



Picture courtesy of Gas Connect Austria

Joint ENTSOG, EASEE-Gas, GIE 6th Data Exchange Workshop

14th October 2026

ENTSOG offices, Brussels

1. Welcome



Piotr Kuś
General Director
ENTSOG

2. Info & Agenda



Douglas Walker Hill
ENTSOG

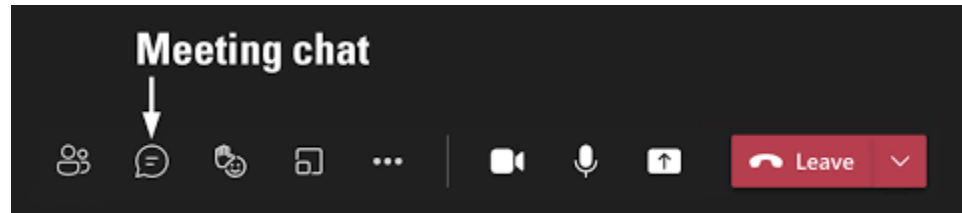
ENTSOE

'Family photo', end of today's session



To be used for social media and marketing etc...

Questions



- *Online please ask your questions via the Teams chat*
- *Physical attendance please ask questions at the end of the presentation*



Agenda Data Exchange Session



DATA EXCHANGE DAY 1

Interoperability,
Validation &
Secure Messaging

14 OCTOBER 2026

BRUSSELS, BELGIUM



EDIG@S
Standardised
data exchange
(Edig@s XML)



VALIDEX
Data validation
& quality
(XSD, Schematron)



AS4
Secure
messaging
& PKI



EASEE-gas
EASEE-connect &
certificate
management



PROGRAMME – DAY 1

14 OCTOBER 2026 | BRUSSELS, BELGIUM

TIME	SESSION	PRESENTER	AFFILIATION
13:00	Welcome	Piotr Kus	ENTSOG
13:05	Agenda	Douglas Hill	ENTSOG
13:10	REMIT updates	David Defour	GIE
13:30	EASEE-gas: Edig@s XML updates & Edig@s conformance review	Jeremy Devillers	Fluxys
13:50	Edig@s validation tool using XSD & Schematron	Rainer Gnan	Bayernets
14:25	Validex: Current status & roadmap	Pim van der Eijk	Sonnenglanz
14:40	Break	–	ALL
15:05	AS4: ENTSOG AS4 v3.6 & v4.0 exploring the differences in PKI architecture	Pim van der Eijk	Sonnenglanz
15:35	EASEE-gas: Migration of certificates	Dirk Serruys	EASEE-gas (TSWG Chair) (Fluxys)
15:55	EASEE-gas: EASEE-connect updates	Jean-Francois van Snick	EASEE-gas (Fluxys)
16:05	AS4: eDel EC AS4 v2.0 tools and updates	Bogdan Dumitriu	EC eDel
16:25	Wrap up Q&A	Douglas Hill	ENTSOG

Our normal wksp formular: **REMIT**>**Edig@s**>**AS4**

but with a twist...deeper insights

3. REMIT Updates



David Defour
CTO
GIE



WORKSHOP ON DATA EXCHANGE
AND DATA SECURITY

14 October 2026

REMIT reporting

GIE as REMIT Reporting Mechanism (**RRM**)

GIE as REMIT Inside Information Platform (**IIP**)

David Defour | GIE CTO – REMIT Administrator



Storage reporting



<https://agsi.gie.eu>

LNG reporting



<https://alsi.gie.eu>

UMM publication



<https://iip.gie.eu>

REMIT II

Impact on GIE as RRM and IIP

- **REMIT Implementing Regulation (EU) 2025/256 on Data Reporting**
REMIT Delegated Regulation (EU) 2026/255 on RRM and IIPs
were published in the Official Journal of the EU and entered into force on 29 April 2026
- **ACER Open Letters** on the implications of the IR and DR were published on 9 April 2026
- **ACER Guidance** and multiple **ACER Consultations** (ongoing)

MAIN TOPICS TO ADDRESS

Confidentiality | Data Integrity | Data Availability | Access Control | Authenticity | Accountability | Reliability

Technical process for the
testing phase as referred to
in Article 5(1)

Application process for **IIPs**
and **RRMs** already
registered and established
in the **Union** as referred to in
Article 8(1)

