Qualifizierte Signatur im elektronischen Messdatenaustausch

Lars Dietze[1], Prof. Dr. Bernd Holznagel, LL.M.[1],
Luigi Lo Iacono[2], Prof. Dr. Christoph Ruland[2]

[1]Institut für Informations-, Telekommunikations- und Medienrecht (ITM)
Universität Münster
Leonardo-Campus 9
48149 Münster
{dietze, holznagel}@uni-muenster.de

[2]Institut für Digitale Kommunikationssysteme (DCS)
Universität Siegen
Hölderlinstraße 3
56078 Siegen
{luigi.lo-iacono, christoph.ruland}@uni-siegen.de

Zusammenfassung: Das Auslesen von Messdaten in elektronischer Form ermöglicht es, diese vom Ursprung bis zur Rechnungsstellung effizient und ohne Medienbruch zu erheben und zu verarbeiten. Gerade im liberalisierten Energiemarkt ist dies von Bedeutung, da eine Vielzahl von Marktteilnehmern miteinander kommunizieren muss. Das im VERNET-Programm geförderte SELMA-Projekt verfolgt das Ziel, einen Standard für den sicheren elektronischen Austausch von Messdaten zu entwickeln und zu etablieren.

Eine der zentralen Anforderungen ist die Gewährleistung der Authentizität und Integrität der über offene Netze ausgelesenen Messdaten, die über die gesamte Lebensdauer der Messdaten nachprüfbar sein sollen. Die technische Umsetzung dieser Anforderungen resultiert in einer Sicherheitsarchitektur, die durch den durchgängigen Einsatz elektronischer Signaturen gekennzeichnet ist. Mit den signierten Datensätzen können die Rechnungen von den Marktteilnehmern auf ihre Authentizität und Integrität hin überprüft werden.

Dieser Beitrag zeigt die gesetzgeberischen Hindernisse auf, die bei der Umsetzung der Anforderungen an qualifizierte Signaturen im elektronischen Messdatenaustausch auftreten und wie dennoch eine größtmögliche Beweiskraft für fortgeschrittene Signaturen erreicht werden kann.

1 Einleitung

Die Liberalisierung der Energiemärkte in Deutschland wurde 1998 mit dem Inkrafttreten des Gesetzes zur Neuregelung des Energiewirtschaftsrechts eingeleitet. Dies führt zu einer Veränderung der Energiemärkte, die durch Deregulierung, freien Netzzugang und erhöhten Wettbewerb erhebliche Auswirkungen auf Energieversorger und Endkunden hat. Eine besondere Herausforderung stellen die Geschäftsprozesse dar, die einen Datenaustausch zwischen nunmehr konkurrierenden Unternehmen erfordern. Hierbei kommt der nun benötigten sicheren und zeitnahen Bereitstellung von Informationen zu gemessenen Energiemengen für Abrechnungszwecke eine besondere Bedeutung zu. Hieraus ergeben sich neue Anforderungen an die Geschäftsprozesse der Energieversorger und an den Verbraucherschutz für den Endabnehmer. Dies war der Ausgangspunkt für das Projekt SELMA (Sicherer elektronischer Messdaten-Austausch, http://www.selma-project.de/), das vom Bundesministerium für Wirtschaft und Arbeit im VERNET-Programm (Sichere und verlässliche Transaktionen in offenen Kommunikationsnetzen, http://www.vernetinfo.de/) gefördert wird.

1.1 Liberalisierter Energiemarkt

Die Liberalisierung der Energiemärkte stellt die Energieversorgungsunternehmen vor neue Herausforderungen und führt zur Neuregelung der Beziehungen der am Energiemarkt beteiligten Parteien. Die folgenden Rollen existieren im liberalisierten Energiemarkt:

1. Der *Abnehmer* nimmt Energie ab und bezahlt für die abgenommene Energie. Die von ihm verbrauchte/abgenommene Energie wird durch ein Messgerät ermittelt und von der Datenakquisition ausgelesen. Abnehmer können bei SELMA die Marktteilnehmer Endkunde, Verteilungsnetzbetreiber und Übertragungsnetzbetreiber sein.

2. Die *Datenakquisition* liest die Messdaten aus. Bei der Messwertbearbeitung werden diese Daten überprüft, gegebenenfalls Primärwerte berechnet oder durch Ersatzwerte ersetzt und in das Format gebracht, in dem sie weitergegeben werden können. Um die aufbereiteten Messdaten von den Messdaten aus der direkten Messung unterscheiden zu können, werden die aufbereiteten Messdaten als Energiedaten bezeichnet.

3. Die *Distribution* ist für die Verteilung von Energie- und Verbrauchsdaten zuständig. In der Regel werden die Energiedaten direkt von der Datenakquisition an die Provision zur Energieabrechnung weitergegeben, andernfalls von der Distribution, wo sie gegebenenfalls aufsummiert werden. Netznutzungsdaten werden zur Abrechnung an das Billing weitergegeben.

4. Die *Provision* stellt dem Abnehmer Energie zur Verfügung. Sie erhält die Energiedaten des Abnehmers entweder von der Distribution oder direkt von der Datenakquisition. Sie kann die Daten – falls notwendig – aufsummieren.

5. Das *Billing* erhält die Abrechnungsdaten für die Netznutzung von der Distribution und die Energiedaten für die Lieferung von der Provision. Das Billing erstellt die Rechnung für den Abnehmer und bietet ihm später die Möglichkeit, die Daten einzusehen. Wenn Daten geändert werden (z.B. Summenbildung), müssen die Messdaten referenziert, vorgehalten und auf Anforderung eingesehen werden können.

6. Die *Prüfbehörden* sind staatliche Kontrollinstanzen, die Kontrollfunktionen bzw. Maßnahmen zum Verbraucherschutz durchführen. Die Bauartzulassung von eichpflichtigen Geräten erfolgt durch die Physikalisch-Technische Bundesanstalt (PTB) auf der Grundlage anerkannter Regeln der Technik. Für die Eichung und die Marktüberwachung eichpflichtiger Geräte nach dem Inverkehrbringen sind die Eichbehörden der einzelnen Bundesländer verantwortlich.

