Konzepte des Standards IEC 61850 gibt es Bestrebungen, den Anwendungsbereich des Standards über die Automatisierung von Umspannwerken auszudehnen, sodass auch die Einbindung von „Distributed Energy Resources“ in das Energienetz und die Vernetzung von einzelnen Stationen und Leitstellen untereinander mit dem Standard IEC 61850 abgedeckt werden kann: *„This standard defines communications within transmission and distribution substations for automation and protection. It is being extended to cover communications beyond the substation to integration of distributed resources and between substations“* (siehe [NIST10b], Teil 4.3). Der Standard IEC 61850 wird darüber hinaus in Teilen erweitert. So soll zusätzlich eine Kommunikation über Web- services eingeführt werden, welche jedoch nicht in Konkurrenz zur Kommunikation über bestehende Kommunikationsprotokolle stehen soll [Engl14]. Dies ermöglicht weitreichende Einsatzmöglichkeiten des Standards IEC 61850.

2.2 IEC 62351

Der Standard IEC 62351 behandelt die Sicherheitsaspekte der Kommunikation in Smart Grids. Neben allgemein gehaltenen Sicherheitsanforderungen und Sicherheitsmaßnahmen sieht der Standard konkrete Maßnahmen für bestimmte Kommunikationsprotokolle vor, welche von verschiedenen Standards verwendet werden. Der Standard IEC 62351 hat demnach Gültigkeit für verschiedene Standards; zu nennen sind an dieser Stelle die Standards IEC 61850, IEC 60870-6 (TASE.2), IEC 60780-5-104 und IEC 60870-5-101 (mehr zu den Standards im nächsten Abschnitt). Für diesen Beitrag sind die Teile 3 und 4 des Standards IEC 62351 von besonderer Bedeutung, da in diesen Teilen die Sicherheit für TCP/IP-basierende Protokolle und die Sicherheit für das MMS-Protokoll selbst behandelt wird, und die nötigen Sicherheitsmaßnahmen beschrieben werden.

2.3 Weitere Standards

Neben den Standards IEC 61850 und IEC 62351 gibt es noch weitere wichtige Standards für die Kommunikation in Smart Grids. Zu nennen sind an dieser Stelle die Standards IEC 60870-6 und IEC 60870-5, welche ebenfalls die Kommunikation zwischen Komponenten des Smart Grids behandeln.

Der Standard IEC 60870-6 beschreibt das Kommunikationsprotokoll „Telecontrol Application Service Element 2“ (TASE.2), welches auch unter dem Namen „ICCP“ (Intercontrol Center Communication Protocol) bekannt ist. Das Protokoll wird für die Kommunikation zwischen verschiedenen Elementen des Systems (z.B. Unterstationen, Netzleitstellen, Energieerzeuger etc.) über ein „Wide Area Network“ (WAN) verwendet und baut auf dem MMS-Protokoll nach ISO 9506 auf, welches auch als Kommunikationsprotokoll von dem Standard IEC 61850 verwendet wird (siehe auch [IEC62351-1] und [NIST10b]).

Der Standard IEC 60870-5 behandelt die Kommunikation zwischen Unterstationen und Netzleitstellen, die Kommunikation selbst basiert auf dem Protokoll DNP3 (Distributed Network Protocol), welches selbst auf TCP/IP aufbaut [IEC62351-1], [VDE13]. Neben der Kommunikation außerhalb der Station kann der Standard IEC 60870-5 auch stationsintern verwendet werden.

2.4 Weitere Dokumente zu Smart Grid Security

Neben dem Standard IEC 62351 gibt es weitere Dokumente, welche von verschiedenen Normungsorganisationen veröffentlicht wurden und sich mit der Sicherheit in Smart Grids beschäftigen. Während sich der Standard IEC 62351 zu großen Teilen mit speziellen Protokollen und Standards beschäftigt, sind diese Dokumente allgemeiner gehalten und behandeln grundsätzliche Aspekte der Sicherheit in Smart Grids.

Das amerikanische NIST („National Institute of Standards and Technology“) veröffentlichte die Richtlinien „NISTIR 7628 Guidelines for Smart Grid Cyber Security“ [NIST10a], welche eine detaillierte Abhandlung der Sicherheit in Smart Grids darstellen.

Neben den amerikanischen Organisationen sollen an dieser Stelle noch die europäischen Normungsorganisationen CEN, CENELEC und ETSI genannt werden, welche zusammen die „European Standardization Organization“ (ESO) bilden und sich ebenfalls (unter anderem) mit der Standardisierung von Smart Grids beschäftigen [SGCG12a], [SGCG12b].