Data validation principles
and **processes** as referred to
in Article 12(1) and (2) by
providing technical standards
for the verification of data

Security measures referred
to in Article 13(1), point (d)

Format of the report on
unplanned downtime or
disruption as referred to in
Article 18(3)

Flagging process set out in
Article 24(4), if applicable

Mechanisms to identify
completeness, omissions
and **obvious errors** in
inside information reports
and **data records** as referred
to in Article 23(1) for IIPs and
Article 27(1) for RRM

Format of the **annual report**
as referred to in Article 33(1)

REMIT recast

IR and DR, ACER Guidance and Technical impact for RRMs and IIPs

IIP / RRM feedback / impact scope



Reporting incident scenarios

1	Inability to publish/submit	Unable to publish or submit to the Agency, but still able to collect data from clients.
2	Collection disruptions	Unable to collect information from clients
3	Data Quality / Timeliness	Still able to submit, but data does not fully meet regulatory requirements (completeness, accuracy, timeliness, validity, consistency).
4	Security Incidents	Any event compromising information security, regardless of whether reporting or disclosure services remain operational.
5	Operational disruptions	Able to disclose/submit information, but one or more operational/system regulatory requirements are not being met. Covers deficiencies in authentication, automated alerts, client communication channels, filtering of disclose information...

Increasing cybersecurity and data quality

NON-EXHAUSTIVE LISTING

- Extend **(Automated) monitoring & alert systems**
 - Notification of clients / platform audience / system health monitor status / version control systems
 - System monitoring for availability, response times, and error rates.
Weekly review, monthly reporting. Alerts when system availability drops below 99,5%.
- **Access control**
 - Organisations shall employ role-based access control (RBAC) or attribute-based access control (ABAC) mechanisms to restrict access exclusively to authorised users, aligned with ISO/IEC 27001:2013 Control A.9.
 - Quarterly access reviews mandatory
 - Apply multi-factor authentication (MFA)
- **Encryption**

Encryption using industry-standard algorithms such as AES-256. Data transmitted across networks must be secured using protocols like TLS version 1.2 or higher. Cfr. ISO/IEC 27001:2013 Control A.10.

Cryptographic key rotation at least every 6 months, Hardware Security Modules (HSMs) or managed Key Management Services (KMS) to generate, store, and protect cryptographic keys, backup copies of encryption keys in geographically separate locations, testing of key recovery processes

Increasing cybersecurity and data quality

NON-EXHAUSTIVE LISTING

- Apply and upgrade security measures ~ **proportionate** to organisation size, system complexity
- Map with **ISO/IEC standard requirements** / **NIS2 requirements** and **national transpositions**.
- **Review** intervals for **security controls** (e.g. formalized quarterly procedure review & firetesting)
- **Certifications** and regulatory attestations from cloud providers (e.g., Azure, AWS)
- Address **Information classifications, definitions** and **data sensitivity** aspects
- Extend **data logging: RRM**s are required to set up a **Register of invalid data & data corrections** implementation of ticketing / tracking system with unique case ID for technical reporting
- Implement and extend **cryptographic controls**, ... *wherever data is identified as sensitive, critical or subject to regulatory or operational protection requirements.*
- **Reporting timelines** : notify on downtimes / disruptions within 24 hours – via dedicated DRP channel
- **Re-Authorisation of RRM**s and **IIP**s in 2027 under the revised REMIT framework
 - *'via fast-track' procedure for re-authorisation (to be used by GIE as established RRM/IIP)*

Increasing cybersecurity and data quality

NON-EXHAUSTIVE LISTING

- DATA MANAGEMENT
 - **Data availability** : multiple mirrored datacentres for system redundancy
 - **Data retention** : set to 5 years for IIP and RRM (already covered by GIE)
 - **Data disposal** : documented permanent and secure destruction methods
 - **Data storage** : minimise for legitimate purposes only GDPR Article 5(1)(c) and ISO/IEC 27701:2019
 - **Data treatment** : staff training programmes, upgrade confidentiality policies
 - **Data loss prevention (DLP)** : Automated alerting and escalation mechanisms for DLP event
 - **Data mapping** : information systems and database inventory mapping
 - **Data classification** : Public, Internal, Confidential, or Restricted. Add auditing trails
 - **Data logging** : comprehensive logging for changes to critical data. 7 years retainment period of audit logs.
 - **Digital signatures** : to ensure authenticity, integrity & non-repudiation. ISO/IEC 27001:2013 Control A.10.1.
- Update of **Data validation principles and processes**
- Update of **Mechanisms to identify completeness, omissions and obvious errors**

