TRADING HUB EUROPE

keep in balance

BDEW AS4 protocol launch in accordance with BSI requirements

Agenda

1. Regulatory background

- Federal Network Agency and BDEW
- BDEW AS4 protocol basics
- BDEW introduction scenario for the gas sector
- Certificates
  - Certificate authority
  - Certificate treble
  - Certificate application process
  - Technical implementation process

2. Project Implementation at THE

- Regulated conversion of market partners
- Conversion concept at THE
- A little bit of technology
- FAQ on the conversion of the electricity sector

TRADING HUB EUROPE

Regulatory background

TRADING HUB EUROPE

Regulatory background

Federal Network Agency and BDEW

Federal Network Agency decision BK7-19-001 of 22 November 2023 on GeLi Gas:

- Federal Network Agency requirements for the final implementation of the Applicability Standard 4 (AS4) message protocol, including the use of a smart meter public key infrastructure effective 1 April 2025

Implementation of BNetzA decision by BDEW:

1. Publication of rules for transfer protocol version 1.8 valid from 1 October 2024
   - Extension of the BDEW AS4 protocol to market communication for all business processes in gas sector
   - 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. Implementation scenario for the transition of electronic gas market communication to AS4
   - to prevent a hard changeover date Publication of EDI@Energy Application Help 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. Publication of rules for transfer protocol version 2.2 valid from 1 October 2024
   - Set of rules applicable after switch to BDEW AS4 profile
   - 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 profile version 1.0 – Consolidated version
   - Description of the technical requirements for the protocol
     - 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

Regulatory background

BDEW AS4 protocol basics

- Metering Point Operation Act (MsbG), Section 52(4)
  - Requirement to use the smart metering PKI for the exchange in data communication
- Technical Guideline TR 03116-3 (2023) of the Federal Office for Information Security (BSI)
  - Security requirements for cryptographic procedures in metering system infrastructure used in the energy sector
  - Definition of cryptographic algorithms and key lengths for certificates to be used in SM PKI
- **No more communication via AS2 or e-mail possible after the effective date**

  According to the BNetzA decision, market communication via e-mail or AS2 is no longer permitted after the introduction of the BDEW AS4 protocol.
- **No more firewall activation**

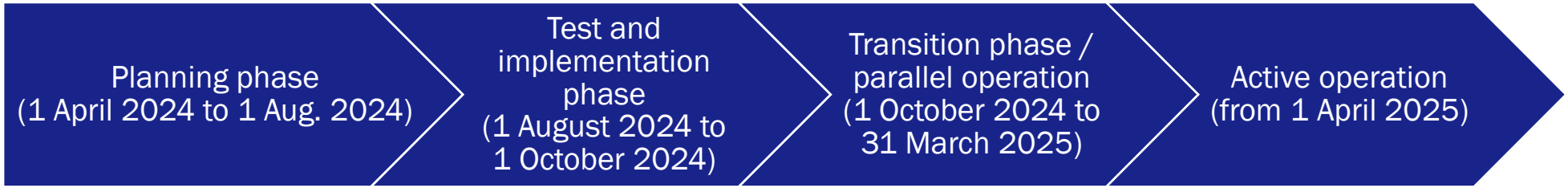
  Thanks to the technology used, firewall activation is no longer required at the start of communication following the introduction of the BDEW AS4 protocol.
- **Use of hardware security modules (HSM) and elliptic-curve cryptography (ECC)**

  Special HSMs approved by BSI are required for the BDEW AS4 protocol. The keys for the certificate are created on the HSM, and they are then submitted to the Certificate Authority (CA), which uses them to create the certificates. Encryption on the HSM involving elliptic-curve cryptographic (ECC) occurs each time a connection is established, and the data is then transmitted in encrypted form.
- **Establishing new connections involves inquiring with the Certificate Authorities (CAs) as to whether a certificate exists**

  When an AS4 connection to a new market partner is established, all CAs are asked whether there is a certificate for the market partner. If a CA has this certificate, it will send it to the requesting market partner.