3 Sicherheit für das MMS-Protokoll

3.1 MMS-Protokoll

In diesem Beitrag soll der Fokus auf das MMS-Protokoll gelegt werden und dieses nach dem Standard IEC 61850 genauer beschrieben werden. Wie aus den Beschreibungen der Standards hervorgeht, wird das MMS-Protokoll in vielen verschiedenen Bereichen eingesetzt, sowohl innerhalb einzelner Schaltstationen als auch in der Kommunikation über Wide Area Networks. Durch die Ausweitung der Anwendungsbereiche der Standards, insbesondere des Standards IEC 61850 kann davon ausgegangen werden, dass das MMS-Protokoll auch in Zukunft eine wichtige Rolle für die Kommunikation in Smart Grids spielen wird. Aus diesem Grund ist es wichtig, dass das Protokoll den aktuellen Sicherheitsanforderungen genügt.

Das MMS-Protokoll wurde ursprünglich für den Einsatz in automatisierten Produktionsanlagen entwickelt. „MMS“ steht für „Manufacturing Messaging Specification“. Das Protokoll selbst ist in dem Standard ISO 9506 spezifiziert. Im Teil 8-1 des Standards IEC 61850 wird ein „Mapping“, also eine Abbildung der ACSI-Dienste auf das MMS-Protokoll definiert [IEC61850-8]. MMS definiert Dienste und Datentypen ähnlich den Diensten und Datentypen des ACSI´s, welches im Teil 7-2 des Standards definiert wurde. MMS ist in dieser Hinsicht gut geeignet, um die Kommunikation zwischen Client und Server zu realisieren. Eine Beschreibung des MMS-Protokolls findet sich in [SISC95]. Die Abbildung der ACSI-Dienste auf die jeweiligen MMS-Dienste gestaltet sich derart, dass zu jedem ACSI-Dienst der entsprechende MMS-Dienst angegeben ist und die jeweiligen Parameter der ACSI-Dienste auf die Parameter der MMS-Dienste abgebildet werden. Die Datenpakete werden unter Verwendung der „Abstract Syntax Notation One“ (ASN.1) definiert. Zu jedem Dienst gibt es ein Request-Datenpaket, welches an den Server geschickt wird, und entsprechend Response-Datenpakete, welche von dem Server zurückgeschickt werden. Des Weiteren gibt es Datenpakete für Fehlermeldungen, falls der Dienst nicht korrekt ausgeführt werden konnte. Die Datenpakete werden auch PDU (Protocol Data Unit) genannt. Teilweise werden die Datenpakete als APDU (Application Protocol Data Unit) bezeichnet, da das MMS-Protokoll auf der Anwendungsebene operiert. Eine komplette Definition der MMS-Datenpakete findet sich in dem Dokument „MMS Syntax“ [SISC94]. Zu beachten ist, dass IEC 61850 nur einen Teil der MMS-Dienste und damit auch nur einen Teil der Definitionen verwendet. Durch die Verwendung der ASN.1-Definitionen sind verschiedene Kodierungen der Datenpakete möglich, der Standard sieht die „Basic Encoding Rules“ vor, welche im Standard ISO/IEC 8825-1 definiert sind. Andere Kodierungen wie XML sind ebenfalls möglich. Alle Kodierungen haben jedoch gemein, dass Datenpakete mithilfe der ASN.1-Definitionen beim Sender kodiert und beim Empfänger dekodiert werden können.

3.2 Bestehende Sicherheitsmaßnahmen

Der Standard IEC 62351 nennt als grundlegende Sicherheitsanforderungen **Datenintegrität, Vertraulichkeit, Verfügbarkeit** und **Nichtabstreitbarkeit.** Der Punkt der Verfügbarkeit soll in diesem Abschnitt ausgeklammert werden, da hier nur das MMS-Protokoll betrachtet wird, Verfügbarkeit aber nicht von einem Protokoll alleine abhängig ist, sondern hauptsächlich von weiteren Faktoren wie den physischen Komponenten des Systems, Mechanismen wie z.B. Firewalls und organisatorischen Maßnahmen.

Die Standards IEC 61850 und IEC 62351 unterscheiden in Bezug auf die Kommunikationsprotokolle zwischen zwei Profilen, bzw. Ebenen. Das T-Profil bezieht sich auf denTransportdienst.

Im Falle des MMS-Protokolls basiert der Transportdienst aus dem TCP/IP Protokoll. Das A-Profil bezieht sich auf die Protokolle der Anwendungsebene, bzw. das MMS-Protokoll. Die Sicherheitsmaßnahmen des Standards IEC 62351 werden für diese beiden Profile separat behandelt.