Increasing cybersecurity and data quality

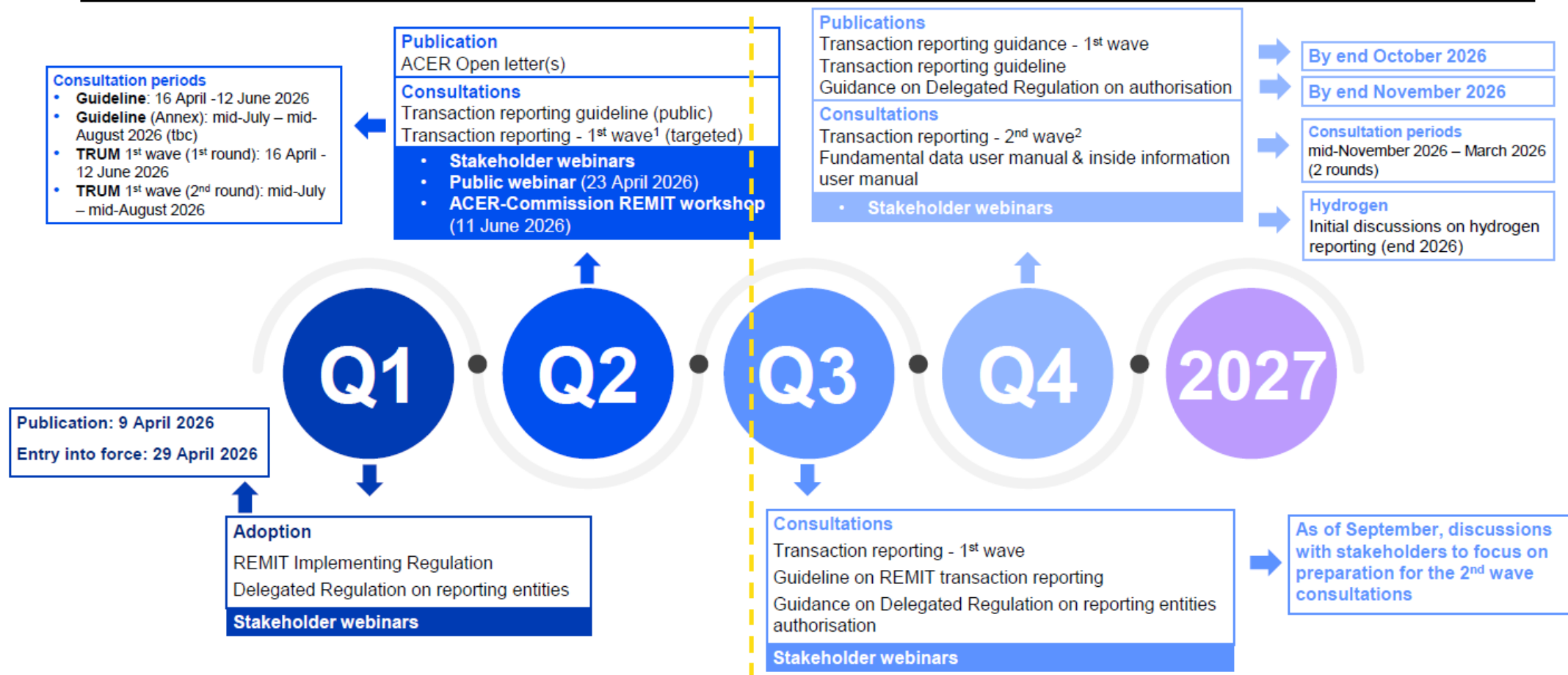
- **Business continuity:**
 - Contractual arrangement with another back-up IIP, at no additional cost to the IIP client
 - Establishment of failover and fallback procedures that specify the automated redirection of IIP clients
 - Provide IIP clients with instructions on the use of back-up facilities and issue periodic reminders
 - Regular testing of backup and recovery procedures
 - RTO (Recovery Time Objectives) : 4 hours for critical systems (ISO/IEC 27001:2013 Control A.17.1.1.)
 - RPO (Recovery Point Objective) not exceeding 1 hour (ISO/IEC 27001:2013 Control A.17.1.1.)
- **Authentication and identity verification** : request for ACER list of recognized authentication solutions
- **RRMs** set up **Register of invalid data**
- **IIPS** are required to set up a **Data Flagging** process for identification of invalid data disclosed via **UMM**
- Publication of **Annual Report** by RRM towards ACER for supervision of reporting entities, including full details of exchanges with clients, with identification, interactions and responsiveness

