

ICS 35.040; 35.240.99

Attribuierung eines Zertifikats basierend auf einem spezifischen Rollenmodell für das Internet der Energie (Energy Security Service)

Attribution of a certificate based on a specific role model for the Internet of energy (energy security services)

Attribution d'un certificat basé sur un modèle de rôle spécifique pour l'Internet de l'énergie (services de sécurité énergétique)

Zur Erstellung einer DIN SPEC können verschiedene Verfahrensweisen herangezogen werden:
Das vorliegende Dokument wurde nach den Verfahrensregeln einer PAS erstellt.

Gesamtumfang 31 Seiten

Bereich Innovation

Inhalt

	Seite
Vorwort	3
Einleitung.....	4
1 Anwendungsbereich	6
2 Begriffe	6
3 Symbole und Abkürzungen	10
4 Anforderungen	12
4.1 Allgemeines	12
4.2 Energiewirtschaft.....	12
4.3 IT-Sicherheit	12
5 Rollenmodell	13
5.1 Allgemeines	13
5.2 Rollen in der Energiewirtschaft	13
5.2.1 Allgemeines	13
5.2.2 Anschlussnehmer	15
5.2.3 Anschlussnutzer	15
5.2.4 Bilanzkreiskoordinator	15
5.2.5 Bilanzkreisverantwortlicher	15
5.2.6 Energiebörse	15
5.2.7 Energiehändler.....	15
5.2.8 Energielieferant.....	15
5.2.9 Erzeuger.....	16
5.2.10 Energieversorgungsunternehmen	16
5.2.11 Kommunikationsdienstleister	16
5.2.12 Mehrwertdienstleister.....	16
5.2.13 Messdienstleister.....	16
5.2.14 Messstellenbetreiber	17
5.2.15 Smart Architecture Betreiber.....	17
5.2.16 Übertragungsnetzbetreiber.....	17
5.2.17 Verteilnetzbetreiber	17
5.3 Authentifizierungsanwendungsfälle des ESS	17
5.3.1 Allgemeines	17
5.3.2 Anwendungsfall Zertifikatsausstellung.....	18
5.3.3 Anwendungsfall Authentifizierung	21
5.3.4 Anwendungsfall Zertifikatsüberprüfung	22
5.4 Authentifizierungsszenarien in den Geschäftsprozessen der Energiewirtschaft	25
5.4.1 Allgemeines	25
5.4.2 ESS-Authentifizierungsszenario: Lieferbeginn (GPKE).....	25
6 Attribute des Security Tokens	28
6.1 Allgemeines	28
6.2 Zertifikatskörper.....	28
6.3 Namensschema Issuer und Subject	29
6.4 Extension Smart Architecture Role	30
Literaturhinweise	31

Vorwort

Die DIN-Spezifikation wurde im Forschungsprojekt „Smart Watts“, Teilvorhaben Smart Architecture) erstellt. Das Vorhaben wurde gefördert vom Bundesministerium für Wirtschaft und Technologie im Rahmen des Förderprogramms E-Energy (Förderkennzeichen Teilvorhaben Smart Architecture: 01ME08015).

Koordiniert wurde die Erarbeitung des Dokuments durch die nachfolgend genannten Verfasser, die allein verantwortlich für den Inhalt sind:

- Dipl.-Inform. Julian Krenge, MBA, Forschungsinstitut für Rationalisierung (FIR) e. V.
an der RWTH Aachen
- Dipl.-Inform. Violetta Panahabadi, Forschungsinstitut für Rationalisierung (FIR) e. V.
an der RWTH Aachen

Das Dokument wurde erstellt unter aktiver Mitarbeit von folgenden Personen und Unternehmen:

- Dieter Bong, Utimaco Safeware AG
- Guido Bunsen, Rechen- und Kommunikationszentrum RWTH Aachen
- Robert Delahaye, Utilicount GmbH & Co. KG
- Hauke Hinrichs, STAWAG AG
- Dr. Frank Pallas, Karlsruher Institut für Technologie (KIT)
- Andreas Philipp, Utimaco Safeware AG
- Martin Pöppe, SOPTIM AG
- Michaela Schraad, Rechen- und Kommunikationszentrum RWTH Aachen

Es wird auf die Möglichkeit hingewiesen, dass einige Texte dieses Dokuments Patentrechte berühren können. Das DIN [und/oder die DKE] sind nicht dafür verantwortlich, einige oder alle diesbezüglichen Patentrechte zu identifizieren.