Teil 3 des Standards IEC 62351 behandelt die Sicherheit für den Transportdienst (das T-Profil). Es wird die Verwendung von TLS nach RFC 2246 [AlDI99] vorgesehen, um den Datenaustausch auf der Transportebene durch eine Verschlüsselung zu sichern [IEC62351-3]. Das TLS-Protokoll sieht auch eine gegenseitige Authentifizierung mittels X.509-Zertifikaten vor. Bei dem Verbindungsaufbau wird ein gemeinsamer Schlüssel ausgehandelt, mit dem der weitere Datenaustausch mit symmetrischen Verfahren verschlüsselt werden soll. TLS bietet ebenfalls die Option, die Integrität der Nachrichten mit einem Message Authentication Code zu sichern. Der Standard IEC 62351-3 schreibt vor, dass diese Option genutzt werden soll [IEC62351-3]. Darüber hinaus definiert der Standard weitere Anforderungen: So müssen beide Kommunikationsteilnehmer ein Zertifikat bereitstellen. Außerdem sollte das Protokoll für die Aushandlung des Schlüssels Schlüssellängen von mindestens 1024 Bit für die asymmetrischen Schlüssel der Partner unterstützen.

Teil 4 des Standards IEC 62351 behandelt die Sicherheit speziell für das MMS-Protokoll, der Fokus liegt also auf der Sicherheit auf Anwendungsebene (A-Profil). Auf der Anwendungsebene soll eine Authentisierung des Kommunikationspartners den unbefugten Zugriff auf Ressourcen verhindern. Der Standard sieht eine Authentisierung der Kommunikationspartner über ACSE beim Aufbau einer Association vor. ACSE steht für „Association Control Service Element“, ist in den Standards ISO/IEC 8649 und ISO/IEC 8650 definiert und kann zum Auf- und Abbau einer Association auf der Anwendungsebene benutzt werden. Eine Authentisierung via ACSE sieht das Senden einer Verbindungsanfrage vor, auf welche der Server dann entsprechend antwortet. Die Verbindungsanfrage wird als AARQ-PDU bezeichnet (AARQ steht für ACSE Association Request), die Antwort als AARE-PDU (AARE = ACSE Association Response PDU). Die Datenpakete (AARQ und AARE) enthalten jeweils ein Datenfeld „Authentication-value“, welches Informationen zur Authentisierung des jeweiligen Senders beinhaltet. Nach ISO/IEC 8650 (der entsprechende Teil ist in dem Standard IEC 62351-4, Teil 5.3 wiedergegeben, siehe [IEC62351-4]) besteht das Feld „Authentication-value“ für das MMS-Protokoll aus drei Teilen:

Authentication-Certificate: Das Feld beinhaltet das X.509-Zertifikat des Senders, welcher sich authentifizieren möchte. Das Zertifikat selbst soll nach den „Basic Encoding Rules“, kurz BER, kodiert werden. Der Standard IEC 62351-4 fordert außerdem, dass das Zertifikat von einer vertrauenswürdigen Zertifizierungsstelle bestätigt wurde und maximal 8192 Bytes lang sein darf.

Time: Dieser Parameter enthält den Zeitpunkt (GMT), an dem das Datenfeld „Authentication-value“ erstellt wurde.

SignedValue: Über den Parameter time, repräsentiert als GENERALIZEDTIME (vgl. ASN.1), ohne zusätzliche Elemente, welche beim Kodieren mittels BER hinzukommen, wird mit einem Hashalgorithmus (SHA1 laut Standard) der Hashwert berechnet und dieser anschließend mit dem RSA-Algorithmus signiert. Es sollte mindestens eine Schlüssellänge von 1024 Bit unterstützt werden.

Der Empfänger prüft den Wert der Signatur und vergleicht den Wert des Feldes time mit der aktuellen Zeit. Der Standard IEC 62351 sieht vor, dass alle PDUs mit einer Zeitdifferenz von

mehr als 10 Minuten als ungültig angesehen werden. Dies würde bedeuten, dass ein Angreifer innerhalb dieser 10 Minuten eine gültige AARQ-PDU konstruieren könnte, indem einfach die Felder des Authentication-value kopiert werden. Mit dieser Kopie der AARQ-PDU könnte ein Angreifer versuchen, sich bei dem Server zu authentifizieren. Diese Angriffsmöglichkeit soll verhindert werden, indem alle folgenden PDUs, welche denselben Wert in dem Feld SignedValue beinhalten, als ungültig angesehen werden (vgl. zu der Authentisierung via ACSE auch IEC 62351-4, Abschnitt 5.3 [IEC62351-4].) Der Standard IEC 62351 empfiehlt des Weiteren, dass alle fehlgeschlagenen Versuche, eine Authentifizierung durchzuführen, protokolliert werden, da diese Anzeichen für einen Angriff auf das System sein können.

Zusammenfassend lassen sich die folgenden Sicherheitsmaßnahmen für TCP/IP und das MMS-Protokoll nennen: Zum einen eine Verschlüsselung der Kommunikation und Gewährleistung der Datenintegrität durch Verwendung des TLS-Protokolls auf der Transportebene als Sicherheitsmaßnahme für das T-Profil und zum anderen eine Authentifizierung auf der Anwendungsebene beim Verbindungsaufbau via ACSE als Sicherheitsmaßnahme für das A-Profil. Im Folgenden soll nun untersucht werden, inwiefern diese bestehenden Sicherheitsmaßnahmen ausreichend sind, und an welchen Stellen weitere sicherheitserhöhende Maßnahmen ergriffen werden müssen, um die bestehenden Anforderungen nach Vertraulichkeit, Authentizität, Integrität und Nichtabstreitbarkeit zu erfüllen.