1.2 Projekt SELMA

Ziel des SELMA-Forschungsvorhabens ist die Erarbeitung eines rechtsverträglichen, technischen Verfahrens, mit dem geldwerte Energiemessdaten unabhängig vom Transportmedium sicher von dezentralen Messgeräten über offene Netze zu den Eigentümern und Nutzern der Messdaten (Versorgungsunternehmen/Energiekunden) übertragen werden können. Dieses Ziel soll durch die Schaffung einer Musterlösung für eichfähige, elektronische Messgeräte und Zusatzgeräte für Elektrizität, Gas, Wasser und Wärme und einer gemäß den Datenschutzgesetzen zulässigen Lösung für die Datenübertragung über offene Kommunikationsnetze erreicht werden.

Die Arbeiten am SELMA-Projekt begannen im Oktober 2001 und dauern bis voraussichtlich Anfang 2005 an. An der Planungs- und Entwicklungsphase des SELMA-Projekts sind insgesamt 14 Projektpartner bestehend aus Energieversorgungsunternehmen (EAM Energie AG, Energie Baden-Württemberg AG, RWE Net AG), Hersteller für Messgeräte und Messgeräte-Managementsysteme (ELSTER GmbH, EMH Elektrizitätszähler GmbH & Co. KG, Görlitz AG, ITF-EDV Fröschl GmbH, Karl Wieser GmbH, Landis+Gyr), Prüf- und Eichbehörden (Arbeitsgemeinschaft für das Mess- und Eichwesen, Bundesamt für Sicherheit in der Informationstechnik, Physikalisch-Technische Bundesanstalt) und universitären Forschungseinrichtungen (Institut für Informations-, Telekommunikations- und Medienrecht, Abt. II, Universität Münster, Institut für Digitale Kommunikationssysteme, Universität Siegen) beteiligt.

2 Sicherheitskonzept für den liberalisierten Energiemarkt

Einen anschaulichen Gesamtüberblick über das SELMA-Sicherheitssystem bietet das in Abbildung 1 dargestellte Transaktionsmodell, das die aufeinander folgenden Aktionen und Transaktionen beim Messdatenaustausch zeigt. Eine detaillierte Beschreibung der SELMA-Sicherheitsarchitektur findet sich in [LR+03]. Das Hauptaugenmerk liegt auf der Berücksichtigung der Anforderungen, die das Signaturgesetz (SigG) [SG01] hinsichtlich der eingesetzten Technik und der verwendeten Verfahren an qualifizierte Signa-

turen stellt, und auf der Frage, wie für den elektronischen Messdatenaustausch im liberalisierten Energiemarkt eine Lösung erarbeitet werden kann, um die Beweiskraft der verwendeten fortgeschrittenen Signaturen zu steigern.

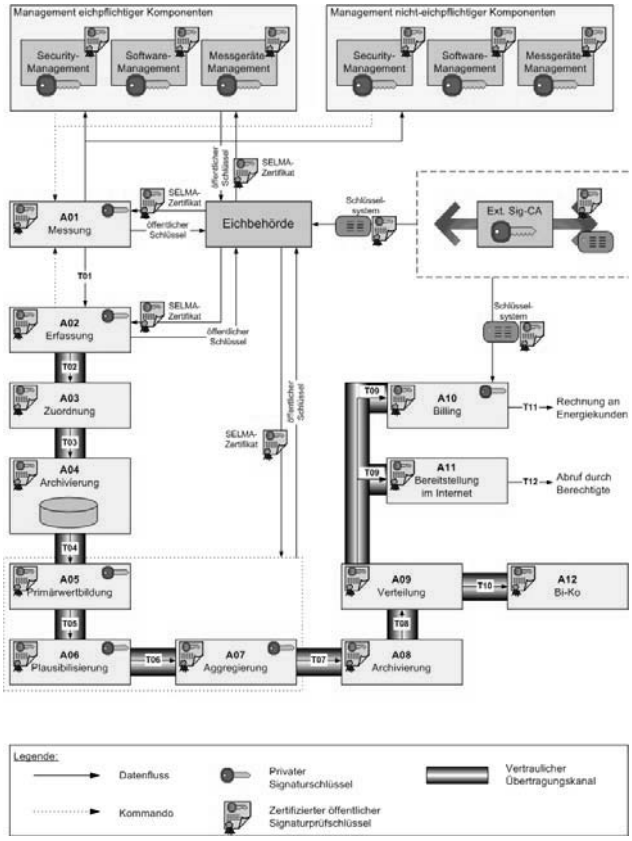

Abbildung 1: SELMA-Sicherheitsarchitektur

Eine zentrale Rolle im SELMA-Projekt spielt die Messung in Aktion *A01* und das dafür eingesetzte SELMA-Messgerät. Es ermittelt Messwerte und versieht diese mit elektronischen Signaturen, um der Anforderung der informationsgebundenen Authentizität gerecht zu werden. Neben der Messeinheit enthält es zwei weitere Module: einen Controller für die Verarbeitung der Messsignale, der höheren Kommunikationsprotokolle sowie für die Steuerung der Messeinheit und eine Signaturerstellungseinheit für sicherheitsrelevante Operationen, das sog. Meter Identification Modul (MIM). Damit der Controller und die Kommunikation zum MIM nicht manipuliert werden können, befinden sich beide Komponenten in dem durch eine Eichplombe geschützten Bereich. Der Controller enthält nach Möglichkeit Funktionen zur Bestimmung von Datum und Uhrzeit, da Zeitstempel ein wichtiger Bestandteil der Kommunikations- und Managementabläufe sind (z.B. Schutz vor Replay-Attacken). Außerdem gibt es ein Kommunikationsmodul, das die unteren Kommunikationsschichten beinhaltet und die physikalische Kommunikation mit der Außenwelt ermöglicht. Das Kommunikationsmodul selbst muss nicht innerhalb

des durch die Eichplombe geschützten Bereichs liegen, da hierüber nur gesicherte Informationen ausgetauscht werden.

