DB NETZE

Elektronischer Datenaustausch per AS4

26.01.2023 | Frankfurt

DB Energie – bringt voran.

Einleitung

Mit Beschluss BK6-21-282 wurde von der Bundesnetzagentur (BNetzA) am 31.03.2022 eine Festlegung zur künftigen „Absicherung der elektronischen Marktkommunikation Strom“ in der Energiesparte Strom 50Hz veröffentlicht. Ziel der neuen Regelung ist die Umstellung des Übertragungswegs vom heutigen Standard verschlüsselter E-Mail-Kommunikation via S/MIME und AS2 auf den Übertragungsweg AS4 (Applicability Statement 4). Die Festlegung sieht für die 50Hz-Netze u.a. vor, ab Oktober 2023 die technischen Voraussetzungen zum Austausch der Vorgaben an den neuen Übertragungsweg zu erfüllen. Ab dem 01.04.2024 soll dann laut BNetzA-Festlegung ausschließlich mittels AS4 kommuniziert werden.

Die BNetzA nennt als Gründe die Weiterentwicklung und Erhöhung des bereits geltenden Sicherheitsstandards. Ein sicherer und zuverlässiger Austausch von Daten zwischen verschiedenen Akteuren der Energiewirtschaft sei eine unablässige Grundvoraussetzung für eine effiziente Abwicklung der elektronischen Marktkommunikation. Zudem seien Angriffe auf die digitale Infrastruktur der Energiewirtschaft nicht mehr nur im Bereich des Theoretischen, sodass Risiken für IT-Sicherheitsvorfälle und Cyberangriffe vermindert werden sollen.

Die Beschlüsse und die dazugehörigen Dokumente können unter den folgenden Links abgerufen werden:
Übersicht BK6-21-282_Beschluss_vom_31.03.2022, Beschluss BK6-21-282, Anlage Einführungsszenario, BDEW_Anwendungshilfe.pdf, Regelung_Uebertragungsweg.pdf

Der Bahnstromnetzbetreiber (BNB) unterstützt den Einsatz von gesicherten Übertragungswegen, um den Datenschutz und die Sicherheit der Kommunikationsprozesse zwischen den verschiedenen Marktteilnehmern im Bahnstromnetz gewährleisten zu können.

Aus diesem Grund soll für den gesamten Datenaustausch im Bahnstromnetz unabhängig von der Marktrolle spätestens ab 01.07.2025 00:00 Uhr ebenfalls der Kommunikationsweg AS4 verwendet werden.

Allgemeine Informationen zu AS4

AS4 ist bereits heute ein etablierter Übertragungsweg und wird bereits als Kommunikationsweg für die Ferngasnetzbetreiber (ENTSOG) verwendet.
Über AS4 ist ausschließlich der Versand von verschlüsselten Nachrichten möglich. Daraus resultiert, dass unverschlüsselte Nachrichten vom Empfänger nicht mehr empfangen und verarbeitet werden können. Die Nachrichten werden zudem als nicht zugestellt angesehen.
Des Weiteren bestätigt AS4 die Authentizität des Absenders und stellt sicher, dass die Nachricht während des Transports unverändert bleibt.

AS4 unterstützt prinzipiell nicht nur die PUSH-Methode, sondern Nachrichten könnten auch per PULL-Methode abrufbar sein. Dies ist derzeit jedoch weder in den bahnstromspezifischen XML-Prozessen noch in den EDIFACT-Prozessen vorgesehen, kann aber prinzipiell zukünftig nicht ausgeschlossen werden.

Die BNetzA stellt zudem weitere Anforderungen zum Sicherheitsniveau: Dies bedeutet, dass Zertifikate weiterhin nur bei Zertifikatsanbietern gemäß Smart Metering-PKI des BSI bestellt werden können und dass der private Schlüssel auf einem HSM (Hardware-Sicherheitsmodul) zum Schutz vor softwaretechnischen Cyberangriffen vorgehalten werden muss. Unter „PKI“ ist die Abkürzung für „Public Key Infrastruktur“ zu verstehen und bedeutet „Infrastruktur für öffentliche Schlüssel“.

Um den Datenaustausch durchführen zu können, wird eine MSH-Software (Messaging Service Handler) benötigt, welche dann letztendlich den AS4-Datenaustausch durchführt. Die Kommunikation mit der anderen Partei muss den vereinbarten AS4-Parametern entsprechen. Die MSH muss zudem auch mit der internen Geschäftsanwendung kommunizieren können.

Wie läuft die Kommunikation heute:

Voraussetzung: Absender und Empfänger haben die erforderlichen Zertifikate (öffentliche Schlüssel) ausgetauscht.