MP Name	ACER code	Number of Invalid Data Records	Number of Instances where the Client was contacted	Data type
---------	-----------	--------------------------------	--	-----------

Timeline

REMIT II implementation

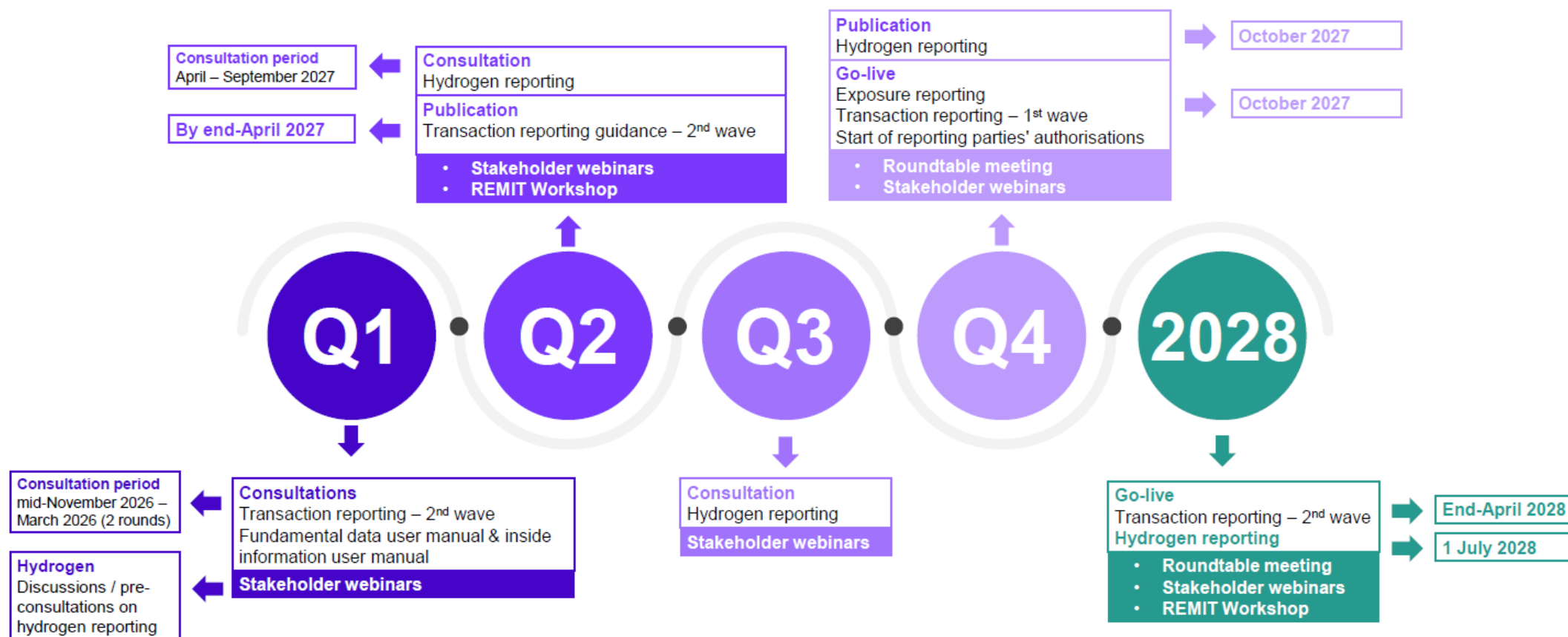
Milestones & timeline for REMIT implementation (2026)



Timeline

REMIT II implementation

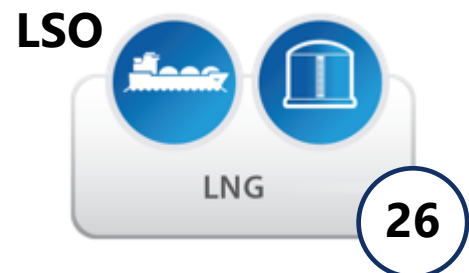
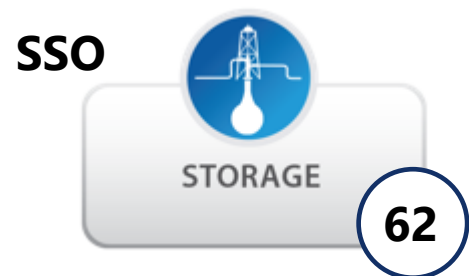
Indicative planning: 2027