Das MIM im SELMA-Messgerät erzeugt sein eigenes asymmetrisches Signaturschlüsselpaar. Dieser Prozess wird in der vertrauenswürdigen Umgebung der Prüfstelle bei der Ersteichung unterhalb der Eichplombe angestoßen. Die Eichbehörden bzw. von den Eichbehörden staatlich anerkannte Prüfstellen dienen als vertrauenswürdige dritte Instanz. Der private Schlüssel bleibt immer im MIM. Als MIMs werden Signaturerstellungseinheiten für qualifizierte Signaturen verwendet. Diese sind nach Common Criteria EAL 4 plus bzw. nach ITSEC E3 hoch zertifizierte und von der RegTP bestätigte Hardwaregeräte, die wirksam das Auslesen des privaten Signaturschlüssels auch für den Benutzer selbst verhindern.

Der öffentliche Schlüssel wird in der Prüfstelle während der Ersteichung aus der MIM ausgelesen und zertifiziert (SELMA-Zertifikat). Die Eichbehörden bzw. staatlich anerkannten Prüfstellen verwenden hierfür ein Schlüsselsystem mit qualifiziertem Zertifikat von einer externen Sig-CA, das den Anforderungen qualifizierter Signaturen genügt und auf einer Chipkarte abgespeichert ist. Es wird zusammen mit einer SigG-konformen Signaturanwendungskomponente (dem sog. SELMA-Zertifikatsgenerator) von den Leitern der Prüfstellen zur Erstellung der SELMA-Zertifikate verwendet. Die Zertifikate und Sperrlisten sind gemäß dem X.509v3 [X509] bzw. dem X.509v2 [X509] Standard aufgebaut.

Bei der Sig-CA handelt es sich um einen extern betriebenen Zertifizierungsdiensteanbieter (ZDA, siehe http://www.regtp.de/elsig/), der asymmetrische Schlüsselsysteme und Zertifikate generiert und zur Verfügung stellt. Die Sig-CA stellt dem befugten Personal der Eichbehörden, der Prüfstellen und der PTB asymmetrische Schlüsselpaare und Zertifikate aus, die den Bestimmungen des SigG hinsichtlich qualifizierter Signaturen entsprechen.

Zur Bereitstellung der SELMA-Zertifikate – insbesondere für die Verifikationsprozesse in den Aktionen *A02* bis *A12* – dient ein Verzeichnisdienst (der sog. SELMA Directory Service, SDS), wobei die SELMA-Zertifikate zusätzlich in die Messgeräte zurück geschrieben werden, um den Prozess der Zertifikatsverteilung zu erleichtern. SELMA-Geräte, deren Zertifikate nicht über den SDS zur Verfügung stehen, können im eichrechtlich relevanten Verkehr nicht verwendet werden.

Neben dem Schlüsselsystem und den Signaturkomponenten zur Erzeugung der SELMA-Zertifikate werden von den Eichbehörden und Prüfstellen MIMs zum Signieren von Management-Kommandos verwendet, die an das Messgerät gesendet werden (Management eichpflichtiger Komponenten). Sie generieren mit ihren MIMs ein eigenes Schlüsselpaar. Der private Signaturschlüssel bleibt in der MIM-basierten Signaturerstellungseinheit des Management-Systems eichpflichtiger Komponenten. Der öffentliche Schlüssel wird ausgelesen und auf vertrauenswürdigem Weg an andere Prüfstellen verteilt.

Damit das SELMA-Messgerät Requests von der Datenakquisitionsstelle und den Management-Systemen verifizieren kann, benötigt es öffentliche SELMA-Prüfschlüssel. Die SELMA-Prüfschlüssel der MIMs der Eichbehörden, der PTB, der ausführenden Prüfstel-

le und anderer Prüfstellen werden zusammen mit den zugehörigen Distinguished Names (DN) in das Messgerät geladen. Dieses Laden erfolgt bei der Ersteichung nicht per Fernübertragung, sondern unmittelbar am SELMA-Gerät durch eine hoheitlich tätige Person (z.B. den Prüfstellenleiter). Die Authentizität und Integrität der in das Gerät geladenen Informationen ist daher a priori gewährleistet. Wegen der rekursiv realisierten Sicherheit bei späterem Wechsel der Schlüssel bleibt diese a priori-Sicherheit bestehen.

Für die Aktionen *A02* bis *A12* des Transaktionsmodells kommen IT-Systeme zum Einsatz. Abhängig von der Aktion, für die die IT-Systeme eingesetzt werden, muss zwischen IT-Systemen ohne Signaturfunktion und IT-Systemen mit Signaturfunktion unterschieden werden. Generell kann davon ausgegangen werden, dass alle IT-Systeme, die in den Aktionen *A02* bis *A12* eingesetzt werden, Signaturen prüfen müssen. Daher sind in den genannten Aktionen Zertifikate bzw. öffentliche Schlüssel zur Signaturprüfung erforderlich.

IT-Systeme mit Signaturfunktion benötigen außerdem einen privaten Signaturschlüssel. Bei der Erfassung (Aktion *A02*) wird der private Schlüssel zum Signieren der Messdatenanforderung benötigt.