3.3 Sicherheitsprobleme

3.3.1 T-Profil

In diesem Abschnitt sollen die Sicherheitsmaßnahmen für das T-Profil untersucht werden. Abbildung 1 zeigt ein typisches Szenario innerhalb einer Station, in dem das MMS Protokoll zum Einsatz kommt.

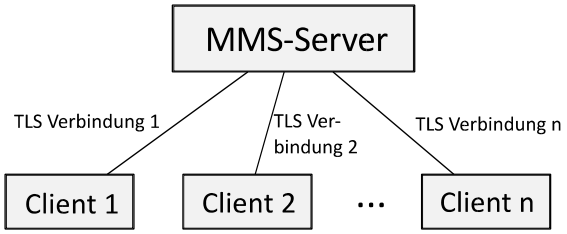

Abb. 1: Typisches Szenario innerhalb eines lokalen Netzwerkes

Bei der Kommunikation über das MMS-Protokoll nach dem Standard IEC 61850 ist das obige Szenario typisch, da die Kommunikation nur in dem lokalen Stationsnetz stattfindet. Jeder Client baut also eine separate Verbindung zu dem Server auf, welche auf der Übertragungsschicht mit TLS gesichert wird. Durch die Verwendung einer Verschlüsselung auf der Transportebene zusammen mit Message Authentication Code ist die Vertraulichkeit der Kommunikation und die Integrität der Daten gesichert. Die Kommunikationspartner können sich nach der gegenseitigen Authentifizierung bei dem Verbindungsaufbau sicher sein, dass die Datenpakete bei der Übertragung nicht manipuliert wurden, da auch ein Message Authentication Code an die Nachrichten angehängt wird. In dieser Hinsicht ist auch die Authentizität des Ursprungs der Daten gesichert, da sich nur zwei Parteien einen gemeinsamen, geheimen Schlüssel teilen, über welchen die Kommunikation gesichert wird. Jedoch definiert der Standard auch Nichtabstreitbarkeit als relevantes Sicherheitsziel. Dieses kann nicht erreicht werden, da sowohl die Verschlüsselung als auch die verwendeten Message Authentication Codes auf symmetrischen Verfahren

beruhen und jeweils einen gemeinsamen Schlüssel voraussetzen: *„Symmetric cryptography is used for data encryption [...] The keys for this symmetric encryption are generated uniquely for each connection [...]“* [AlDi99]. Zwar benutzen Client und Server verschiedene Schlüssel für die Berechnung des MACs, welche jedoch aus einem gemeinsamen Geheimnis, in RFC 2246 „pre_master_secret“ genannt, generiert werden: *„By sending a correct finished message, parties thus prove that they know the correct pre_master_secret“* [AlDi99].

3.3.2 Das A-Profil

Externe Kommunikationsanbindungen können durch Gateways erreicht werden, welche die Verbindungen von mehreren Clients bündeln und die Datenpakete weiterleiten. Ein Beispiel für dieses Szenario wäre beispielsweise ein Schaltbefehl, welcher von einem Kontrollzentrum über das Gateway der Station an den Server weitergeleitet wird. Ein solches Szenario ist in Abbildung 2 dargestellt.

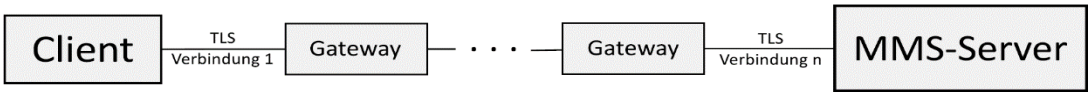

Abb. 2: Externe Anbindung einer Komponente

Hier ergeben sich weitere Probleme, denn wie im letzten Abschnitt bereits angedeutet wurde, basiert die Sicherheit der Kommunikation ausschließlich auf TLS, nachdem die gegenseitige Authentifikation via ACSE stattgefunden hat. Da TLS nur die Kommunikation zwischen zwei TCP-Instanzen betrifft, können die ausgetauschten Daten in den TCP-Instanzen, in der Praxis also von den Gateways, verändert werden.

Ein weiteres Problem stellt die Authentifizierung über ACSE dar, so wird hier nur ein Zeitstempel signiert. Besser wäre es jedoch, wenn die signierten Daten weitere Informationen über Sender und den bestimmten Empfänger enthalten. Sind diese Informationen nicht enthalten, könnte ein Angreifer die PDU kopieren und sich bei einem anderen Server innerhalb der Gültigkeitsdauer des „Authentication-value“ erfolgreich authentifizieren. Für Nichtabstreitbarkeit müsste für jedes Datenpaket eine Authentifizierung des Ursprungs erfolgen, jedoch ist dies nicht von dem MMS-Protokoll vorgesehen. Bei Betrachtung der Definitionen der MMS-PDUs (siehe [SISC94]) fällt auf, dass keine Signaturen für einzelne Datenpakete vorgesehen sind.