Der Absender erzeugt eine E-Mail mit einer XML- oder EDIFACT-Datei.
Die E-Mail wird
- mit seinem eigenen privaten Schlüssel signiert,
- mit dem öffentlichen Schlüssel des Empfängers verschlüsselt
- und an den Empfänger versendet.

Der Empfänger empfängt die E-Mail,
- entschlüsselt diese mit seinem privaten Schlüssel,
- prüft den Absender und die Unversehrtheit der E-Mail mit dem öffentlichen Schlüssel des Absenders
- und quittiert dem Sender den Empfang mit einer EDIFACT-Empfangsbestätigung oder einer XML-Nachrichtenquittung.

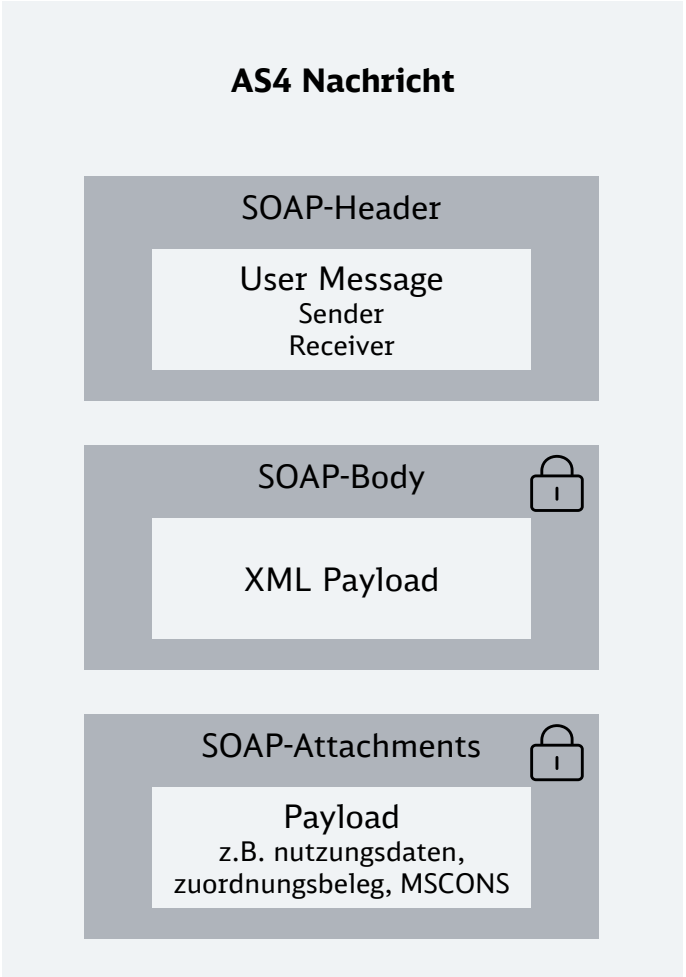
Aufbau einer verschlüsselten Nachricht

Der fachliche Aufbau der XML-/oder EDIFACT-Nachricht ändert sich mit der Umstellung auf den Kommunikationsweg AS4 nicht. Dies bedeutet, dass beispielsweise eine XML-Nachricht „nutzungsdaten“ fachlich mit den identischen Elementen aufgebaut sein muss, um beim BNB korrekt verarbeitet werden können. Viel mehr ändert sich die „Hülle“ der XML-Nachricht.