In den Aktionen *A05*, *A06* und *A07* wird jeweils ein privater Signaturschlüssel verwendet, um in diesen Aktionen ggf. im Sinne der PTB-A 50.7 [PA04] neu generierte Messwert-äquivalente Daten mit einer Signaturerstellungseinheit zu signieren (in Abbildung 1 durch den gepunkteten Kasten gruppiert). Diese IT-Systeme werden im Weiteren Messgeräte-äquivalente IT-Systeme genannt. Eichrechtlich müssen diese IT-Systeme – sofern im Sinne der PTB-A 50.7 die Bildung neuer Messwerte erfolgt – hinsichtlich der Vertrauenswürdigkeit dasselbe Niveau haben wie das SELMA-Messgerät. Es gilt, wie bei den vom Messgerät generierten Messwerten, dass eichrechtlich relevante Messwerte durch den Abnehmer eindeutig rückverfolgbar sein müssen. Messgeräte-äquivalente IT-Systeme und Datenerfassungssysteme verfügen über ein MIM. Im Inneren der manipulationssicheren MIM ist der private Signaturschlüssel gespeichert. Der korrespondierende öffentliche Schlüssel wird durch die entsprechende Prüfstelle zertifiziert (SELMA-Zertifikat).

Beim Billing (Aktion *A10*) wird ein privater Signaturschlüssel benötigt, wenn die Rechnung in elektronischer Form an den Abnehmer ausgestellt wird. Will man ausschließlich elektronische Rechnungen und Gutschriften ohne Begleitdokumente austauschen, so greift ab dem 01.01.2002 die Rechtslage des § 14 Absatz 3 Nr. 1 Umsatzsteuergesetz. Es wird mindestens eine qualifizierte elektronische Signatur nach dem SigG gefordert. Das dazu nötige qualifizierte Zertifikat und das Schlüsselsystem werden von der externen Sig-CA erstellt und auf einer Chipkarte ausgegeben.

Zur Verwaltung der SELMA-Messgeräte werden verschiedene Management-Systeme verwendet. Das Security-Management erlaubt z.B. Schlüssel-Updates, das Rechte-Management und das Stellen der Uhrzeit. Die Parametrisierung der Messgeräte ist über das Messgeräte-Management möglich. Mit dem Software-Management lässt sich die Software der Messgeräte verwalten und updaten. Die Management-Funktionen können nur von autorisierten Stellen ausgeführt werden. Dazu werden die nötigen Kommandos

digital signiert und die Berechtigungen durch das Rechte-Management im Messgerät kontrolliert. Da es bei den Management-Funktionen – z.B. bei der Parametrierung oder beim Software-Download – Komponenten gibt, die eichpflichtig sind und nur von hoheitlich tätigem Personal (Eichbeamter oder staatlich anerkannter Prüfstellenleiter) ausgeführt werden dürfen, wird zwischen dem Management eichpflichtiger und nicht-eichpflichtiger Komponenten unterschieden. Beim Management eichpflichtiger Komponenten sind die Anforderungen des Eichrechts zu berücksichtigen.

Findet eine der in Abbildung 1 dargestellten Transaktionen über ein unsicheres Netz statt und beinhaltet diese personenbezogene Daten i.S.d. Datenschutzrechts oder soll sie aus anderen Gründen vertraulich sein, so muss die Übertragung verschlüsselt werden. Die Kommunikation in Transaktion *T01* muss hingegen nicht vor dem Abhören geschützt werden, da die übertragenen Messdaten keinen Personenbezug enthalten, sondern pseudonymisiert sind. In der Datenerfassungsstelle werden die Daten zur Weiterverarbeitung einer natürlichen Person zugeordnet. Bei allen weiteren Transaktionen kommen daher Verschlüsselungskomponenten zum Einsatz, die eine transportgebundene Vertraulichkeit realisieren.

3 Elektronische Signaturen im SELMA-Umfeld

In diesem Kapitel werden die im SELMA-System von den Messgeräten und den Messgeräte-äquivalenten Systemen verwendeten elektronischen Signaturen nach dem Signaturgesetz [SG01] klassifiziert. In Frage kommt eine Einordnung als fortgeschrittene elektronische Signatur nach § 2 Nr. 2 SigG oder als qualifizierte elektronische Signatur nach § 2 Nr. 3 SigG.

3.1 Klassifikation als fortgeschrittene elektronische Signatur

Eine fortgeschrittene elektronische Signatur ist gemäß § 2 Nr. 2 SigG eine elektronische Signatur, die

a) ausschließlich dem Signaturschlüssel-Inhaber zugeordnet ist,

b) die Identifizierung des Signaturschlüssel-Inhabers ermöglicht,

c) mit Mitteln erzeugt wird, die der Signaturschlüssel-Inhaber unter seiner alleinigen Kontrolle halten kann und

d) mit den Daten, auf die sie sich bezieht, so verknüpft ist, dass eine nachträgliche Veränderung der Daten erkannt werden kann.

Zunächst müssen im SELMA-Konsortium die Signaturschlüssel eindeutig einem Signaturschlüssel-Inhaber zugeordnet sein. Aus der Definition des Begriffs des Signaturschlüssel-Inhabers in § 2 Nr. 9 SigG als natürliche Person, die Signaturschlüssel besitzen und denen die zugehörigen Signaturprüfschlüssel durch qualifizierte Zertifikate zugeordnet sind, ergeben sich hinsichtlich der Verwendung fortgeschrittener elektronischer

Signaturen im SELMA-Verfahren zwei Probleme. Zum einen können nach dem Wortlaut des § 2 Nr. 9 SigG Signaturschlüssel nur natürlichen Personen zugeordnet werden, wohingegen im SELMA-Forschungsvorhaben der Schlüssel einem SELMA-Messgerät zugeordnet ist. Zum anderen kann diese Zuordnung nur durch qualifizierte Zertifikate vorgenommen werden, was die Anwendung fortgeschrittener elektronischer Signaturen ausschließt. Beide Vorschriften sind zu weitreichend und widersprechen dem Sinn und Zweck der Regelung hinsichtlich fortgeschrittener elektronischer Signaturen. Nach dem Sinn und Zweck des § 2 Nr. 9 SigG gilt diese Vorschrift deshalb nur für qualifizierte Signaturen. Dies ergibt sich aus einer systematischen Auslegung dieser Vorschrift im Zusammenhang mit § 2 Nr. 7 SigG, nach dem qualifizierte Zertifikate ebenfalls nur für natürliche Personen ausgestellt werden können. Der Anwendungsbereich des § 2 Nr. 9 SigG wird insoweit durch Auslegung teleologisch reduziert. Daraus folgt, dass fortgeschrittene elektronische Signaturen anders als qualifizierte elektronische Signaturen nicht einer natürlichen Person zugeordnet sein müssen, sondern wie im SELMA-Forschungsprojekt einem Messgerät zugeordnet sein können. Die Voraussetzung des § 2 Nr. 2 lit. a) SigG ist somit erfüllt.

