Technischer FAQ AS4

Inhalt

Welche Zertifikatsanbieter gibt es?

Eine aktuelle Übersicht aller Zertifikatsanbieter in der Smart-Meter PKI finden Sie unter: https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/Smart-metering/Smart-Meterin-PKI/Registrierte_Sub-CAs/registrierte_sub_cas.html

Hinweis: Nichte alle hier gelisteten Zertifikatsanbieter /Betreiber einer Sub-CA) stellen die für AS4 benötigten EMT.MAK Zertifikate aus.

Wie komme ich von dem 256-Bit Schlüssel aus der Schlüsselableitung auf einen 128 Bit Schlüssel für Schlüsselverschlüsselung (kw-aes128)?

Das Kürzen des Schlüssels für die Schlüsselverschlüsselung ist Bestandteil der Key Derivation Function(KDF), siehe auch:

TR-03116-3: Fußnote 17, Seite 28:

> Die ConcatKDF wird in NIST SP800-56A [38] spezifiziert. Die Vorgaben für Kürzung auf die jeweilige Schlüssellänge sind hierbei in NIST SP800-56C [39] dargelegt.

Im Dokument NIST SP800-56C Kapitel 4.1:

> … Set DerivedKeyingMaterial equal to the leftmost L bits of Result(reps).

Beinhaltet der Aufruf des Testservice eine Übertragungsdatei?

Der Aufruf des Testservice beinhaltet immer eine Übertragungsdatei, siehe EDI@Energy-Dokument Regelungen zum Übertragungsweg für AS4, Version 2.0 bzw. 2.1 Kapitel 7.1.

Hinweis: Auch in diesem Datenaustausch ist die Übertragungsdatei ist zu signieren und zu verschlüsseln.

Beinhaltet der Aufruf des Service Wechsel des Übertragungsweg eine Übertragungsdatei?

Der Aufruf des Service darf, muss aber keine Übertragungsdatei beinhalten. Wenn eine Übertragungsdatei übermittelt wird, muss diese signiert und verschlüsselt sein. Eine gegeben falls vorhandene Übertragungsdatei muss, ignoriert werden.

Wird keine Übertragungsdatei übermittelt, darf der Aufruf innerhalb eines Mime-Parts oder auch ohne, also nur mittels Soap-Envelope erfolgen.

Welche Elemente sind zu signieren?

Es gilt:

- Das „Messaging Element“ muss immer signiert werden
- Wenn vorhanden, muss die Übertragungsdatei im zweiten Mime-Part signiert werden.
- Das Body-Element im Soap-Envelope sollte signiert werden.

Das bedeutet für die Services

1. Service = https://www.bdew.de/as4/communication/services/MP:

   Es wird das „Messaging Container Element“ und der Body des zweiten Mime Parts signiert.
   Der Body-Part im Soap-Envelope ist leer (`<S11:Body/>`) und darf signiert werden.

2. Service = http://docs.oasis-open.org/ebxml-msg/ebms/v3.0/ns/core/200704/service

   Es wird das „Messaging Container Element“ und der Body des zweiten Mime Parts signiert.
   Der Body-Part im Soap-Envelope ist leer (`<S11:Body/>`) und darf signiert werden.

3. Service = https://www.bdew.de/as4/communication/services/pathSwitch

   a. Der Service Aufruf erfolgt mittels einer „einfachen Soap-Nachricht“:
      Es wird das „Messaging Container Element“ signiert.
      Der Body-Part im Soap-Envelope ist leer (`<S11:Body/>`) und darf signiert werden.

   b. Der Service Aufruf erfolgt eines Mime-Part:

      Es wird das „Messaging Container Element“ signiert.
      Der Body-Part im Soap-Envelope ist leer (`<S11:Body/>`) und darf signiert werden.

Wie erfolgt die Angabe des Elements "#509PKIPathv1"?

Die Anforderungen zur Nutzung dieses Elements kommt aus dem Dokument „OASIS Web Services Security (WSS)“ (Link: https://www.oasis-open.org/committees/tc_home.php?wg_abbrev=wss).

Hier findet sich der Verweis auf „Web Services Security 3 X.509 Certificate Token Profile“. (Link: „http://docs.oasis-open.org/wss-m/wss/v1.1.1/os/wss-x509TokenProfile-v1.1.1-os.html).

Für die Syntax und Codierung dieses Elements wird verwiesen auf:
ITU-T X-SERIES RECOMMENDATIONS: Information Technology – Open Systems Interconnection – The Directory: Public-key and attribute certificate frameworks
(Link: „https://www.itu.int/rec/T-REC-X.509-201910-I“)

Auf den Seiten 20ff findet sich die gesuchte Spezifikation.

Veröffentlichung von Sperrlisten

Quelle:Technische Richtlinie BSI TR-03109-4 Smart Metering PKI - Public Key Infrastruktur für Smart Meter Gateways Version 1.2.1 Datum: 09.08.2017

> Die Root-CA und die Sub-CAs müssen deren Sperrlisten wahlweise über HTTP [1] **oder** LDAP [4] zum freien Herunterladen bereitstellen (siehe Abbildung 8). Hierbei müssen die in [13] definierten Zeiten eingehalten werden. Damit die Authentizität der jeweiligen Sperrliste überprüft werden kann, müssen die hierfür erforderlichen Zertifikate zusätzlich zur Sperrliste frei abrufbar sein.

Dürfen Übertragungsdateien vor der Übermittlung komprimiert werden?

Bei der Nutzung von AS4 als Übertragungsweg wird ausschließlich die im Übertragungsprotokoll zu verwendende Komprimierung genutzt. Die Übertragungsdateien dürfen nicht vorab komprimiert werden.

Ist die Angabe eines Ports in der Angabe der Adresse des AS4 Webservice zulässig?

Die Angabe des Ports in der Angabe der Adresse des AS4 Webservice ist immer zulässig. Er muss enthalten sein, sofern ein vom Standard 443 abweichender Port verwendet wird. Insbesondere darf ein Port > 1000 gewählt werden.