Das Thema dieser DIN-Spezifikation ist nicht Gegenstand eines nationalen, europäischen oder internationalen Normungsvorhabens. Es existiert jedoch die DIN-Spezifikation DIN SPEC 91214:2011-03, Identifikationsschema und Namensdienst im Internet der Energie (Energy Name Service).

Einleitung

In Zeiten sich ändernder Rahmenbedingungen in der deutschen Energiewirtschaft ist es von Notwendigkeit, dass der Wettbewerb auf den Energiemärkten durch größere Differenzierungsmöglichkeiten und durch einen verbesserten Systemzugang gefördert wird. Energiesysteme sollen eine höhere Aufnahmefähigkeit für erneuerbare und dezentral erzeugte Energien vorweisen. Auch die Prozesse im Energiehandel sollen effizienter gestaltet werden und die vorhandene Infrastruktur soll durch ein effizienteres Lastmanagement und einen sparsameren Energieeinsatz wirksamer genutzt werden.

Eine der großen Herausforderungen zur effizienten Gestaltung des Energiehandels und Energieverbrauchs ist die Anzahl und Vielzahl der Marktteilnehmer, Anlagen und Geräte, die im Rahmen ihrer jeweiligen Tätigkeit täglich größere Mengen an Informationen und Daten austauschen, Transaktionen durchführen, Verträge schließen und Versorgungsgeschäfte abwickeln. Damit dieser enorme Informationsaustausch im Markt in sicherer und vor allem in effizienter Art und Weise abläuft, wird ein spezifisches Informationslogistikkonzept für die Energiebranche benötigt.

Die Entwicklung der entsprechenden Informationslogistik und Anreizsysteme ist Gegenstand des Forschungsprojekts Smart Watts. Konkret wurde eine Infrastruktur für das sog. „Internet der Energie“ entworfen, die auf dem Konzept der losen Kopplung von Informationstechnologie-Systemen (IT-Systemen) basiert. In dieser Infrastruktur, „Smart Architecture“ (SMA) genannt, können Informationen zwischen Organisationen und Systemen ohne hohen Einrichtungsaufwand ausgetauscht werden.

Technisch basiert die SMA auf Web-Services, die eine Kommunikation der verschiedenen Akteure und Systeme innerhalb der Energiewirtschaft ermöglichen. Zur Koordination der Kommunikation werden die Funktionen der SMA in sechs Basis-Services gebündelt und angeboten. Das Namensschema des „Energy Name Service“ (ENS) dient der Identifikation von Objekten im Internet der Energie und ist bereits als DIN SPEC 91214 veröffentlicht. Der ENS setzt das Namensschema als Teil des DNS um, wodurch er sich nahtlos in die globale Domainstruktur einfügt. Dies erlaubt analog zum DNS die Zuweisung von mehreren Identifikatoren zu einem Objekt im Internet der Energie.

Die SMA stellt ein intelligentes, IKT-basiertes Bindeglied für unternehmensübergreifende Geschäftsprozesse dar. Folglich muss sie die funktionalen und nicht-funktionalen Anforderungen an eine flexible und offene Architektur des Internets der Energie berücksichtigen. Hierbei spielt die Umsetzung eines IT-Sicherheitskonzepts bei der Entwicklung der SMA eine entscheidende Rolle, welches die wesentliche Aufgabe hat, kommunizierende Akteure der SMA während des Informationsaustausches durch den Angriff von Dritten zu schützen. Es muss gegen Vertraulichkeitsverletzung, Manipulation sowie Störung der Informationsübertragung durch entsprechende Vorkehrungen und Beachtung von IT-Security-Policies präventiv vorgegangen werden.