Die Voraussetzung des § 2 Nr. 2 lit. b) SigG wird dadurch erfüllt, dass jedes Messgerät einen unterschiedlichen privaten Schlüssel zum Signieren der Nachrichten erhält, so dass die Zuordnung des Schlüssels zum Messgerät gewährleistet ist. Darüber hinaus wird durch die Verwendung des SELMA-Zertifikats die Identifizierung des Messgeräts als Signaturschlüssel-Inhaber sichergestellt. Das Erfordernis des Zertifikats ergibt sich aus der amtlichen Begründung des Gesetzgebers zum Signaturgesetz [BSG00]. Auch pseudonymisierte Bezeichnungen wie die des Messgeräts erfüllen die Identifikationsfunktion (http://www.regtp.de/tech_reg_tele/start/in_06-02-03-00-00_m/#FAQ 19).

Des Weiteren wird die Signatur im MIM des Messgeräts erzeugt, das sowohl durch eine Eichplombe als auch durch zertifizierte Soft- und Hardware-technische Sicherungen vor dem Auslesen geschützt ist. Der Signaturschlüssel wird vor der Inbetriebnahme in dem Gerät generiert und nur dort gespeichert. Selbst die Neugenerierung privater Schlüssel kann nur von außen angestoßen werden. Sie werden nicht außerhalb des Geräts generiert und von außen in das MIM des Geräts geladen. Aufgrund dieser Tatsachen stellen die verwendeten Signaturschlüssel i.S.d. § 2 Nr. 2 lit. c) SigG Mittel dar, die der Signaturschlüssel-Inhaber unter seiner alleinigen Kontrolle halten kann.

Schließlich gewährleisten die i.R.d. elektronischen Signaturen eingesetzten asymmetrischen kryptographischen Verfahren und die sicheren Hash- und Signaturalgorithmen und -parameter, dass Messdaten und Signaturen derart miteinander verknüpft sind, dass eine nachträgliche Veränderung der Daten erkannt werden kann. Somit erfüllen die von den Messgeräten verwendeten Schlüsselsysteme die Anforderungen des Signaturgesetzes an fortgeschrittene elektronische Signaturen.

3.2 Klassifikation als qualifizierte elektronische Signatur

Fraglich ist, ob die im SELMA-Konsortium verwendeten elektronischen Signaturen darüber hinaus die Anforderungen des Signaturgesetzes an qualifizierte elektronische Signaturen erfüllen. Der Einsatz qualifizierter Signaturen ermöglicht umfassendes

rechtsverbindliches Handeln im elektronischen Rechtsverkehr [HO03]. Dazu müssten die verwendeten Signaturen gemäß § 2 Nr. 3 SigG zusätzlich zu den Anforderungen an fortgeschrittene elektronische Signaturen

a) auf einem zum Zeitpunkt ihrer Erzeugung gültigen qualifizierten Zertifikat beruhen und

b) mit einer sicheren Signaturerstellungseinheit erzeugt werden.

Qualifizierte Zertifikate sind gemäß § 2 Nr. 7 SigG elektronische Bescheinigungen, die für natürliche Personen ausgestellt werden, die einen bestimmten gesetzlich vorgeschriebenen Inhalt haben (§ 7 SigG) und deren Zertifizierungsdiensteanbieter bestimmten gesetzlichen Anforderungen genügen muss (Anforderungen der §§ 4 bis 14 oder des § 23 SigG und der Signaturverordnung (SigV) [SV01]).

Zwar können qualifizierte elektronische Signaturen auch im automatischen Verfahren generiert werden [RF04]. Solche Signaturen werden dem Betreiber einer Datenverarbeitungsanlage (DV-Anlage) als natürlicher Person dann zugerechnet, wenn der Einsatz der Anlage auf seinem Willen beruht und er sich die von der DV-Anlage hergestellte Erklärung als eigene zurechnen lassen will [ME04]. Allerdings bedarf die qualifizierte Signatur wie die eigenhändige Unterschrift einer natürlichen Person als Aussteller. Die alleinige Zuordnung der qualifizierten Signatur zu einer natürlichen Person rechtfertigt sich aus dem Sinn und Zweck der Regelung, die qualifizierte Signatur der eigenhändigen Unterschriften gleichzustellen. Dies ist europa-rechtlich durch Art. 5 Abs. 1 SigRL vorgegeben [EGS00]. Darüber hinaus ist die betroffene Person, auf die die automatisiert erzeugten Signaturen zurückgeführt werden können, einem großen Haftungsrisiko ausgesetzt. Um dem entgegen zu wirken müsste man deswegen innerbetriebliche Haftungsübernahmeregelungen und Vorkehrungen für den Fall des Ausscheidens des verantwortlichen Mitarbeiters treffen.

Nach den Vorgaben der SELMA-Konsortialpartner werden die Zertifikate auf die Messgeräte ausgestellt und nicht auf eine natürliche Person. Es ist keine natürliche Person bestimmt worden, der die Erklärungen der Messgeräte und der Messgeräte-äquivalenten Geräte unter Übernahme des Haftungsrisikos zugerechnet werden.