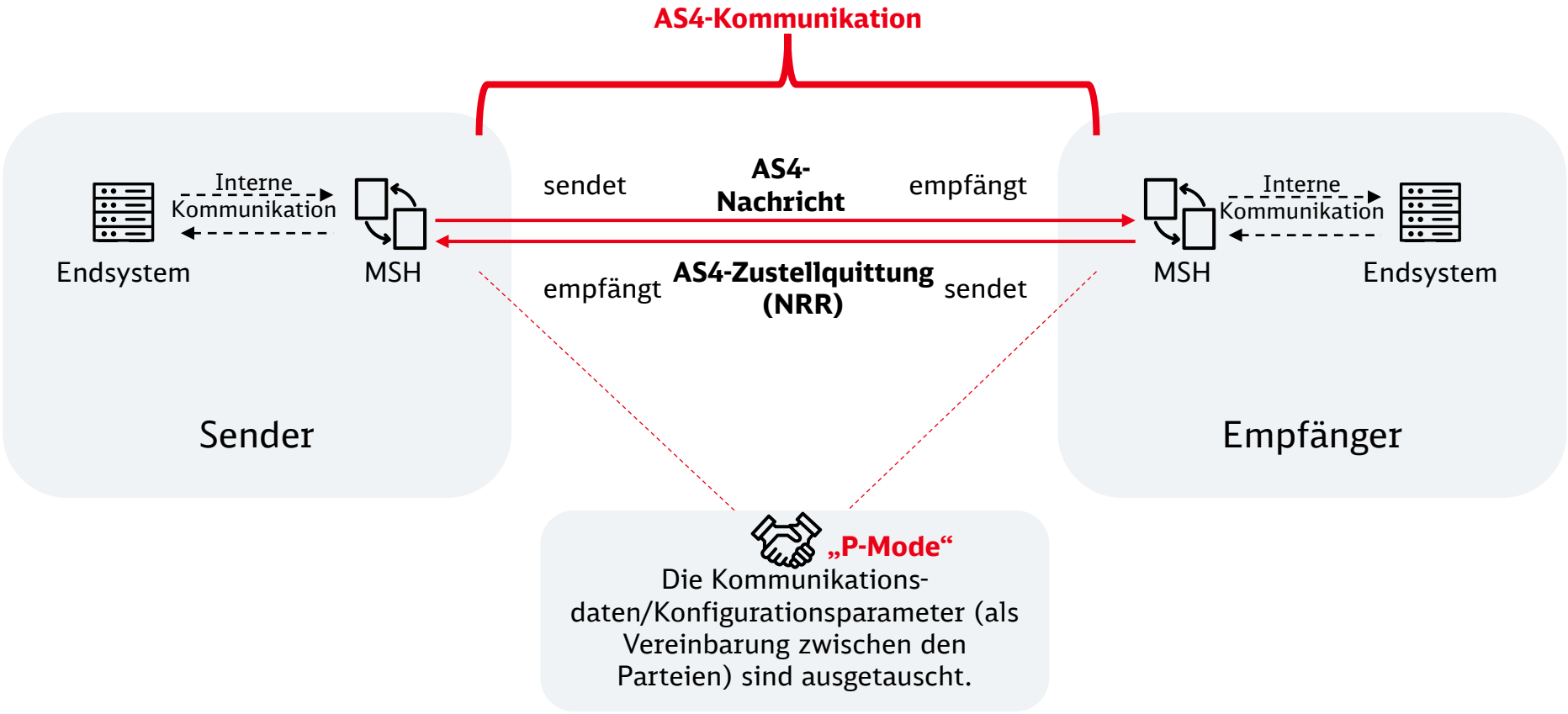
Beispiel anhand eines versendeten Zuordnungsbelegs:
Der Zuordnungsbeleg, bzw. die Nachricht vom Typ ediTfzZuordnung wird vom BNB erstellt. Der fachliche Inhalt sowie der technische Aufbau der Nachricht ist identisch zur bisherigen Übermittlung. Dieser sog. Payload wird nun mit einem Zertifikat analog zu heute inhaltlich verschlüsselt und signiert.

Der Payload wird daraufhin mit einer Hülle im XML-Format (sog. Overload) ummantelt. Dieser Overload wird mittels einer TLS (Transport Layer Security) asymmetrisch verschlüsselt.

Mittels AS4 wird eine Nachricht somit doppelt verschlüsselt. Kann eine Nachricht vom Empfänger nicht entschlüsselt werden, so teilt der Empfänger dies dem Sender über eine Error-Meldung mit.



Wie läuft die Datenübertragung ab?



Vorbedingung: Die Marktpartner sind einander bekannt, die Konfigurationsparameter (u.a. mit Informationen zu IP-Adressen, zu öffentlichen Schlüsseln für die Verschlüsselung, Informationen zu Nachrichtenkomprimierung, etc...) ausgetauscht sowie die AS4-Verbindung getestet. Das Senden sowie Empfangen wird durch eine P-Mode-Konfiguration geregelt, die eine Vereinbarung zwischen den Parteien über die Anwendung des AS4-Nachrichtenaustauschs darstellt.