Ein weiteres Problem, welches bei einer Kommunikation über Gateways entsteht, ist das folgende: Während der Server bei einer direkten Verbindung nach erfolgter Authentifizierung wissen konnte, von wem ein Datenpaket gesendet wurde, ist die Authentifikation des Ursprungs der Daten bei einer Kommunikation über Gateways ebenfalls nicht möglich, da die Daten von mehreren Clients über eine einzelne TCP-, bzw. TLS-Verbindung zwischen den Gateways übertragen werden. Die Informationen über den originären Sender gehen verloren [FHDS10]. Auch dieses Problem hat seinen Ursprung in der Tatsache, dass die Datenpakete auf Anwendungsebene keine Informationen über den Absender bereitstellen. Es ist offensichtlich, dass ohne eine Authentisierung des Ursprungs der Daten das Kriterium der Nichtabstreitbarkeit unmöglich zu erfüllen ist.

4 Eine Sicherheitslösung für das MMS-Protokoll

4.1 Ziel

Es ist klar geworden, dass die Sicherheitsmaßnahmen, welche vom Standard IEC 62351 vorgeschrieben werden, generell nicht ausreichend sind, um Nichtabstreitbarkeit zu realisieren. Darüber hinaus entstehen bei der Kommunikation über mehrere Stationen weitere Probleme, sodass letztendlich weder die Sicherung der Vertraulichkeit und Datenintegrität als auch die Authentifizierung des Ursprungs der Daten nicht mehr möglich ist. Die Sicherheitsprobleme rühren hauptsächlich daher, dass die Sicherheit der Kommunikation ausschließlich von TLS abhängig ist, nachdem die Verbindung aufgebaut wurde und die gegenseitige Authentifizierung über ACSE stattgefunden hat. Darüber hinaus hat sich gezeigt, dass bestimmte Szenarien dazu führen können, dass die Sicherheitsmaßnahmen für das T-Profil nicht greifen und somit einige Sicherheitsprobleme entstehen. Aus diesem Grund müssen weitere Sicherheitsmaßnahmen auf der Anwendungsebene eingeführt werden, um sämtliche Sicherheitsanforderungen zu erfüllen. Das Ziel, welches also erreicht werden soll, ist eine anwendungsorientierte Ende-zu-Ende Sicherheit (A-Profile Security), welche unabhängig von der unterliegenden Netztopologie (Verbindung über ein lokales Netzwerk oder über ein „Wide Area Network“ mit mehreren Gateways) gewährleistet werden soll. Abbildung 3 veranschaulicht den Unterschied zwischen der anwendungsorientierten Sicherheit und der (bisherigen) Sicherheit auf Transportebene (T-Profile Security).

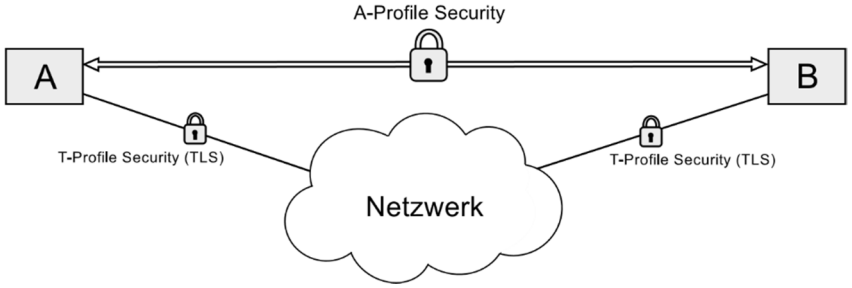

Abb. 3: Das Ziel: Sicherheit auf Anwendungsebene unabhängig von der Kommunikationsstruktur

Es lassen sich drei wesentliche Sicherheitsanforderungen nennen, welche auf der Anwendungsebene realisiert werden sollen:

- Authentizität des Ursprungs *sämtlicher* Nachrichten.
- Nichtabstreitbarkeit sämtlicher Aktionen. Dies beinhaltet Schaltbefehle, gesendete Statusinformationen, Lesen und Schreiben von beliebigen Werten, etc.
- Nachweisbarkeit und Zurechenbarkeit von sämtlichen Handlungen zu einem späteren Zeitpunkt.