Der Basis-Service „Energy Security Service“ (ESS) setzt das Sicherheitskonzept für die SMA um. Hauptbestandteile des Sicherheitskonzeptes des ESS ist die Umsetzung einer Registrierung der Objekte der SMA, die Zertifikatsvergabe und eines Single-Sign-On Verfahrens (SSO). Durch das SSO-Verfahren wird einem Subjekt ermöglicht, durch eine einmalige Authentifizierung für mehrere Dienste authentifiziert zu sein. Die technische Umsetzung kann durch ein Ticket-Verfahren in einer Public-Key-Infrastruktur (PKI) realisiert werden. Hier wird einem Subjekt nach der Authentifizierung durch den ESS ein „digitales Zertifikat“ (auch „Ticket“ oder „Security Token“ genannt) ausgestellt, wodurch das Subjekt für alle anderen Dienste einen Authentifizierungsnachweis besitzt.

Für die Erstellung von digitalen Zertifikaten bzw. Security Tokens existieren mehrere Standards. Für den ESS wurde der X.509 Standard [siehe RFC 3280 und RFC 5280] gewählt, durch den eine Referenzstruktur für das Zertifikat X-509.v3 [siehe RFC 5280] vorgegeben wird. Dabei bietet dieser Standard die Möglichkeit der Token-Erweiterung, welche für die Authentifizierung von Subjekten speziell für die SMA spezifiziert wurden. Im Besonderen ist es notwendig, die Rolle des zu autorisierenden Subjekts in dem Security Token zu hinterlegen, damit der Betreiber eines Dienstes (Service-Betreiber) identifizieren kann, ob das jeweilige Subjekt als Anbieter oder Konsument bestimmter Informationen innerhalb des Geschäftsprozesses agiert.

In dieser DIN SPEC werden sogenannte Pseudonymzertifikate nicht betrachtet. Der entworfene Security Token richtet sich vor allem an die kritischen Prozesse, wie die Wechselprozesse im Messwesen (WiM) und Geschäftsprozesse zur Kundenbelieferung mit Elektrizität (GPKE), bei denen gegenseitige Kenntnis der Identität notwendig ist. Der Energy Security Service an sich erlaubt auch Pseudonymzertifikate, welche jedoch in diesem Dokument nicht spezifiziert sind.

Ergebnis dieser DIN SPEC ist ein für die Energiewirtschaft spezifisches Rollenmodell für den ESS zur Ausführung des Authentifizierungsprozesses. Basierend auf diesem Rollenmodell ist die Attribuierung des „Energy Security Tokens“ (EST) für den ESS vorgenommen.

1 Anwendungsbereich

Dieses Dokument richtet sich an interessierte Einrichtungen in der Energiewirtschaft, welche sich mit den Fragen der Gestaltung des überbetrieblichen Informationsaustausches beschäftigen. Dieses Dokument richtet sich sowohl an Entwickler eines Betreibers einer IT-Architektur als auch an Entwickler der Konsumenten, die die Dienste der IT-Architektur in Anspruch nehmen.

Durch dieses Dokument wird ein **spezifiziertes Rollenmodell für die Authentifizierung im Internet der Energie** definiert, um den Authentifizierungsprozess zwischen verschiedenen Akteuren und folglich heterogenen IT-Architekturen zu realisieren. Basierend auf den definierten Rollen im spezifizierten Rollenmodell wird es dem ESS ermöglicht einen Energy Security Token (EST) auszustellen, mit dem sich ein Subjekt bei anderen Diensten oder Akteuren authentifiziert. Für die Umsetzung werden bereits etablierte Sicherheitskonzepte und Sicherheitsstandards verwendet. Sowohl für die Verschlüsselung als auch Signierung von Nachrichten werden die bekannten Sicherheitsstandards verwendet.

