TeleTrusT EBCA
European Bridge Certificate Authority

TeleTrusT EBCA "PKI-Workshop"

Berlin, 22.06.2017

E-Mail-Verschlüsselung – aktuelle Entwicklungen am Beispiel der Energiebranche

Dr. Burkhard Wiegel
CEO, Zertificon Solutions GmbH

Digitale Agenda 2014-17 – Auswirkungen auf die Marktkommunikation der Energiewirtschaft

Bundesministerium für Wirtschaft und Energie

Gesetz zur Digitalisierung der Energiewende

Bundesnetzagentur

Festlegungsverfahren zur Anpassung der Vorgaben zur elektronischen Marktkommunikation an die Erfordernisse des Gesetzes zur Digitalisierung der Energiewende

Az.: BK6-16-200 / BK7-16-142

bdew
Energie. Wasser. Leben.

edi@energy.
Datenformate Strom & Gas

Neue Vorgaben: Verpflichtende Verschlüsselung der Marktkommunikation.

Referenziert wird: **BSI-TR 03116**, Inhaltsverschlüsselung nach S/MIME 3.2

edi@energy. Datenformate Strom & Gas

Gemäß BNetzA-Beschluss2 sind grundsätzlich die kryptographischen Vorgaben der BSI TR 03116-4 (Stand: 23. Februar 2016) anzuwenden und einzuhalten. Die zu nutzenden Parameter und hiervon anzuwendenden Abweichungen sind in diesem Dokument beschrieben.

Es gelten **sehr detaillierte Vorgaben** für

Regelungen im Detail – S/MIME 3.2 & CAs

5.5 Verschlüsselung und Signatur von E-Mails

Jede E-Mail, mit der in der deutschen Energiewirtschaft eine EDIFACT-Übertragungsdatei ausgetauscht wird, ist zu verschlüsseln und zu signieren, spätestens ab dem 01.06.2017. Dabei sind die in diesem Kapitel genannten Regelungen einzuhalten:

- Im Sinne der 1:1-Kommunikation ist der Datenaustausch geschäftsprozessunspezifisch zu betreiben, d. h. die Verschlüsselung und Signatur der E-Mail erfolgt für alle Nachrichtentypen[8] einheitlich. Es müssen somit alle Übertragungsdateien von einem Absender an einen Empfänger verschlüsselt und signiert werden.
- Das Verschlüsseln und Signieren von E-Mails ist ausschließlich nach dem S/MIME-Standard gestattet. Es muss mindestens die Version 3.2 (IETF RFC 5751, Veröffentlichungsjahr 2010) verwendet werden.[9]

...

Quelle: http://www.edi-energy.de/files2/EDI@Energy-Regelungen-zum-%C3%9Cbertragungsweg_v1.1_Lesefassung.pdf

Regelungen im Detail – Zertifikate & Algorithmen

5.5.2 Zertifikate: Parameter und Anforderungen

Die Zertifikate müssen die nachfolgenden Anforderungen erfüllen[13]:

- Das Zertifikat muss von einer CA ausgestellt sein, die den unter Kapitel 5.5.1 genannten Anforderungen genügt.
- Alle bis zum 31.12.2017 ausgestellten Zertifikate sind mit den Signaturalgorithmen sha-256RSA oder sha-512RSA (Signaturverfahren RSASSA-PKCS1-v1_5) zu signieren. Sie sind bis zur maximalen Zertifikatsgültigkeit (maximal 3 Jahre) im Interimsmodell der Marktkommunikation verwendbar.
- Alle ab dem 01.01.2018 neu ausgestellten Zertifikate müssen mit RSASSA-PSS signiert sein.[14]
- Jedes Zertifikat muss Informationen für eine Rückrufprüfung enthalten, d. h. einen `CRLDistributionPoint`, unter dem jederzeit aktuelle CRL zur Verfügung stehen.
- Die Gültigkeit des Zertifikats darf maximal 3 Jahre betragen.
- Das Zertifikat muss mindestens die Verwendungszwecke Schlüsselverschlüsselung und digitale Signatur im Feld `KeyUsage` enthalten.
- Für die verschiedenen, für die Marktkommunikation nötigen Anwendungszwecke „Signatur“ und „Verschlüsselung“ ist dasselbe Schlüsselpaar zu generieren und dementsprechend ein sogenanntes Kombizertifikat auszustellen und zu verwenden.
- Das Zertifikat muss eine fortgeschrittene elektronische Signatur ermöglichen.[15]

…

Quelle: http://www.edi-energy.de/files2/EDI@Energy-Regelungen-zum-%C3%9Cbertragungsweg_v1.1_Lesefassung.pdf