Diese drei Ziele sind zusammenhängend und müssen zusammen umgesetzt werden, so ist die Authentisierung des Ursprungs aller Nachrichten eine notwendige Voraussetzung für Nichtabstreitbarkeit von Handlungen, was wiederum die Grundlage für die Zurückverfolgung und Zurechenbarkeit von allen Handlungen ist. Bei dem Kriterium der Nichtabstreitbarkeit kann zwischen zwei Fällen unterschieden werden. So steht in den Richtlinien des NIST zur Nichtabstreitbarkeit: *„Non-repudiation protects individuals against later claims by an author of not having authored a particular document, a sender of not having transmitted a message, a receiver of not having received a message, or a signatory of not having signed a document“*. [NIST10a].

Mit dem Begriff der Nichtabstreitbarkeit sind also im Endeffekt zwei Sicherheitsdienste gemeint: Ein Sender einer Nachricht soll später nicht abstreiten können, die entsprechende Nachricht gesendet zu haben. Ebenso soll der Empfänger einer Nachricht später nicht abstreiten können, eine bestimmte Nachricht empfangen zu haben.

4.2 Erforderliche Maßnahmen

Die Authentizität des Ursprungs aller Datenpakete kann mit digitalen Signaturen und Identitäten der Kommunikationsteilnehmer in Form von Zertifikaten erreicht werden. Das Konzept sieht vor, dass alle Datenpakete, welche gesendet werden, im Endeffekt also jede MMS-PDU mit einer digitalen Signatur und einem Zeitstempel versehen werden müssen, damit der Ursprung eines jeden Datenpakets von dem Empfänger verifiziert werden kann. Zusätzlich soll ebenfalls der Name des Empfängers in dem Datenpaket gespeichert werden, um ein Abfangen und Weiterleiten von Datenpaketen an andere Instanzen zu erkennen. Darüber hinaus müssen alle Datenpakete, sowohl die gesendeten als auch die empfangenen, in einem sicheren Speicher protokolliert werden, damit sämtliche Aktionen in dem System zu einem späteren Zeitpunkt rückverfolgt und mithilfe der (ebenfalls protokollierten) Signaturen der entsprechenden Instanz zugeordnet werden können. Die Möglichkeit der Rückverfolgung aller Aktionen ist wichtig, um im Falle eines durch Schaltfehler und inkorrekte Einstellungen verursachten Schadens den jeweiligen Urheber bzw. die verantwortliche Instanz zu finden.

4.3 Zugriffskontrolllisten

Durch die Tatsache, dass nun die Authentizität des Ursprungs jedes einzelnen Datenpakets sichergestellt ist, lässt sich das Sicherheitsniveau mit Serverseitigen Zugriffskontrolllisten weiter erhöhen. Im Folgenden werden die Zugriffskontrolllisten auch ACL („Access Control List“) genannt. Der Standard IEC 62351 nennt als weitere Bedrohung interne Mitarbeiter, welche Sabotageaktionen durchführen könnten: *„Disgruntled employees are one of the primary threats for attacks on power system assets“* ([IEC62351-1] Teil 5.2.3.2). Zugriffskontrolllisten ermöglichen eine Einteilung der Clients in weitere Stufen als nur „vertrauenswürdig“ und „nicht vertrauenswürdig“. Nicht jeder Client benötigt Vollzugriff auf den Server für die Erfüllung seiner Aufgaben. Einem „Monitoring-System“, welches nur bestimmte Werte lesen muss, würde z.B. nur der Lesezugriff gestattet. Die Zugriffskontrolle verringert den potentiellen Schaden, der entstehen kann, wenn ein Angreifer die Kontrolle über einen Client erlangen konnte. Die *„NISTIR 7628 Guidelines for Smart Grid Security“* sehen eine rollenbasierte Zugriffskontrolle vor. Eine „Rolle“ ist in dem Zusammenhang eine Menge von Rechten, welche dem Inhaber der jeweiligen Rolle zugestanden werden. Ein Benutzer kann dabei eine oder mehrere Rollen innehaben, abhängig von seiner Aufgabe in dem System (Vgl. [NIST10a], Volume 1, Teil 7.3.23).

5 Umsetzung mit XML-Signaturen

Ein zentraler Punkt des Konzepts ist die Umsetzung der Maßnahmen für das MMS-Protokoll, was die Frage beinhaltet, wie die Datenpakete möglichst einfach mit weiteren Informationen und zuletzt mit einer Signatur versehen werden können. Wie bereits im Abschnitt 4.2.1 angedeutet wurde, sehen die ASN.1-Definitionen der MMS-PDUs selbst keine Verwendung von digitalen Signaturen vor. Dieses Konzept sieht daher die folgende Möglichkeit vor, die Datenpakete zu sichern: Durch die Verwendung der ASN.1-Definitionen der Datenpakete sind verschiedene Kodierungen der Datenpakete möglich. Während normalerweise die „Distinguished Encoding Rules“ verwendet werden, erlaubt ASN.1 ebenfalls eine XML-Kodierung der Datenpakete, die sogenannten „XML Encoding Rules“, kurz XER. An XML-Kodierte Datenpakete

können dann XML-Signaturen angefügt werden. Das XML-Format zeichnet sich durch eine hohe Flexibilität aus. Die XML-Dokumente werden als „Document Object Model“ dargestellt, sie bestehen aus verschiedenen Knoten welche wiederum Inhalte und weitere Knoten enthalten können.