Es kommen im Rahmen des SELMA-Forschungsvorhabens also keine qualifizierten Zertifikate zum Einsatz. Die verwendeten elektronischen Signaturen sind somit nicht als qualifizierte elektronische Signaturen nach § 2 Nr. 3 SigG zu klassifizieren. Hinsichtlich der Rechtsgültigkeit der Erklärung hat dies keine negativen Auswirkungen. Die Verwendung qualifizierter elektronischer Signaturen für die Energieabrechnung ist weder gesetzlich noch rechtsgeschäftlich vorgeschrieben. Allerdings bedeutet dies hinsichtlich des Beweiswerts der verwendeten Signaturen, dass die Signaturen nicht von der Anscheinsbeweisregelung des § 292a ZPO profitieren. Sie unterliegen der freien richterlichen Beweiswürdigung nach § 286 ZPO. Je nach der verwendeten Technik können fortgeschrittene elektronische Signaturen allerdings verschiedene Sicherheitsgrade aufweisen. Im Folgenden soll das Maß der Sicherheit der im SELMA-Forschungsvorhaben verwendeten Signaturen anhand eines Vergleichs des SELMA-Sicherheitsstandards mit den gesetzlichen Vorgaben zur qualifizierten elektronischen Signatur bestimmt werden.

3.3 Wertung der Beweiswirkung der elektronischen Signaturen im SELMA-Umfeld

Da das SELMA-Konsortium hinsichtlich der verwendeten elektronischen Signaturen eine hohe Beweiskraft anstrebt, hat es sich zum Ziel gesetzt, soweit wie möglich die technischen Voraussetzungen für qualifizierte Signaturen zu erfüllen. Die organisatorischen Voraussetzungen (das Ausstellen qualifizierter Zertifikate, die Aufsetzung und der Betrieb einer Public-Key-Infrastruktur, etc.) sind dagegen nicht Gegenstand von SELMA.

3.3.1 Sicherungsinfrastruktur

Das SigG stellt i.V.m. der SigV eine Vielzahl organisatorischer Anforderungen auf, die ein ZDA bei der Ausstellung qualifizierter Zertifikate zu beachten hat. Diese Anforderungen gelten nicht hinsichtlich der im SELMA-Verfahren verwendeten fortgeschrittenen elektronischen Signaturen. Die Aufgaben des ZDA übernehmen im SELMA-Verfahren die Eichbehörden bzw. die staatlich anerkannten Prüfstellen. Die Prüfstellenleiter stellen SELMA-Zertifikate und die Certificate Revocation List (CRL) aus.

Da Veränderungen an SELMA-Zertifikaten wegen ihrer SigG-konformen elektronischen Signatur rückverfolgt werden können, sind die Zertifikate auch vor Angriffen aus der Sphäre des Trust-Centers hinreichend geschützt. An die Prüfstellen werden deswegen nicht die gleichen hohen organisatorischen Anforderungen gestellt, wie sie das SigG für ZDA vorsieht. Hauptaufgabe der Prüfstellen ist es, die Zertifikate zu erzeugen und zuverlässig verfügbar zu machen. Anders als das dem Signaturgesetz zugrunde liegende Regelungsprinzip, demzufolge die Sicherheit der elektronischen Signatur durch technische und organisatorische Vorkehrungen gewährleistet wird, legt das SELMA-Sicherheitskonzept den Schwerpunkt auf die Sicherheit der verwendeten Technik:

- So wie der ZDA Personen, die ein qualifiziertes Zertifikat beantragen, zuverlässig zu identifizieren hat (§ 5 Abs. 1 S. 1 SigG), identifiziert die Prüfstelle zuverlässig das Messgerät anhand der digitalen Signatur und generiert daraufhin das SELMA-Zertifikat.

- Ebenso wie der ZDA gemäß § 5 Abs. 1 S. 2 SigG hat der SDS das Zertifikat jederzeit für jeden über öffentlich erreichbare Kommunikationsverbindungen nachprüfbar und abrufbar zu halten.

- Die SELMA-Zertifikate werden bei der Inbetriebnahme des Messgeräts durch den Verteilungsnetzbetreiber ausgelesen. Die Daten des Zertifikats können gemäß § 5 Abs. 4 S. 1 SigG nicht unbemerkt gefälscht oder verfälscht werden. Eine Fälschung würde bei Überprüfung der digitalen Signatur durch den Vergleich der Hashwerte bemerkt werden. Die Zertifikate werden vom Verteilnetzbetreiber (VNB) auf diese Weise unverfälscht an den SDS zur Verbreitung weitergeleitet.

- Da der Signaturschlüssel im MIM des Messgeräts generiert und gespeichert wird und nicht ausgelesen werden kann, verbleibt der private Schlüssel immer in der Signaturerstellungseinheit des Messgeräts. Damit hat das SELMA-Konsortium gemäß § 5 Abs. 4 S. 2 SigG Vorkehrungen getroffen, um die Geheimhaltung der Signaturschlüssel zu gewährleisten.

- Auch der Inhalt des SELMA-Zertifikats entspricht den Angaben des § 7 SigG für qualifizierte Zertifikate, da es nach dem X.509v3-Standard aufgebaut ist.

Zusammenfassend erfüllt das SELMA-Forschungsvorhaben die Vorschriften der technischen Anforderungen an Zertifizierungsdiensteanbieter.

Eine Einschränkung erfährt diese Wertung hingegen dadurch, dass bis zum jetzigen Zeitpunkt noch offen ist, wer den SDS betreiben wird. Somit kann noch keine Aussage über die Zuverlässigkeit und die interne Betriebsorganisation des SDS getroffen werden. Dies betrifft insbesondere die Anforderungen an den Nachweis der erforderlichen Zuverlässigkeit und Fachkunde (§ 4 Abs. 2 S. 1-3 SigG) und an das Sicherheitskonzept (§ 4 Abs. 2 S. 4 SigG i.V.m. § 2 SigV).

3.3.2 Sicherheit der verwendeten technischen Komponenten

Das SigG stellt eine Vielzahl von Anforderungen an die Sicherheit der beim Einsatz qualifizierter Signaturen verwendeten technischen Komponenten. Diese betreffen die für den Einsatz qualifizierter Signaturen geforderten sicheren Signaturerstellungseinheiten.

