TRADING HUB EUROPE
keep in balance

Einführung BDEW-AS4-Protokoll nach BSI Vorgaben

Agenda

1. Regulatorischer Hintergrund

- Bundesnetzagentur und BDEW
- Grundlagen BDEW-AS4-Protokoll
- BDEW-Einführungsszenario für die Sparte Gas
- Zertifikate
  - Certificate Authority
  - Zertifikatstripel
  - Zertifikatsbeantragung
  - Technische Implementierung

2. Umsetzung des Projekts bei THE

- Regulierte Umstellung der Marktpartner
- Umstellungskonzept bei THE
- Ein wenig Technik
- FAQ zur Umstellung der Sparte Strom

TRADING HUB EUROPE

Regulatorischer Hintergrund

TRADING HUB EUROPE

Regulatorischer Hintergrund

Bundesnetzagentur und BDEW

Festlegung BK7-19-001 der Bundesnetzagentur GeLi Gas vom 22.11.2023:

- Vorgabe der Bundesnetzagentur zur endgültigen Umsetzung des Nachrichtenprotokolls Applicability Standard 4 (AS4) einschließlich der Verwendung einer Smart-Meter-Public-Key-Infrastruktur mit Wirktermin 01.04.2025

Umsetzung der Festlegung der BNetzA durch den BDEW:

1. Veröffentlichung der Regelungen zum Übertragungsweg Version 1.8 mit Gültigkeit ab 01.10.2024
   - Ausweitung des BDEW-AS4-Protokolls auf die Marktkommunikation für alle Geschäftsprozesse in der Sparte Gas
   - https://www.edi-energy.de/index.php?id=38&tx_BDEW_BDEW%5Buid%5D=2307&tx_BDEW_BDEW%5Baction%5D=download&tx_BDEW_BDEW%5Bcontroller%5D=Dokument&cHash=c6d817b4e8038cfea85ba643f2a26df7
2. Einführungsszenario zur Umstellung der elektronischen Marktkommunikation Gas auf AS4
   - zur Verhinderung eines harten Umstellzeitpunktes Veröffentlichung der EDI@Energy Anwendungshilfe 1.0
   - https://www.edi-energy.de/index.php?id=38&tx_BDEW_BDEW%5Buid%5D=2318&tx_BDEW_BDEW%5Baction%5D=download&tx_BDEW_BDEW%5Bcontroller%5D=Dokument&cHash=9cea53f02676c1c7d089a798080d4eea
3. Veröffentlichung der Regelungen zum Übertragungsweg Version 2.2 mit Gültigkeit ab 01.10.2024
   - Gültiges Regelwerk nach dem Wechsel auf das BDEW AS4-Profil.
   - https://www.edi-energy.de/index.php?id=38&tx_BDEW_BDEW%5Buid%5D=2305&tx_BDEW_BDEW%5Baction%5D=download&tx_BDEW_BDEW%5Bcontroller%5D=Dokument&cHash=d146bff7cf320096c23a94c55f59fcb4
4. BDEW AS4-Profil Version 1.0 Konsolidierte Lesefassung
   - Beschreibung der technischen Vorgaben an das Protokoll
     - https://www.edi-energy.de/index.php?id=38&tx_BDEW_BDEW%5Buid%5D=2091&tx_BDEW_BDEW%5Baction%5D=download&tx_BDEW_BDEW%5Bcontroller%5D=Dokument&cHash=c3338aa8cb55e5946a1b0d1dbfdc2e0a

TRADING HUB EUROPE

Regulatorischer Hintergrund

Grundlagen BDEW-AS4-Protokoll

- Messstellenbetriebsgesetz (MsbG) §52 Abs.4
  - Anforderung der Verwendung der Smart-Meter-PKI für den Austausch in der Datenkommunikation
- Technischen Richtlinien TR 03116-3 (Stand 2023) des Bundesamtes für Sicherheit in der Informationstechnologie (BSI)
  - Sicherheitsanforderungen für den Einsatz kryptographischer Verfahren in der Infrastruktur von Messsystemen im Energiesektor
  - Definition von kryptographischen Algorithmen und Schlüssellängen für Zertifikate, die in der SM-PKI eingesetzt werden müssen
- **Keine Kommunikation mehr per AS2 oder Mail ab dem Wirktermin möglich**