Die XML-Dokumente können so um weitere Knoten erweitert werden. Um Nichtabstreitbarkeit zu erreichen, müssen dem Datenpaket neben einer Signatur weitere Informationen angefügt werden, so ist mindestens ein Zeitstempel erforderlich, um den genauen Zeitpunkt, an dem das Datenpaket gesendet wurde, erforderlich um Replay-Angriffe auszuschließen. Da auch Nichtabstreitbarkeit des Empfangs von Nachrichten gefordert ist, sieht das Konzept vor, dass der Server mit der Antwort auch gleichzeitig den Empfang der zugehörigen Anfrage bestätigt. Für diesen Zweck müssen weitere Informationen über das zugehörige Datenpaket in der Antwort gespeichert werden: Zum einen ein Hashwert der zugehörigen Anfrage, welcher die Anfrage hinreichend genau identifiziert und des Weiteren ein Zeitstempel des Zeitpunkts, an dem die Anfrage empfangen wurde. All diese zusätzlichen Daten werden in das Dokument eingebettet und anschließend mit der Signatur gesichert.

XML-Signaturen werden in dem Standard „XML Signature Syntax and Processing“ des World Wide Web Consortiums, kurz W3C genannt, spezifiziert [XMLDSIG]. XML-kodierte Datenpakete mit XML-Signaturen sind zwar vergleichsweise lang, jedoch bringt die Verwendung von XML-Signaturen auch Vorteile: XML-Signaturen unterstützen verschiedene Signaturverfahren, welche von Signatur zu Signatur unterschiedlich sein können. XML-Signaturen unterstützen den Austausch von X.509-Zertifikaten, was von Vorteil ist, falls eine Verifikation der Zertifikate mittels einer „Public Key Infrastructure“ zum Einsatz kommen soll. Dabei kommt zu Hilfe, dass jeweils nur ein ausgewählter Kreis von Personen und Prozessen Zugriff auf die Komponenten und ihre Ressourcen haben wird. Das folgende Listing zeigt beispielhaft eine XML-kodierte MMS-APDU, welche eine Verbindungsanfrage des Clients an einen Server darstellt welche zusätzlich mit weiteren Informationen und einer Signatur erweitert wurde. Die zusätzlichen Daten sind an das Ende des Dokuments angefügt und zur besseren Unterscheidung als separater Block dargestellt. Der besseren Übersichtlichkeit wurden mit … gekennzeichnete Teile ausgelassen.

```
<MmsPdu>
<initiateRequestPdu>
<localDetailCalling>65000</localDetailCalling>
<proposedMaxServOutstandingCalling>5</proposedMaxServOutstandingCalling>
<proposedMaxServOutstandingCalled>5</proposedMaxServOutstandingCalled>
<proposedDataStructureNestingLevel>10</proposedDataStructureNestingLevel>
<mmsInitRequestDetail>
<proposedVersionNumber>1</proposedVersionNumber>
<proposedParameterCBB>11110001000</proposedParameterCBB>
<servicesSupportedCalling> 11101110000111000000000...</servicesSupportedCalling>
</mmsInitRequestDetail>
</initiateRequestPdu>

<timestamp>130723271596204607</timestamp>
<addressee>ServerDistinguishedName</addressee>
<Signature xmlns="http://www.w3.org/2000/09/xmldsig#">
<SignedInfo>
<CanonicalizationMethod Algorithm="http://www.w3.org/TR/2001/REC-xml-c14n-
                                   20010315"/>
<SignatureMethod Algorithm="http://www.w3.org/2001/04/xmldsig-more#ecdsa-
sha256"/>
</SignedInfo><SignatureValue>
8L2BZWqElXJAQr5AWUznbxnhMCFeOfGPxPv4q6POOoz0PUYS4buHioaKCvhTqQaR
9UBs6RDY9Hq4csvM4NCTnQ==</SignatureValue>
<KeyInfo><KeyName>IssuerName,SubjectName</KeyName></KeyInfo></Signature>

</MmsPdu>
```

Eine Implementierung unter Verwendung von XML bringt den zusätzlichen Vorteil, dass die Lösung mit XML-Signaturen prinzipiell auf alle Systeme angewendet werden kann, die XML-basierte Übertragungsprotokolle verwenden. Ein Beispiel dafür ist eine Erweiterung des Standards IEC 61850. Dort ist neben der Abbildung der Client/Server Funktionen auf MMS (IEC 61850-8-1) eine Abbildung auf Webservices unter Verwendung des ebenfalls auf XML basierenden Protokolls XMPP geplant (IEC 61850-8-2). Siehe auch [Engl14].

