Konsolidierte Lesefassung mit Fehlerkorrekturen

Stand: 27.09.2024

Regelungen zum Übertragungsweg für API-Webdienste

Version:	1.0
Ursprüngliches Publikationsdatum:	03.07.2024
Anzuwenden ab:	04.04.2025
Autor:	BDEW

Inhaltsverzeichnis

1 Einleitung 3

2 Terminologie 3

2.1 Schlüsselwörter in der API-Guideline 3

3 Technische Vorgaben der API-Webdienste 3

3.1 Netzwerk 3
3.2 Transportebene 3
3.3 Inhaltsdatensicherungsebene 4
3.4 Zertifikate und Smart Metering PKI 4

4 Quellen 5

5 Änderungshistorie 6

1 Einleitung

Dieses Dokument regelt die Sicherheits- und Schutzmechanismen, die im Rahmen des elektronischen Datenaustauschs für regulierte Prozesse zwischen den Marktpartnern der deutschen Energiewirtschaft für den Übertragungsweg[1] API-Webdienste in der Marktkommunikation einzuhalten sind.

Gemäß BNetzA-Beschlüsse[2] sind grundsätzlich die kryptographischen Vorgaben der BSI TR 03116-3 anzuwenden und einzuhalten, sowie die Nutzung der Smart Metering-PKI des BSI, nach § 52 Abs. 4 MsbG vorzusehen.

2 Terminologie

2.1 Schlüsselwörter in der API-Guideline

Die Schlüsselwörter „MÜSSEN“ (Englisch „MUST“), „DÜRFEN NICHT“ (Englisch „MUST NOT“), „ERFORDERLICH“ (Englisch „REQUIRED“), „SOLL“ (Englisch „SHALL“), „SOLL NICHT“ (Englisch „SHALL NOT“), „SOLLTE“ (Englisch „SHOULD“), „SOLLTE NICHT“ (Englisch „SHOULD NOT“), „EMPFOHLEN“ (Englisch „RECOMMENDED“), „DÜRFEN“ (Englisch „MAY“), and „FREIWILLIG“ (Englisch „OPTIONAL“) in diesem Dokument sind zu interpretieren gemäß [RFC2119]. Dabei spielt die Groß- und Kleinschreibung keine Rolle.

3 Technische Vorgaben der API-Webdienste

3.1 Netzwerk

MUST Alle Kommunikationsendpunkte werden durch DNS-Namen und nicht durch IP-Adressen bestimmt. Die beschriebenen Webservices müssen IPv4 implementieren und SOLLTEN IPv6 implementieren (Dual Stack).

Der API-Nutzer des API-Webservice MUSS in der Lage sein, die TLS-Verbindung über IPv4 herzustellen.

3.2 Transportebene

MUST Zum Aufbau der http-Verbindung MUSS das Protokoll Transport Layer Security (TLS) nach den Regeln in [TR03116-3] (Kapitel TLS-Kommunikation im WAN und in der Marktkommunikation) eingesetzt werden.

MUST Für den Aufbau der TLS-Verbindung ist die Erweiterung Server Name Identification (SNI) gemäß [RFC6066] bzw. [RFC8449] zu unterstützen und zu verwenden.

---

[1] Mit „Übertragungsweg“ wird in diesem Dokument das bezeichnet, was auch als „Kommunikationskanal“, „Kommunikationsweg“ „Transportprotokoll“ oder „Übertragungsprotokoll“ bezeichnet wird.

[2] Vgl. [BK6-21-282] und Fortentwicklung mit [BK6-22-128] und [BK6-22-024].

3.3 Inhaltsdatensicherungsebene

MUST Jede API-Interaktion und der übertragene Payload wird signiert. Dies gilt sowohl für http-Requests als auch synchrone Responses, in denen ein Payload enthalten ist.

MUST Die dabei anzuwendenden Algorithmen (Hash- und Signatur-Algorithmus) sowie die Hinweise zur Umsetzung, sind in [TR03116-3] in den Kapiteln 8 und 9 identisch beschrieben und soweit hier anzuwenden.

Signiert wird die angesprochene Ressource (URI) inklusive aller Query-Parameter, die http-Kopfzeilen creationDateTime, transactionId und soweit vorhanden initialTransactionId, und die übermittelte Payload (JSON-Objekt)[3].

Vor der Berechnung des Hashwerts eines JSON-Objekts muss dieses kanonisiert werden gemäß [RFC8785].

Der zu signierende Digest wird dann berechnet (Der Hash für die http-Kopfzeile „initialTransactionId“ wird nur berechnet und in die Gesamtberechnung aufgenommen, wenn sie vorhanden ist!):

› Hash(Hash(URI) + Hash(Payload) + Hash(CreationDateTime) + Hash(transactionId) + Hash(initialTransactionId))

Digest und Signatur werden in den http-Header Feldern X-BDEW-DIGEST und X-BDEW-SIGNATURE Base64-kodiert abgelegt.