  Entsprechend der Festlegung der BNetzA ist mit der Einführung des BDEW-AS4 Protokolls die Marktkommunikation mittels Mail oder AS2 verboten.
- **Keine Firewallfreischaltung mehr**

  Mit Einführung des BDEW-AS4 ist aufgrund der Technologie keine Firewallfreischaltung zum Kommunikationsbeginn mehr erforderlich.
- **Verwendung von Hardware Security Modulen (HSM) und speziellen Verschlüsselungskurven (ECC)**

  Für das BDEW-AS4 Protokoll werden spezielle vom BSI freigegebene HSM‘s benötigt. Auf dem HSM werden die Schlüssel für das Zertifikat erstellt, die dann an die Certificate Authority (CA) übergeben werden, die daraus die Zertifikate erstellt. Auf dem HSM wird bei jedem Verbindungsaufbau die Verschlüsselung über die elliptisch kryptographischen Kurven (engl. Elliptic Crypto Curve kurz ECC) ausgehandelt und die Daten anschließend verschlüsselt übermittelt.
- **Neue Verbindungen werden über eine Zertifikatsabfrage bei den Certificate Authorities (CA‘s) eingerichtet**

  Wenn eine AS4 Verbindung zu einem neuen Marktpartner aufgebaut wird, wird bei allen CA‘s abgefragt, ob für den Marktpartner ein Zertifikat hinterlegt ist. Besitzt eine CA dieses Zertifikat, übermittelt sie dieses an den anfragenden Marktpartner.

TRADING HUB EUROPE

Regulatorischer Hintergrund

BDEW-Einführungsszenario zur Umstellung der elektronischen Marktkommunikation Gas auf AS4:

TRADING HUB EUROPE

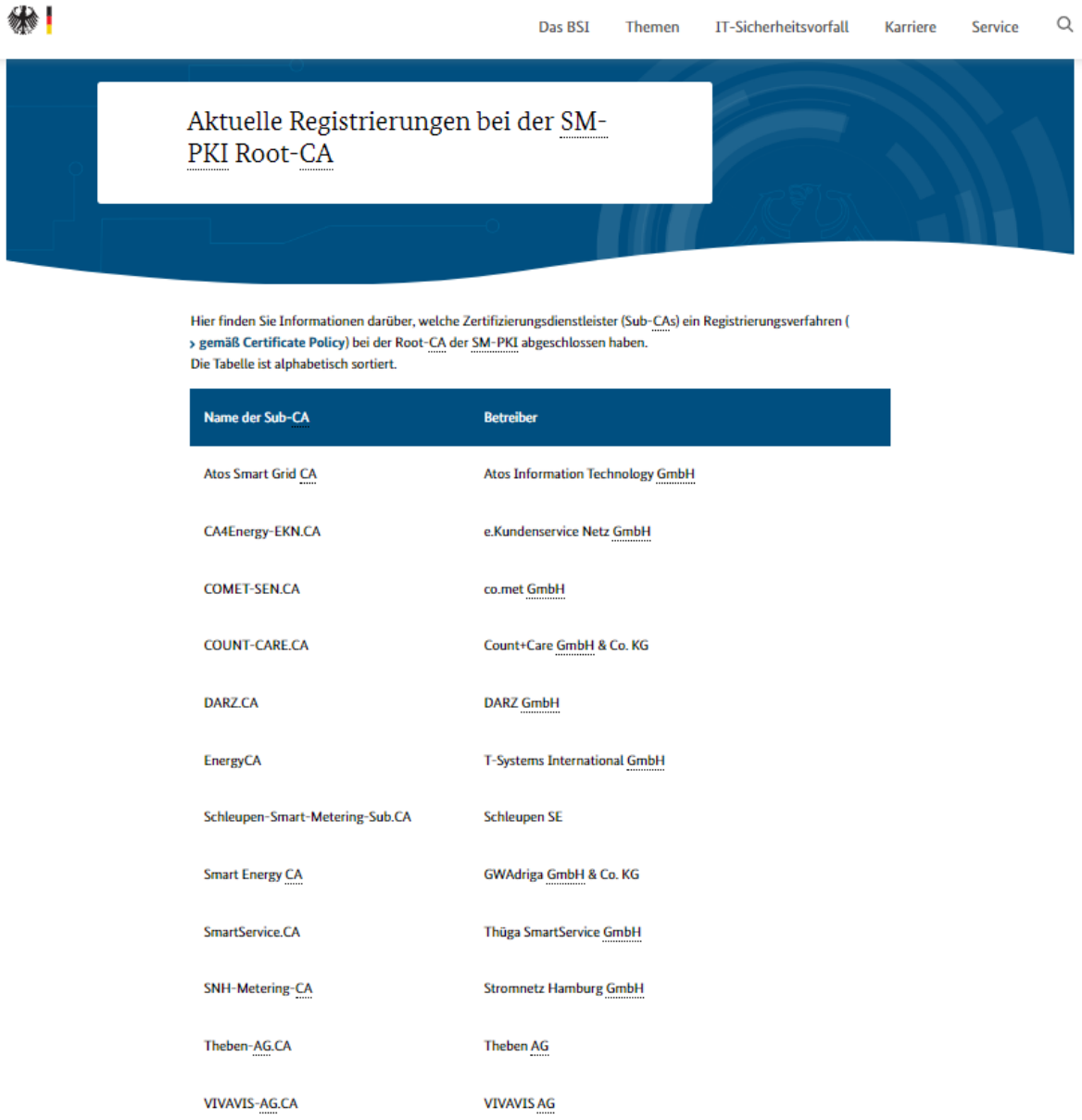
Regulatorischer Hintergrund

Anforderungen an die Certificate Authority (CA)

Nicht jede CA darf ein Zertifikat für die BDEW-AS4-Kommunikation ausstellen.

- Die CA muss vom BSI akkreditiert sein.

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



Das BSI Themen IT-Sicherheitsvorfall Karriere Service

Aktuelle Registrierungen bei der SM-PKI Root-CA

Hier finden Sie Informationen darüber, welche Zertifizierungsdienstleister (Sub-CAs) ein Registrierungsverfahren (› gemäß Certificate Policy) bei der Root-CA der SM-PKI abgeschlossen haben.
Die Tabelle ist alphabetisch sortiert.

Name der Sub-CA	Betreiber
Atos Smart Grid CA	Atos Information Technology GmbH
CA4Energy-EKN.CA	e.Kundenservice Netz GmbH
COMET-SEN.CA	co.met GmbH
COUNT-CARE.CA	Count+Care GmbH & Co. KG
DARZ.CA	DARZ GmbH
EnergyCA	T-Systems International GmbH
Schleupen-Smart-Metering-Sub.CA	Schleupen SE
Smart Energy CA	GWAdriga GmbH & Co. KG
SmartService.CA	Thüga SmartService GmbH
SNH-Metering-CA	Stromnetz Hamburg GmbH
Theben-AG.CA	Theben AG
VIVAVIS-AG.CA	VIVAVIS AG

TRADING HUB EUROPE

Regulatorischer Hintergrund

Zertifikatstripel

Für das BDEW-AS4 Protokoll wird ein Zertifikatstripel pro Marktpartner-ID (MP-ID) benötigt,

bisher reichte ein Kombi-Zertifikat pro Unternehmen,

Nun werden pro Marktrolle drei Zertifikate benötigt.

- Das Zertifikatstripel besteht aus einem
  - TLS-Zertifikat (Aufbau der gesicherten Kommunikation mittels ECC)
  - Signaturzertifikat (Authentifizierung von Sender und Empfänger)
  - Verschlüsselungszertifikat (Ver- und Entschlüsselung der EDIFACT-Nachricht)
- In den Zertifikaten sind die Marktpartner-ID (MP-ID) und der Kommunikationsendpunkt (AS4-Server inklusive Pfad auf dem Server) verpflichtend anzugeben.
- Für jede MP-ID wird ein eigener AS4-Endpunkt benötigt

Regulatorischer Hintergrund

Erforderliche Dokumente für die Zertifikatsbeantragung

- Schriftliche Bestätigung des DVGW, dass die MP-ID zum Unternehmen gehört (DVGW-Zuteilungsurkunde) gem. Certificate Policy der Smart-Meter-Public-Key-Infrastruktur (BSI)
- Aktueller Handelsregisterauszug des Unternehmens
- Separate Zertifikatsanträge je MP-ID und Kommunikationsrolle für Test- und Wirkzertifikate
  - Erklärung der Kommunikationsrolle im Antrag (Gateway-Administrator (GWA), Externer Marktteilnehmer (EMT), etc.)