Regulatory background

BDEW implementation scenario for the transition of electronic gas market communication to AS4:



TRADING HUB EUROPE

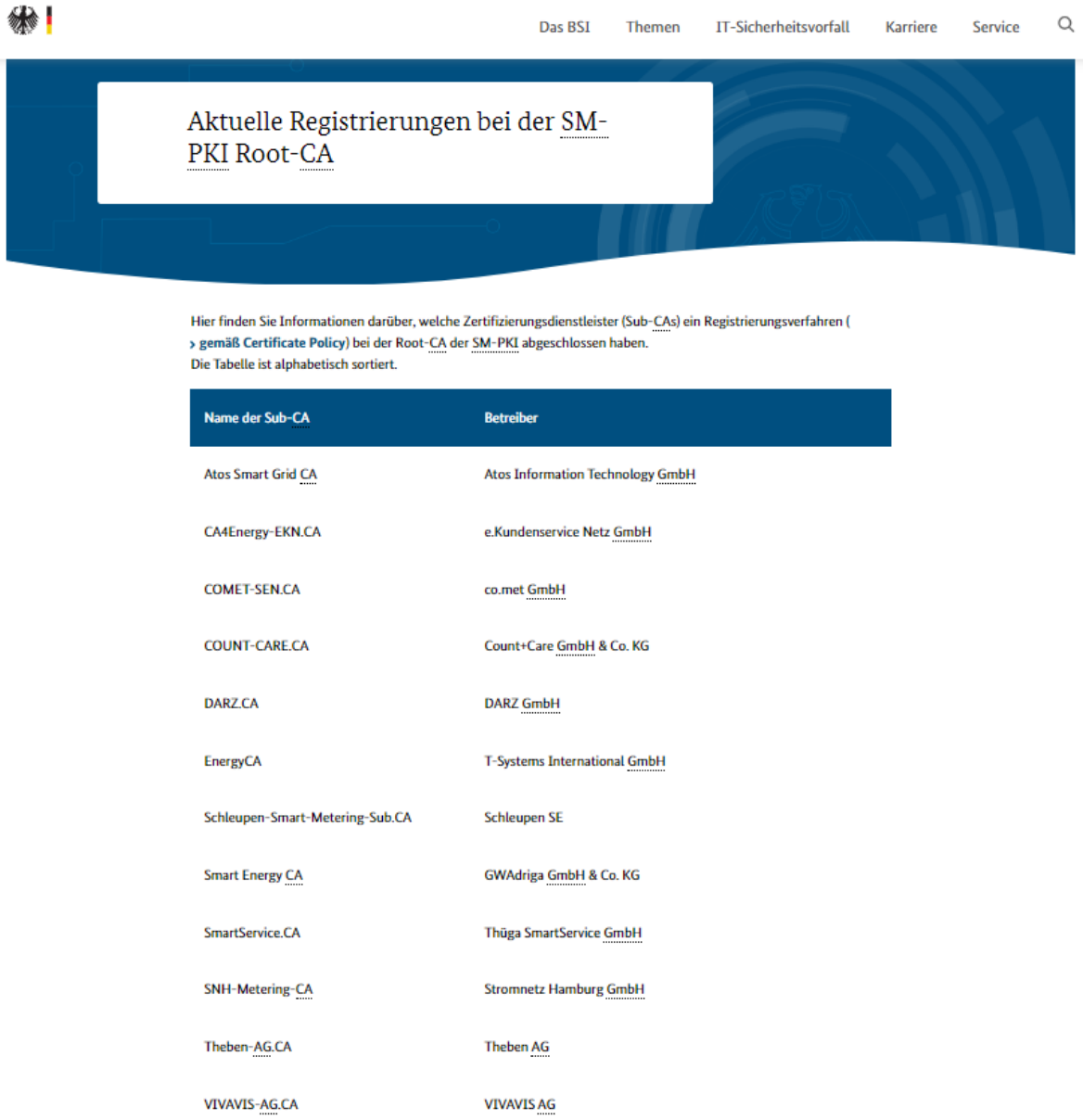
Regulatory background

Requirements to be met by Certificate Authority (CA)

Not every CA is authorised to issue a certificate for BDEW AS4 communication.