Das Zertifikat mit dem zum Signieren verwendeten öffentlichen Schlüssel wird in dem HTTP-Header-X-BDEW-CERT hinterlegt. Die Kodierung des Zertifikats in einem HTTP-Header Feld ist in Kapitel 2.1 in [RFC9440] für TLS Zertifikate beschrieben und ist hier in gleicher Weise zu verwenden.

Die mittels des API-Aufrufs übertragenen Parameter und Payload werden nicht verschlüsselt.

3.4 Zertifikate und Smart Metering PKI

Die Kommunikation wird durch Verwendung der Smart Metering PKI (SM-PKI) des BSI abgesichert. Die Vorgaben der Certificate Policy (CP) der SM-PKI müssen eingehalten werden. Die Vertrauensdiensteanbieter müssen eine Sub-CA-Instanz im Sinne der CP der SM-PKI sein. Die Kommunikationspartner, API-Nutzer und Anbieter, sind nach dem Rollenkonzept der SM-PKI in der Rolle passiver EMT, sofern der Kommunikationspartner nicht durch Regelungen außerhalb dieses Regelwerks zur API die Rolle eines aktiven EMT wahrnehmen muss.

[3] Alle für die fachliche Verarbeitung eines Requests erforderlichen Parameter müssen in der Signatur enthalten sein. Insbesondere bedeutet dies, dass alle weiteren http-Header rein informatorischen Charakter haben und keinen Einfluss auf die fachliche Verarbeitung eines Requests haben dürfen.

4 Quellen

[BK6-21-282] Beschluss (BK6-21-282) und Anlagen zur Absicherung der elektronischen Marktkommunikation Strom, Bundesnetzagentur, 31.03.2022.

[BK6-22-128] Beschluss (BK6-22-128) und Anlagen zur prozessualen Abwicklung von Steuerungshandlungen in Verbindung mit intelligenten Messsystemen (iMS) (Universalbestellprozess), 21.11.2022.

[BK6-22-024] Beschluss (BK6-22-024) und Anlagen zu Regelungen für einen beschleunigten werktäglichen Lieferantenwechsel in 24 Stunden (LFW24), 21.03.2024.

[CP-SM-PKI] Certificate Policy der Smart Metering PKI. Version 1.1.2, 25.01.2023. https://www.bsi.bund.de/dok/7615484

[RFC2119] Key words for use in RFCs to Indicate Requirement Levels. IETF RFC 2119. March 1997. https://www.rfc-editor.org/rfc/rfc2119

[RFC6066] Transport Layer Security (TLS) Extensions: Extension Definitions, ITEF RFC 6066. Januar 2011. https://www.rfc-editor.org/rfc/rfc6066

[RFC8449] Record Size Limit Extension for TLS IETF RFC 8449. August 2018. https://www.rfc-editor.org/rfc/rfc8449

[RFC8785] JSON Canonicalization Scheme (JCS). IETF RFC 8785. June 2020. https://www.rfc-editor.org/rfc/rfc8785

[TR03116-3] Technische Richtlinie BSI TR-03116 Kryptographische Vorgaben für Projekte der Bundesregierung. Teil 3: Intelligente Messsysteme. 06.12.2022. https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/TechnischeRichtlinien/TR03116/BSI-TR-03116-3.html

5 Änderungshistorie

Änd-ID	Ort	Änderungen		Grund der Anpassung	Status
		Bisher	Neu		
14000	Deckblatt	Version: 1.0 Publikationsdatum: 03.07.2024 Anzuwenden ab: 01.10.2024	**Konsolidierte Lesefassung mit Fehlerkorrekturen** **Stand: 27.09.2024** Version: 1.0 **Ursprüngliches** Publikationsdatum: 03.07.2024 Anzuwenden ab: 01.10.2024	Version aktualisiert. Zusätzlich wurden im gesamten Dokument Schreibfehler, Layout, Internetadressen etc. korrigiert, die keinen Einfluss auf die inhaltliche Aussage haben.	Fehler (27.09.2024).
14001	Kapitel 3.3 Inhaltsdaten-sicherungsebene	› Hash(URI) + Hash(Payload) + Hash(CreationDateTime) + Hash(transactionId) + Hash(initialTransactionId)	› **Hash(**Hash(URI) + Hash(Payload) + Hash(CreationDateTime) + Hash(transactionId) + Hash(initialTransactionId)**)**	Fehlendes doppelte Hash ergänzt.	Fehler (27.09.2024).
14002	Kapitel 5 Ansprechpartner	5. Ansprechpartner Mathias Böswetter E-Mail: mathias.boeswetter@bdew.de Telefon: +49 30 300 199 1526	~~5. Ansprechpartner~~ ~~Mathias Böswetter~~ ~~E-Mail: mathias.boeswetter@bdew.de~~ ~~Telefon: +49 30 300 199 1526~~	Harmonisierung an andere EDI@Energy-Dokumente.	Fehler (27.09.2024).