Technische Implementierung

- Generierung des Schlüssels der Testzertifikate im HSM des Marktpartners nach Prüfung aller Dokumente und Freigabe durch die CA
- Übergabe der auf dem HSM erzeugten Schlüssel an die CA zur Erzeugung und Speicherung des Zertifikats durch die CA
- Bei der CA nachgewiesener erfolgreicher Test mit einem Testzertifikat

Umsetzung des Projekts bei THE

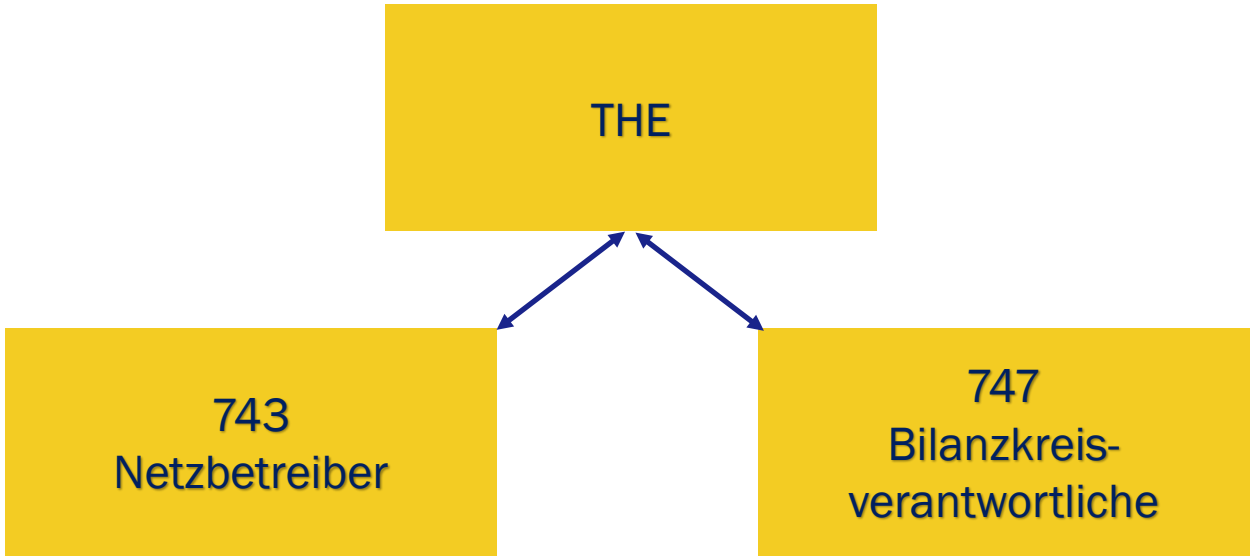
TRADING HUB EUROPE

Umsetzung des Projekts bei THE

Regulierte Umstellung der Marktpartner

- In der Zeit vom 01.10.2024 bis zum 01.11.2024 soll die Initiierung des Wechsels durch Senden einer AS4-Nachricht mit dem Service „Wechsel des Übertragungswegs“ nur vom Marktgebietsverantwortlichen ausgehen*

➔ Keine automatisierte Umstellung (Handshake)



*gem. Einführungsszenario AS4 für die Sparte Gas

TRADING HUB EUROPE

Umsetzung des Projekts bei THE

Konzept zur Umstellung der Marktpartner bei THE

- Begleitende Marktinformationen über verschiedene Kanäle (Mails, Kundenveranstaltungen, Pressemitteilungen, etc.)
- Tests von AS4-Verbindungen zu einzelnen Marktpartnern (Piloten) **ab August 2024**
- Abfrage von Wunschterminen /-zeiträumen bei den Marktpartnern durch THE zur Umstellung auf AS4
- Enge Abstimmung mit bekannten Dienstleistern zur möglichen Massenumstellung