5.5.3 Algorithmen und Schlüssellängen für S/MIME

Es sind folgende Algorithmen und Schlüssel mit den genannten Schlüssellängen zu verwenden[16]:

- Signatur:
  - Hashfunktion (Hash algorithm): SHA-256 oder SHA-512 (gemäß IETF RFC 5754).
  - Signaturverfahren (Signature algorithm): Grundsätzlich soll, sofern bei Sender und Empfänger verfügbar, eingesetzt werden: RSASSA-PSS (gemäß IETF RFC 4056). Vom 01.06.2017 bis 31.12.2017 muss zur Wahrung der Interoperabilität unterstützt werden: sha256RSA / sha512RSA (RSASSA-PKCS1-v1_5) Ab 01.01.2018 muss ausschließlich eingesetzt werden: RSASSA-PSS (gemäß IETF RFC 4056)

    RSA Schlüssellänge mindestens 2048 Bit

Quelle: http://www.edi-energy.de/files2/EDI@Energy-Regelungen-zum-%C3%9Cbertragungsweg_v1.1_Lesefassung.pdf

5.5.3 Algorithmen und Schlüssellängen für S/MIME

- Verschlüsselung:
  - Inhaltsverschlüsselung (Content encryption): AES-128 CBC oder AES-192 CBC (gemäß IETF RFC 3565).
  - Schlüsselverschlüsselung (Key encryption): Grundsätzlich soll, sofern bei Sender und Empfänger verfügbar, eingesetzt werden:
    RSAES-OAEP
    (gemäß IETF RFC 3447).
    Vom 01.06.2017 bis 31.12.2017 muss zur Wahrung der Interoperabilität unterstützt werden:
    RSAES-PKCS1-v1_5
    Ab 01.01.2018 muss ausschließlich eingesetzt werden:
    RSAES-OAEP
    (gemäß IETF RFC 3447)

    RSA Schlüssellänge mindestens 2048 Bit.

Quelle: http://www.edi-energy.de/files2/EDI@Energy-Regelungen-zum-%C3%9Cbertragungsweg_v1.1_Lesefassung.pdf

5.5.1 Zertifizierungsstellen

Das Zertifikat muss von einer Zertifizierungsstelle (engl. Certification Authority = CA) ausgestellt sein, die Zertifikate diskriminierungsfrei für Marktpartner der deutschen Energiewirtschaft anbietet. Es darf kein sogenanntes selbstausgestelltes Zertifikat sein.[11]

Die CA, von der das Zertifikat ausgestellt ist, muss den nachfolgenden Anforderungen genügen:[12]

- Die CA verfügt über einen Rückrufservice, über den Zertifikate widerrufen werden können. Dazu führt sie eine sogenannte Zertifikatsperrliste (englisch certificate revocation list, CRL), welche öffentlich zugängig ist.

Darüber hinaus sollten insbesondere die folgenden Kriterien berücksichtigt werden:

- Die IT-Sicherheit des CA-Betriebs ist durch ein Audit / eine Zertifizierung nach einem anerkannten Audit / Zertifizierungs-Standard geprüft. Es wird eine Zertifizierung nach BSI TR-03145, Secure Certification Authority operation empfohlen.
- Der Registrierungsservice, einschließlich an Dienstleister (Registrare) ausgelagerter Service, erfolgt auf einem hohen Sicherheitsniveau.
- Die Vertrauenswürdigkeit des Betreibers und des Betriebs, auch unter Berücksichtigung von Eingriffsrechten Dritter, ist gegeben.
- Der Rechtsstand, insbesondere in Bezug auf das geltende Haftungs- und Datenschutzrecht genügt den Anforderungen des Unternehmens, dass das Zertifikat beantragt.

Quelle: http://www.edi-energy.de/files2/EDI@Energy-Regelungen-zum-%C3%9Cbertragungsweg_v1.1_Lesefassung.pdf

Lösungsentwurf: E-Mail Gateway zur Marktkommunikation mit Z1 Funktionsmodul „EDI@Energy Mako 2017“

- **Unterstützt die von der BNetzA geforderten Algorithmen** gemäß S/MIME v3.2 und TR-03116-4 ohne zusätzlichen administrativen Aufwand.
- Bildet das **streng reglementierte Management der Zertifikate** für Verschlüsselung und Signatur ab.
- **Übernimmt den Zertifikatsaustausch** der Marktteilnehmer.
- Erfüllt die **organisatorischen Regelungen zum Übertragungsweg durch**
  - **Regelerweiterungen**
  - **Clearing-Postfächer**
- Sämtliche E-Mails inkl. der EDI-Marktkommunikation werden lückenlos dokumentiert und sind über **Reports** abrufbar.

Vielen Dank für Ihre Aufmerksamkeit!