6 Ausblick

Es wurde klar, dass die bestehenden Sicherheitsmaßnahmen nicht ausreichend sind, um alle Sicherheitsanforderungen zu erfüllen. Insbesondere durch neue Anwendungsgebiete des Standards IEC 61850 außerhalb des ursprünglichen Anwendungsbereichs entstehen Probleme, welche dazu führen, dass die verwendeten Protokolle um weitere Sicherheitsmaßnahmen erweitert werden müssen. Die vorgestellte Sicherheitslösung zeigt einen möglichen Weg auf, um eine „wirkliche“ Ende-zu-Ende Sicherheit für das MMS-Protokoll auf Anwendungsebene zu realisieren, und insbesondere die Kriterien der Nichtabstreitbarkeit und der Nachweisbarkeit zu erfüllen. Aufbauend auf dem Konzept können weitere Sicherheitsmaßnahmen eingeführt werden, so erlaubt XML ebenfalls eine Verschlüsselung der Daten, was die Möglichkeit eröffnet, die gesamten Sicherheitsmechanismen auf der Anwendungsebene zu realisieren und die Transportebene des Protokollstacks schlanker zu gestalten. Hier könnte dann geprüft werden, ob diese Maßnahme Vorteile in der Performance gibt. Ähnliche Entwicklungen findet man bei der Diskussion um die Auswahl der Protokolle für das „Internet of Things (IoT)“.

Zu dem vorgestellten Konzept existiert bereits eine Implementierung, welche in einer simulierten Umgebung innerhalb der Testszenarien funktioniert. Um jedoch die Tauglichkeit der Implementierung zu überprüfen, müssen jedoch weitere Tests unter realistischen Bedingungen durchgeführt werden.

Literatur

[AlDi99] C. Allen T. Dierks. The TLS Protocol Version 1.0. RFC 2246, January 1999.

[Engl14] H. Englert. Neue Kommunikationskonzepte für den Netzbetrieb – aktuelle Entwicklungen in der IEC 61850. Smart Grids Forum, Hannover Messe, 2014 https://www.vde.com/de/smartgrid/forum/beitraege/Documents/2014-04-09-neue-kommunikationskonzepteenglert.pdf

[FHDS10] S. Fries, H. J. Hof, T. Dufaure, M. G. Seewald. Security for the Smart Grid - Enhancing IEC 62351 to Improve Security in Energy Automation Control. Technical report, 2010. In: International Journal on Advances in Security, vol. 3 no 3 & 4, http://www.iariajournals.org/security/.

[IEC61850-1] IEC 61850-1: Communication networks and systems in substations – Introduction and overview, October 2006.

[IEC61850-7] IEC 61850-7-2: Communication networks and systems for power utility automation – Part 7-2: Basic information and communication structure – Abstract communication service interface (ACSI), April 2011.

[IEC61850-8] IEC 61850-8-1: Communication networks and systems for power utility automation - Part 8-1: Specific communication service mapping (SCSM) - Mappings to MMS (ISO 9506-1 and ISO 9506-2) and to ISO/IEC 8802-3, February 2012.

[IEC62351-1] IEC 62351-1: Power systems management and associated information exchange – Data and communications security Part 1: Communication network and system security - Introduction to security issues, May 2007.

[IEC62351-3] IEC 62351-3: Data and Communication Security – Part 3: Profiles Including TCP/IP, June 2007.

[IEC62351-4] IEC 62351-4: Data and Communication Security – Part 4: Profiles Including MMS, June 2007.

[NIST10a] The Smart Grid Interoperability Panel Cyber Security Working Group. NISTIR 7628 Guidelines for Smart Grid Cyber Security, August 2010.

[NIST10b] Office of the National Coordinator for Smart Grid Interoperability. NIST Special Publication 1108, NIST Framework and Roadmap for Smart Grid Interoperability Standards, Release 1.0, January 2010.

[SGCG12a] Smart Grid Coordination Group. Smart Grid Reference Architecture. Report, CEN-CENELEC-ETSI, November 2012.

[SGCG12b] Smart Grid Coordination Group. Smart Grid Information Security. Report, CEN-CENELEC-ETSI, November 2012.

[SISC94] Systems Integration Specialists Company, Inc. SISCO MMS Syntax, 1994. Eine Beschreibung der MMS Syntax nach ISO 9506-2.
http://www.sisconet.com/downloads/mms_abstract_syntax.txt

[SISC95] Systems Integration Specialists Company, Inc. Overview and Introduction to the Manufacturing Message Specification (MMS), 1995.
http://www.sisconet.com/downloads/mmsovrlg.pdf

[VDE13] The German Roadmap E-Energy / Smart Grids 2.0 - Smart Grid Standardization Status, Trends and Prospects. VDE, DKE, 2013.

[XMLDSIG] XML Signature Syntax and Processing (Second Edition), June 2008. W3C Recommendation. Abrufbar unter http://www.w3.org/TR/xmldsig-core/.