Sichere Signaturerstellungseinheiten sind gemäß § 2 Nr. 10 SigG Software- und Hardwareeinheiten zur Speicherung und Anwendung des jeweiligen Signaturschlüssels, die mindestens die Anforderungen nach § 17 oder § 23 SigG und der SigV erfüllen und die für qualifizierte elektronische Signaturen bestimmt sind.

Gemäß § 17 Abs. 1 SigG erfüllen sichere Signaturerstellungseinheiten folgende Voraussetzungen:

a) Sie machen Fälschungen der Signaturen und Verfälschungen signierter Daten zuverlässig erkennbar und

b) sie schützen gegen unberechtigte Nutzung der Signaturschlüssel.

Die erstgenannten Sicherheitsfunktionen erfüllen elektronische Signaturen auf der Basis asymmetrischer Verschlüsselungssysteme. Der Signierungsprozess basiert auf standardisierten Verfahren. Im SELMA-Projekt werden als Signaturalgorithmus elliptische Kurven auf der Basis des ECDSA zur Signaturschlüsselgenerierung, Signaturerstellung und Signaturprüfung verwendet. Sie weisen eine Schlüssellänge von mindestens 192 bit auf und verwenden als Hashfunktion SHA-1. Zur Generierung des Schlüsselpaares wird ein physikalischer Zufallszahlengenerator, wie z.B. im Infineon SLE66CX640P vorhanden, verwendet. Die RegTP hat ECDSA als für die Erzeugung der Signaturschlüssel und SHA-1 für das Hashen der zu signierenden Daten als geeignet bewertet und zur Erzeugung der Schlüssel physikalische Zufallsgeneratoren ausdrücklich empfohlen [RTP04].

Die letztgenannte Voraussetzung erfüllen sichere Signaturerstellungseinheiten dadurch, dass der Signaturschlüssel erst nach Identifikation des Inhabers durch Besitz und Wissen oder durch Besitz und biometrisches Merkmal angewendet werden kann (§ 15 Abs. 1 S. 1 SigV) sowie dadurch, dass der Signaturschlüssel sich nicht aus Signaturprüfschlüssel und Nachricht errechnen lässt und nicht duplizierbar ist (§ 15 Abs. 1 S. 4 SigV). Problematisch für die Verwendung automatisiert erzeugter elektronischer Signaturen ist lediglich das Erfordernis des § 15 Abs. 1 S. 1 SigV, nach dem sich der Inhaber des Signaturschlüssels vor der Verwendung des Schlüssels durch Besitz und Wissen bzw. durch Besitz und ein biometrisches Merkmal ausweisen muss. Das Gesetz geht von dem Normalfall aus, dass eine natürliche Person sich einer Signaturerstellungseinheit bedient, um eine Nachricht zu signieren. In diesem Fall besteht die Gefahr, dass ein Unbefugter elektronische Signaturen generieren kann, die sich die in der Signatur ausgewiesene Person zurechnen lassen muss. Im SELMA-Projekt hingegen ist die Signaturerstellungseinheit im Messgerät zum einen durch die Eichplombe zum anderen durch hard- und softwaretechnische Sicherungen vor der Benutzung durch Unbefugte geschützt. Ein Zugriff von außen ist nur nach Identifikation durch einen elektronisch signierten Request möglich. Eines weiteren Identifikationsmerkmals wie einer PIN oder eines biometrischen Merkmals bedarf es deswegen nicht.

Des Weiteren ist gemäß § 17 Abs. 3 SigG (i.V.m. § 15 Abs. 3 SigV) sicherzustellen, dass die technischen Komponenten für Zertifizierungsdienste

a) bei Erzeugung und Übertragung von Signaturschlüsseln die Einmaligkeit und Geheimhaltung der Signaturschlüssel gewährleisten und eine Speicherung außerhalb der sicheren Signaturerstellungseinheiten ausschließen und

b) qualifizierte Zertifikate, die gemäß § 5 Abs. 1 S. 2 SigG nachprüfbar oder abrufbar gehalten werden, vor unbefugter Veränderung und unbefugtem Abruf schützen.

Die erste Voraussetzung wird durch die Art der Schlüsselgenerierung im MIM des Messgeräts, das eine Übertragung der Signaturschlüssel ausschließt, erfüllt. I.R.d. SELMA-Verfahrens werden die Anforderungen an sichere Signaturerstellungskomponenten, wie sie für den Einsatz qualifizierter elektronischer Signaturen gelten, durch akkreditierte Prüfstellen evaluiert und von einer zugelassenen Zertifizierungsstelle nach den technischen Regelwerken Common Criteria EAL 4 plus bzw. nach ITSEC E3 hoch zertifiziert (§ 17 Abs. 4 i.V.m. § 18 SigG i.V.m. § 16 SigV). Die Anforderungen an die Sicherheit der SELMA-Zertifikate werden durch die Verwendung signaturgesetzkonformer asymmetrischer Schlüsselsysteme eingehalten.

Schließlich werden durch die verwendeten Management-Systeme und die Eintragung von Veränderungen in Logbücher sicherheitstechnische Veränderungen an technischen Komponenten nach § 15 Abs. 1-3 SigV für den Nutzer erkennbar (§ 15 Abs. 4 SigV).