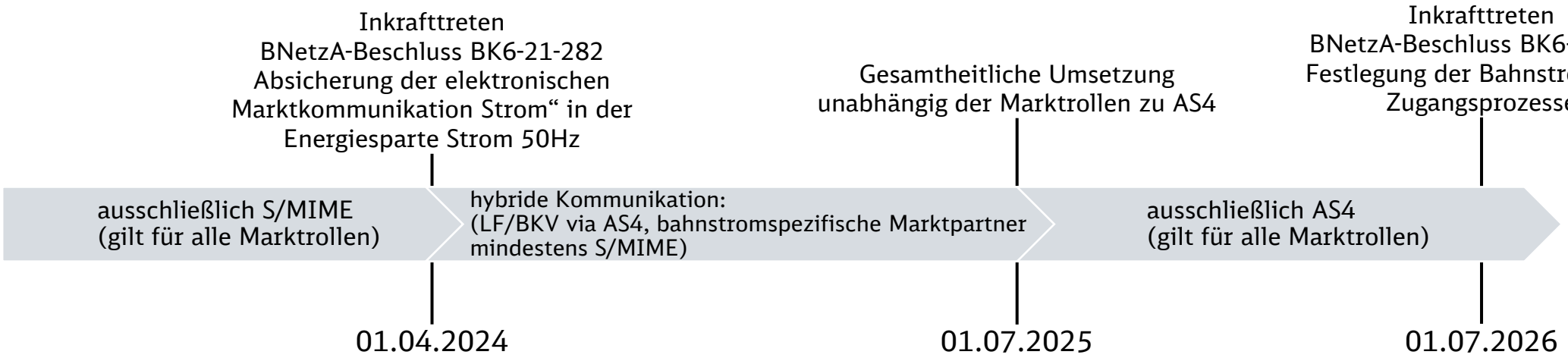
Ein Endsystem erzeugt eine Nachricht und übergibt diese an sein „MSH“. Der Sender baut über das Internet zunächst eine sichere Verbindung via WebService mit TLS-Protokoll auf und schickt die verschlüsselte Nachricht im Push-Verfahren zum „MSH“ des Empfängers. Im Nachgang erhält der Sender der Nachricht im Erfolgsfall eine Bestätigung über den Erhalt beim Kommunikationspartner (AS4-Zustellquittung (NRR)). Im Gegensatz zur E-Mail-Kommunikation (asynchrones Verfahren) kann somit sichergestellt werden, dass eine Nachricht tatsächlich beim Empfänger eingegangen ist.

Übergangszeitraum

Bis zum 01.04.2024 00:00 darf im Bahnstromnetz der DB Energie GmbH lediglich der Kommunikationsweg „Verschlüsselter E-Mail-Kommunikation via S/MIME“ gemäß den gültigen Regelungen zum Übertragungsweg des Bundesverband der Energie- und Wasserwirtschaft (BDEW) angewendet werden.
Die aktuell gültige Regelung kann hier abgerufen werden.

Für den Zeitraum zwischen 01.04.2024 bis 01.07.2025 wird es in einem Übergangszeitraum möglich sein, sowohl den Kommunikationsweg „Verschlüsselter E-Mail-Versand via S/MIME“ als auch „AS4“ zu verwenden. Marktpartner, die ebenfalls in 50Hz-Netzen agieren (wie Lieferanten und Bilanzkreisverantwortliche) und somit unter die anfangs genannte BNetzA-Festlegung fallen, müssen bereits ab 01.04.2024 mit dem BNB via AS4 kommunizieren. Die Kommunikation mit den bahnstromspezifischen Marktpartnern (Eisenbahnverkehrsunternehmen, Halter, Messstellenbetreiber, Kommunikationsdienstleister) wird weiterhin mindestens mittels verschlüsselter E-Mail-Kommunikation via S/MIME stattfinden. Sie haben jedoch im Übergangszeitraum die Möglichkeit, bereits vor dem 01.07.2025 auf die AS4-Kommunikation umzustellen.

Ab 01.07.2025 00:00 muss dann unabhängig von der Marktrolle der Kommunikationsweg AS4 verwendet werden.



Vorgehen bei Wechsel des Übertragungswegs

Um den Wechsel des Übertragungswegs durchführen zu können, haben sich als Vorbedingung beide Parteien über die Datenaustauschadressen (mindestens die URL des AS4-Webservice-Aufrufs (AS4-Adresse)) inklusive der zu verwendenden Zertifikate zu verständigen.

Des Weiteren kann mittels eines Testservice sichergestellt werden, dass der grundsätzliche Verbindungsaufbau möglich ist. Um den Wechsel initiieren zu können, übermittelt der Initiator eine AS4-Nachricht mit dem Service „Wechsel des Übertragungswegs“ an seinen Marktpartner. Mittels der „Zustimmung zum Wechsel des Übertragungswegs“ kann der Empfänger dem Initiator mitteilen, dass auch er den Übertragungsweg AS4 zum Austausch von Übertragungsdateien nutzen möchte.

Zur weiteren Absicherung eines sicheren Datenaustausches definiert das BDEW AS4-Profil neben den Services zum Übertragen von Übertragungsdateien und einem Testservice einen weiteren Service zum Wechsel des Übertragungswegs.

Weitere Informationen zu den Vorbedingungen sowie zum Wechsel des Übertragungswegs können aus den Regelungen zum Übertragungsweg für AS4 sowie dem BDEW AS4-Profil entnommen werden.


DB
NETZE