Für das digitale Zertifikat ist eine Erweiterung notwendig, um die Besonderheiten des Strommarkts zu berücksichtigen und eine entsprechende Identitätskontrolle zu erlauben. Im Fokus steht die Freigabe der verschiedenen in der Energiewirtschaft relevanten Informationsobjekte und Prozesse. Basierend auf dem definierten Rollenmodell werden die jeweiligen Erweiterungen des „Energy Security Tokens“ definiert, so dass für die jeweiligen Akteure sichtbar wird, in welcher Funktion (Provider oder Consumer) ein Subjekt eine bestimmte Information anfordert.

2 Begriffe

Für die Anwendung dieses Dokuments gelten die folgenden Begriffe.

2.1

Akteur

(en: actor)

handelnde Person in einer Wirkungsdomäne, der eine Rolle zugeordnet ist

[QUELLE: Die Deutsche Normungsroadmap E-Energy/Smart Grid, S. 18]

Anmerkung 1 zum Begriff: Abweichend zur Deutschen Normungsroadmap sind Akteure nur Personen, keine Elemente.

2.2

Anwendungsfall

(en: use case)

gebündelte Betrachtung aller Fälle, die bei der Erreichung eines Zieles eintreten können

[QUELLE: Die Deutsche Normungsroadmap E-Energy/Smart Grid, S. 19]

2.3

Attribuierung

(en: attribution)

Zuschreibung von Eigenschaften und Verhalten

2.4

Authentifizierung

(en: authentication)

Überprüfung der angegebenen Identität einer Entität

[QUELLE: DIN EN ISO/IEC 19762-1:2012-06]

2.5**Autorisierung**

(en: authorization)

Methode zur Sicherstellung, dass Produkte oder Personen, die auf Informationen, Funktionen oder Services zugreifen, auch die Berechtigung dazu haben

[QUELLE: DIN EN 50491-4-1:2012-11]

2.6**Berechtigung**

(en: access)

Freigabe, Erlaubnis oder Ermächtigung für einen Benutzer oder eine Komponente für eine Aktivität

[QUELLE: DIN EN 50132-5-1:2012-11]

2.7**Datenschutz**

(en: information privacy)

Schutz sensibler Daten

2.8**Dienst**

(en: service)

Bereitstellung von Funktionalität über eine definierte Schnittstelle

[QUELLE: DIN SPEC 91214:2011-03]

2.9**Eigentümer**

(en: owner)

Akteur, der die rechtliche Herrschaft über eine Sache hat

2.10**Element**

(en: element)

physisches oder logisches Ding im Internet der Energie, das nicht vertragsfähig ist

[QUELLE: DIN SPEC 91214:2011-03]

2.11**Entität**

(en: entity)

jedes konkrete oder abstrakte Objekt einschließlich Assoziationen zwischen Gegenständen

[QUELLE: DIN EN 61360-1:2004-12]

2.12**Gruppe**

(en: group)

Ansammlung beliebig vieler Objekte einer oder verschiedener Objektklassen

[QUELLE: DIN SPEC 91214:2011-03]

2.13**Identifikationsschema**

(en: identification scheme)

eine formale Sprache zur Darstellung von Identifikatoren

[QUELLE: DIN SPEC 91214:2011-03]

2.14

Identifikator

id

(en: identifier)

Bezeichner zur Identifikation, der alle notwendige Information enthält, um das, was identifiziert werden soll, von allem anderen innerhalb des Identifikationsbereichs zu unterscheiden

[QUELLE: DIN SPEC 91214:2011-03]

Anmerkung 1 zum Begriff: Vergleiche Uniform Resource Identifiers in RFC 3986

2.15

Identität

(en identity)

Relation, die eintritt, wenn zwei oder mehr Objekte in ihren signifikanten Eigenschaften übereinstimmen

[QUELLE: DIN 31646:2013-01]

Anmerkung 1 zum Begriff: Technisch wird dies durch einen Identifikator umgesetzt.