Ein Problem für die Beweiswürdigung ergibt sich aus der langen Gültigkeit der SELMA-Schlüsselsysteme. Das SELMA-Konsortium hat sich darauf verständigt, dass die Gültigkeit der SELMA-Schlüsselsysteme 23 Jahre beträgt. Dieser lange Zeitraum wurde deswegen gewählt, um den Aufwand für Schlüssel- und Zertifikatsmanagement gering zu

halten. Dies steht im Widerspruch zum Gültigkeitszeitraum qualifizierter Zertifikate, der nach § 14 Abs. 3 SigV höchstens fünf Jahre beträgt. Diese Frist für die Aufbewahrung qualifizierter Zertifikate zur Nachprüfung beträgt gemäß § 4 Abs. 1 SigV weitere fünf Jahre, so dass qualifizierte Signaturen maximal zehn Jahre nachprüfbar sind. Eine Ausnahme von diesem Gültigkeitszeitraum besteht dann, wenn die eingesetzten Algorithmen und zugehörigen Parameter sich als ungeeignet erwiesen haben. In diesem Fall endet die Gültigkeit bereits vor Ablauf der gesetzlichen Frist. Die gesetzliche Frist ist eine Vermutungsregel für die Sicherheit der verwendeten Technik. Diese Vermutung wird dementsprechend widerlegt, sobald die verwendete Technik sich als unsicher herausgestellt hat. Daraus folgt der Vorrang der technischen Analyse vor der gesetzlichen Vermutungswirkung. Gleiches gilt für die im Rahmen des SELMA-Konsortiums verwendeten elektronischen Signaturen. Auch sie verlieren ihre Gültigkeit, sobald die Technik sich als unsicher erwiesen hat. Die abweichende Regelung der Geltungsdauer spielt demgegenüber eine untergeordnete Rolle. Ausschlaggebend bleibt die Sicherheit der verwendeten Technik. Deswegen sind die kryptographischen Systemparameter und insbesondere die Schlüssellänge für den entsprechenden Zeitraum nach den Maßgaben der RegTP zu wählen [RTP04]. Außerdem muss in Stichprobenverfahren zur Verlängerung der Eichgültigkeit, die Prüfung der kryptographischen Systemparameter (Kurve, Kurvenparameter, Schlüssellängen, etc.) integriert werden. Unter Berücksichtigung dieser Faktoren ist die Geltungsdauer von 23 Jahren zulässig und unter dem Gesichtspunkt der Datensicherheit vertretbar, wenn innerhalb dieses Zeitraums die technische Sicherheit positiv festgestellt wird.

4 Zusammenfassung

Voraussetzung für einen funktionierenden liberalisierten Wettbewerb in der Energiewirtschaft ist die zeitnahe Bereitstellung von Informationen zu gemessenen Energiemengen für Abrechnungszwecke. Alle berechtigten Marktteilnehmer müssen daher diskriminierungsfrei und neutral Zugang zu eichrechtlich gesicherten Energiemessdaten erhalten. Die Messdaten stellen im liberalisierten Energiemarkt Marktinformationen dar, die einen großen und wechselnden Teilnehmerkreis betreffen und für die auch aus der Sicht des Verbraucherschutzes hohe Anforderungen an die Sicherheit (Authentizität, Vertraulichkeit, Integrität) gelten müssen.

Im SELMA-Projekt ist der liberalisierte Energiemarkt analysiert und sind die Anforderungen an die Sicherheit aufgestellt worden. Darauf aufbauend ist eine Sicherheitsarchitektur erarbeitet worden, die den genannten Sicherheitsanforderungen genügt. So ist die Grundlage dafür geschaffen worden, dass geldwerte Energiemessdaten unabhängig vom Transportmedium sicher und ecommercefähig von dezentralen Messgeräten über offene Netze zu den Eigentümern und Nutzern der Messdaten übertragen werden können. Durch die SELMA-Technik ist die Vertrauenswürdigkeit der elektronisch ausgelesenen und ausgetauschten Energiemessdaten genauso hoch, wie die vom Display eines Messgeräts angezeigten Messdaten.

Die technischen Vorkehrungen des SELMA-Sicherheitskonzeptes vermitteln hinsichtlich der verwendeten technischen Komponenten ein der Sicherheit qualifizierter Signaturen vergleichbares Maß.

Literaturverzeichnis

[EGS00] Richtlinie 1999/93 EG des Europäischen Parlaments und des Rates über gemeinschaftliche Rahmenbedingungen für elektronische Signaturen vom 13. Dezember 1999, ABl. EG Nr. L 13 vom 19. Januar 2000.

[HO03] Holznagel, B.: Recht der IT-Sicherheit. München 2003, S. 57.

[LR+03] Lo Iacono, L., Ruland, Ch., Wahl, A.: Einsatz der elektronischen Signatur für den Messdatenaustausch im liberalisierten Energiemarkt, Telematik 2003 (VDI-Berichte 1785).

[ME04] Mehrings, in: Hoeren/Sieber, Handbuch Multimedia Recht, 13.1, Rn. 113, Stand: April 2004.

[PA04] PTB-A 50.7, Anforderungen an elektronische und softwaregesteuerte Messgeräte und Zusatzeinrichtungen für Elektrizität, Gas, Wasser und Wärme, Stand April 2004, abrufbar unter: http://www.ptb.de/de/org/q/q3/q31/ptb-a/_ptb-a.htm

[RTP04] RegTP, Bekanntmachung zur elektronischen Signatur nach dem Signaturgesetz und der Signaturverordnung (Übersicht über geeignete Algorithmen) vom 02. Januar 2004, BAnz. Nr. 30, S. 2537 ff., abrufbar unter: http://www.regtp.de/imperia/md/content/tech_reg_t/digisign/163.pdf

[RF04] Roßnagel, A., Fischer-Dieskau, S.: Automatisiert erzeugte elektronische Signaturen, MMR 2004, S. 133 ff.

[SG01] Gesetz über Rahmenbedingungen für elektronische Signaturen (Signaturgesetz-SigG) vom 16. Mai 2001, BGBl. I 2001, S. 876.

[BSG00] Amtliche Begründung zum Signaturgesetz vom 16.11.2000, BT-Drs. 14/4662, S. 18.

[SV01] Verordnung zur elektronischen Signatur (Signaturverordnung-SigV) vom 16. November 2001, BGBl. I 2001, S. 3074.

[X509] ITU-T-Recommendation X.509. Auch publiziert als ISO/IEC 9594-8: Information Technology – Open Systems Interconnection – The Directory: Public-Key and attribute certificate frameworks, Juni 1997.