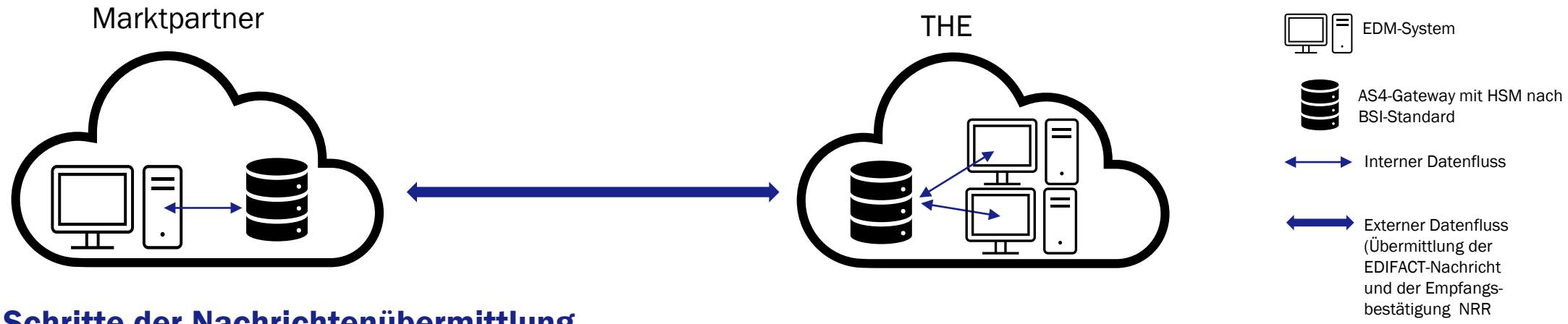
Herausforderungen

- Dauer der Erstellung von Zertifikaten durch die Certificate Authorities (CA‘s) unterschiedlich lang
- Parallele Verwendung von ENTSOG-AS4 und BDEW-AS4, je nach Prozess

TRADING HUB EUROPE

Umsetzung des Projekts bei THE

Ohne ein wenig Technik geht es leider nicht…



Schritte der Nachrichtenübermittlung

1. Aufbau der gesicherten Verbindung über die TLS-Zertifikate
2. Signaturprüfung anhand des Signaturzertifikats
3. Senden der technischen Empfangsbestätigung Non-Repudiation-Receipts (NRR)
4. Entschlüsselung der Nachricht
5. Syntax- und Semantikprüfung der EDIFACT-Nachricht
6. Versand CONTRL

TRADING HUB EUROPE

Umsetzung des Projekts bei THE

Fragen, die bisher für die Sparte Strom durch edi@energy beantwortet wurden (FAQ):

Was passiert nach einem Wechsel nach dem Wirktermin?

- Ein Wechsel per Pathswitch ist dann nicht mehr gestattet.

In welcher Form sind komprimierte Daten zu übermitteln?

- Es wird keine doppelte Komprimierung von Daten geben.

Welches Kryptographiemodul ist gestattet?

- Es müssen Kryptographiemodule gemäß Security Level 1 nach „Key Lifecycle Security Requirements“ verwendet werden.

Ist eine Regelung zur Höchstdauer der Zustellung einer NRR angedacht, bzw. ab welchem Zeitraum kann man davon ausgehen, dass eine AS4-Nachricht nicht zugestellt wurde und die Nachricht erneut gesendet werden kann

- Zurzeit ist keine Regelung geplant, die die Zeiten für den Aufruf des AS4 Web-Service betrifft.

TRADING HUB EUROPE

Vielen Dank für Ihre Aufmerksamkeit!

Team Datenmanagement

T: +49 2102 59796 401

M: datenmanagement@tradinghub.eu

TRADING HUB EUROPE

TRADING HUB EUROPE

keep in balance

Trading Hub Europe GmbH

Hauptsitz:
Kaiserswerther Straße 115
40880 Ratingen

Standort Berlin:
Anna-Louisa-Karsch-Straße 2
10178 Berlin

www.tradinghub.eu

Geschäftsführer

Dr. Thomas Becker, Jörg Ehmke,
Torsten Frank, Dr. Sebastian Kemper

Amtsgericht Düsseldorf, HRB 93885