2.16

Internet der Energie

ioe

(en: internet of energy)

Ansammlung aller Objekte (Organisationen, Personen, Geräte, usw.) die mittels Informations- und Kommunikationstechnologie (IKT) zum Zwecke einer effizienten Energieversorgung über das Internet miteinander kommunizieren oder referenziert werden, sowie deren Beziehungen zueinander

[QUELLE: DIN SPEC 91214:2011-03]

2.17

Kunde

(en: customer)

Person oder Organisation, die eine Leistung im Rahmen einer geschäftlichen Beziehung mit einem Leistungsanbieter erhält

[QUELLE: DIN EN 1545-2:2006-02]

2.18

Lastgangmessung

(en: load course measurement)

zeitbezogene Bedarfsermittlung elektrischer Leistung

2.19

Leistungs-Frequenz-Regelung

(en: power and frequency control)

Regelverfahren zur Einhaltung der elektrischen Größen an den Grenzen der Regelzonen von Übertragungsnetzbetreibern (ÜNB)

2.20

Messsystem

(en: measuring system)

komplette Zusammenstellung von Messinstrumenten und anderen Geräten zur Durchführung bestimmter Messungen

[QUELLE: DIN EN ISO 14532:2007-09]

2.21

Nutzer

(en: user)

Person, die einen Anschluss oder Dienst in Anspruch nimmt

2.22

Objekt

(en: object)

abstraktes Konzept zur Erfassung physischer und logischer Dinge die im Internet der Energie gesondert identifizierbar sind

[QUELLE: DIN SPEC 91214:2011-03]

2.23

Person

(en: person)

eine natürliche Person oder eine juristische Person

[QUELLE: DIN SPEC 91214:2011-03]

2.24

Regelleistung

(en: operating reserve)

kurzfristige Leistungsanpassungen durch regelfähige Kraftwerke zum Ausgleich von Differenzen zwischen Ein- und Auspeisung

2.25

Registrierung

(en: registration)

Vorgang des Eintragens in ein Verzeichnis

2.26

Rolle

(en: role)

abstraktes Konzept, das Eigenschaften von juristischen oder natürlichen Personen zusammenfasst

[QUELLE: DIN SPEC 91214:2011-03]

2.27

sensible Daten

(en: sensitive data)

schutzbedürftige, zumeist personenbezogene und geschäftskritische Daten

2.28

Single-Sign-On

SSO

(en: single-sign-on)

Anmeldungsverfahren, das einem Nutzer nach einmaliger Authentifizierung alle Dienste freischaltet, für die er autorisiert ist

2.29

Stammdaten

(en: reference data)

Datensatz über betrieblich relevante Daten

2.30

Standardlastprofil

SLP

(en: standard load profiles)

repräsentativer Lastgang eines Kunden ohne Lastgangmessung

Anmerkung 1 zum Begriff: Bei geringem Jahresgesamtverbrauch

2.31

Trusted Third Party

TTP

(en: trusted third party)

Entität, die zwischen zwei Parteien vermittelt und der beide Parteien vertrauen

2.32

Unternehmen

(en: company)

privatwirtschaftlicher Betrieb, der innerhalb der Smart Architecture Produkte oder Dienstleistungen zur Verfügung stellt oder in Anspruch nimmt

2.33

Verifikation

(en: verification)

Bestätigung durch Überprüfung und objektiven Nachweis, dass die festgelegten Anforderungen erfüllt wurden

[QUELLE: DIN EN 50126:2000-03]

2.34

Zertifikat

(en: certificate)

digitales Zertifikat zur Bestätigung einer Identität

3 Symbole und Abkürzungen

ANU	Anschlussnutzer
BiKo	Bilanzkreiskoordinator
BK	Bilanzkreis
BKV	Bilanzkreisverantwortlicher
BNetzA	Bundesnetzagentur
C	Consumer
CA	Certificate Authority
CRL	Certificate Revocation List
DER	Distributed Energy Resource
DIN	Deutsches Institut für Normung e. V.
DNS	Domain Name System
DSL	Digital Subscriber Line
ENS	Energy Name Service