- The CA must be accredited by BSI.

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

Regulatory background

Certificate treble

The BDEW AS4 protocol requires a combination of three certificates ("certificate treble") for each market partner ID (MP ID). Previously, a combined certificate *("Kombi-Zertifikat"*) per company was sufficient. Now, three certificates are required per market role.

- The certificate treble consists of a
  - TLS certificate (secure ECC communication setup)
  - Signature certificate (authentication of sender and recipient)
  - Encryption certificate (encryption and decryption of EDIFACT message)
- The certificates must show the market partner IDs (MP IDs) and the communication endpoint (AS4 server including the path on the server).
- Each MP ID requires its own AS4 endpoint.

Regulatory background

Documents required for certificate application process

- Written confirmation from DVGW (German Association for Gas and Water Economy) that the MP ID belongs to the company (DVGW certificate of assignment *"Zuteilungsurkunde"*) in accordance with the Smart Meter Public Key Infrastructure (BSI) Certificate Policy
- Current extract from commercial register for the company
- Separate certificate applications for each MP ID and communication role for the test/effective certificates
  - Communication role (gateway administrator (GWA), external market participant (EMT), etc.) to be explained in application

Technical implementation process

- Generation of the key for the test certificates in the market partner's HSM after inspection of all documents and approval by CA
- Transfer of the keys generated on the HSM to CA for generation and storage of the certificate by CA
- Successful test proven to CA (with test certificate)

TRADING HUB EUROPE

Project Implementation at THE

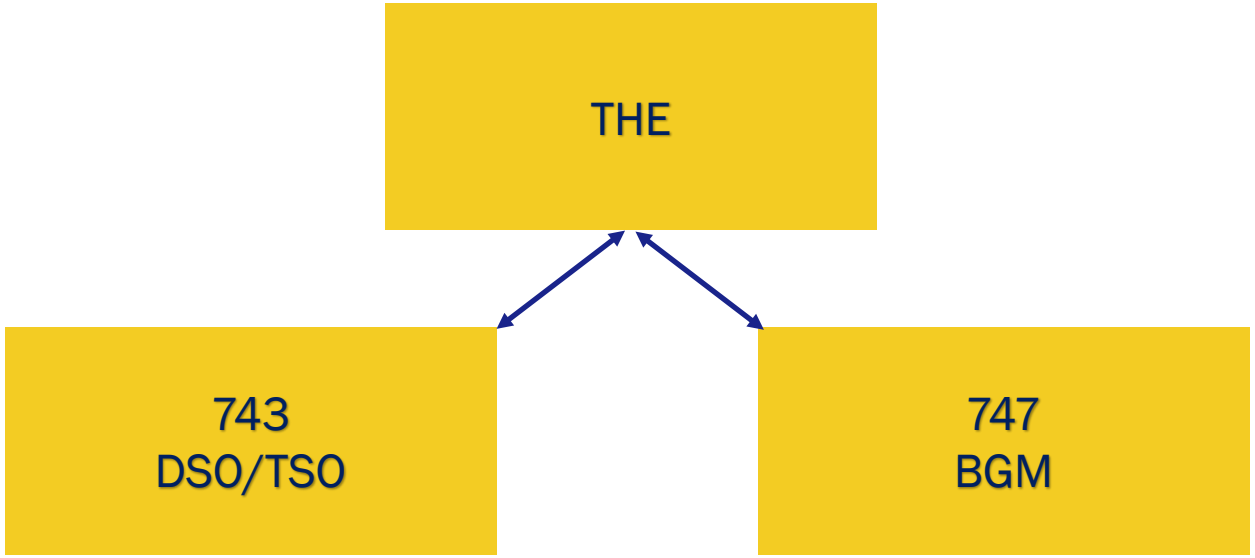
TRADING HUB EUROPE

Project delivery at THE

Regulated conversion of market partners

- In the period from 1 October 2024 to 1 November 2024, the switch should only be initiated by the market area manager sending an AS4 message specifying the "Change of transfer protocol" service*

➔ No automated changeover (handshake)



*AS4 implementation scenario for the gas sector

TRADING HUB EUROPE

Project delivery at THE

THE concept for market partner conversion

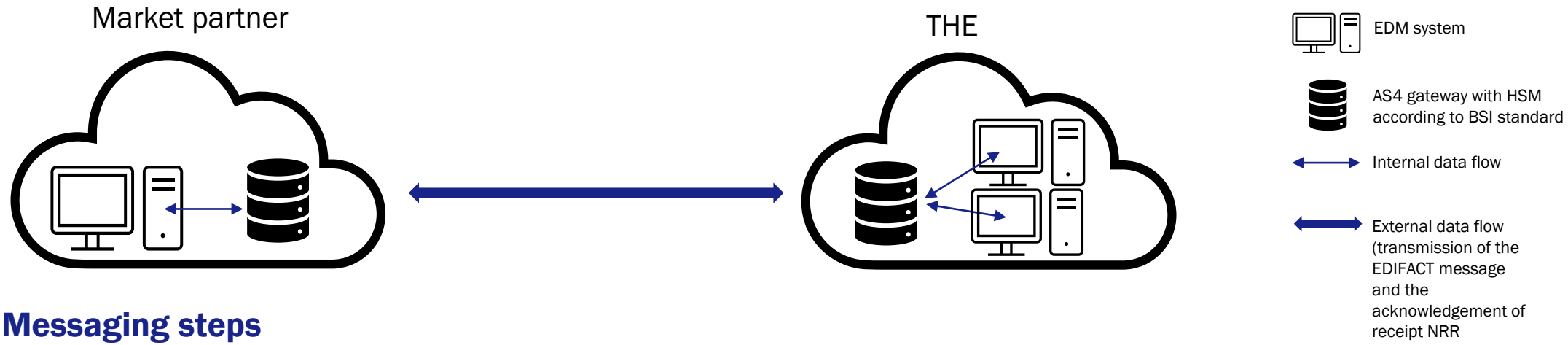
- Market information provided via various channels (e-mails, customer events, press releases, etc.)
- Tests of AS4 connections to individual market partners (pilots) **from August 2024**
- THE survey among market partners about desired dates/periods for changeover to AS4
- Close coordination with known service providers for possible mass conversion

Challenges

- Different lengths of time required by Certificate Authorities (CAs) to create certificates
- Parallel use of ENTSOG-AS4 and BDEW AS4, depending on process

Project delivery at THE

Unfortunately, you can't do it without a little bit of technology…



Messaging steps

1. Establish secure connection via TLS certificates
2. Verify signature using the signature certificate
3. Send technical acknowledgement of receipt – Non-Repudiation of Receipts (NRR)
4. Decrypt message
5. Perform syntax and semantic check of EDIFACT message
6. Send CONTRL message

TRADING HUB EUROPE

Project delivery at THE

Questions previously answered by edi@energy for electricity sector (FAQ):

What happens following a switch after the effective date?

- A switch via Pathswitch is then no longer permitted.

How should compressed data be transmitted?

- There will be no double compression of data.

Which cryptographic module is permitted?

- Cryptographic modules in accordance with Security Level 1 of the "Key Lifecycle Security Requirements" must be used.

Are there any plans for a rule on the maximum duration of the exchange of an NRR, or after what time can it be assumed that an AS4 message has not been delivered and the message can be sent again?

- There are no plans at present for a rule on times for calling the AS4 web service.

Are there differences between the VTP nomination via EU-XML an EDIFACT? Is there another service needed for XML nomination on the VTP?

- No, both nomination types will be transferred via service MP.

TRADING HUB EUROPE

Thank you.

Data Management Team

Phone: +49 2102 59796 401

E-mail: datenmanagement@tradinghub.eu

TRADING HUB EUROPE

TRADING HUB EUROPE

keep in balance

Trading Hub Europe GmbH

Head office:
Kaiserswerther Straße 115
40880 Ratingen

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

www.tradinghub.eu

Managing Directors

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

Düsseldorf Local Court, HRB 93885