REMIT & Transparency Platforms

Data processing / AS4 adoption status

GIE REGISTERED REPORTING MECHANISM **REMIT 9**
Separate Production + Acceptance/Test environment



RRM
IIP

4984 users

22 countries

141 operators

WEBGUI 74
Online Forms
XML Upload

SFTP 16

AS2 28

- 5

AS4 33

+ 13

SOAP



REMIT Reports
GIE Receipts
ACER Receipts

Evolution since

01/10/2025

AS4 is now the primary method to submit data

FacilityReports (AGSI/ALSI) per gasDay scheduled, **publication time 19:30 daily**
second processing run at 23:00
ISO8601 time format, UTC only

GIE REGISTERED REPORTING MECHANISM **REMIT**

850+ files/day

cd data arc



SENTIA
accenture



REMIT Reports
ACER Receipts



SFTP

AS4

ACER
European Union Agency for the Cooperation of Energy Regulators

ARIS
ACER REMIT Information System



RSSfeed

IIP REMIT UMM
Inside Information Platform

TRANSPARENCY PLATFORMS

AGSI
Aggregated Gas Storage Inventory

ALSI
Aggregated LNG Storage Inventory



RSSfeed



ATOM | RSS | JSON | CSV | PDF | XLSX

250000 datacalls/day

2000+ API users

3 XML schemas
6 reporting types
- sFAR - IFAR
- sUNR - IUNR
- sPAR - UMM

The logo features a stylized power symbol (a circle with a vertical line and a horizontal line) integrated with the letter 'G'. The letters 'IE' are in a clean, sans-serif font. The entire logo is white and set against a background of glowing blue cubes with binary code (0s and 1s) on their faces.

GIE

THANK YOU

For your attention

Avenue de Cortenbergh 100
1000 Brussels - BELGIUM

T +32 2 209 05 00
gie@gie.eu

@GIEBrussels
www.gie.eu

4. EDIG@S. 6.1 – 2026 updates



Jeremy Devillers
Fluxys

0.

Agenda



1. Introduction to EASEE-gas and Edig@s
2. Work done in 2026
 - a) MARSIT documentation rework
 - b) Overnomination Response message
 - c) REMIT version 6.1
 - d) Scorecard process
 - e) Promotion activities
3. Edig@s Roadmap for 2027

01.

Introduction



FOUNDED IN
2002

80+
EUROPEAN
MEMBERS



EASEE-gas
Streamlining the gas business

edig@s
The European message format for the gas market



EASEE-gas promotes and develops solutions for the simplification and streamlining of trading and physical transfer of gas.

Created to drive market **harmonisation** and technical **interoperability** by aligning regulatory requirements with business needs through active cooperation across the entire gas value chain.

Edig@s
Who are we?

EASEE-gas
Streamlining the gas business

edig@s
The European message format for the gas market

equinor

VNG
Handel & Vertrieb

entsog

gmsl

**Amber
Grid**

storengy

axway

snam

GASSCO

GASCADE

ENGIE

GAZ
system

gasum
crossing borders in energy

SERCOMGAS

CEGH

PRISMA.
European Capacity Platform

fluxys

conexus
BALTIC GRID

Ørsted

CEΘAL

eni

ENERGINET

exeta

natran

THE
TRADING
HUB
EUROPE
keep in balance

SWISSGAS

volue

**uni
per**

FGSZ
A MOL-CSOPORT TAGJA

**GAS CONNECT
AUSTRIA**

TEREGA

TürkAkım
Gaz Taahhüt A.Ş.

ECC
European
Commodity
Clearing

NET4GAS

PSvdL
CONSULTING

navitasoft

EnBW

energyone

TANAP

02.

Work done



1. Introduction to EASEE-gas and Edig@s

2. **Work done in 2026**

- a) MARSIT documentation rework
- b) Overnomination Response message
- c) REMIT version 6.1
- d) Scorecard process
- e) Promotion activities

3. Edig@s Roadmap for 2027

Introduction

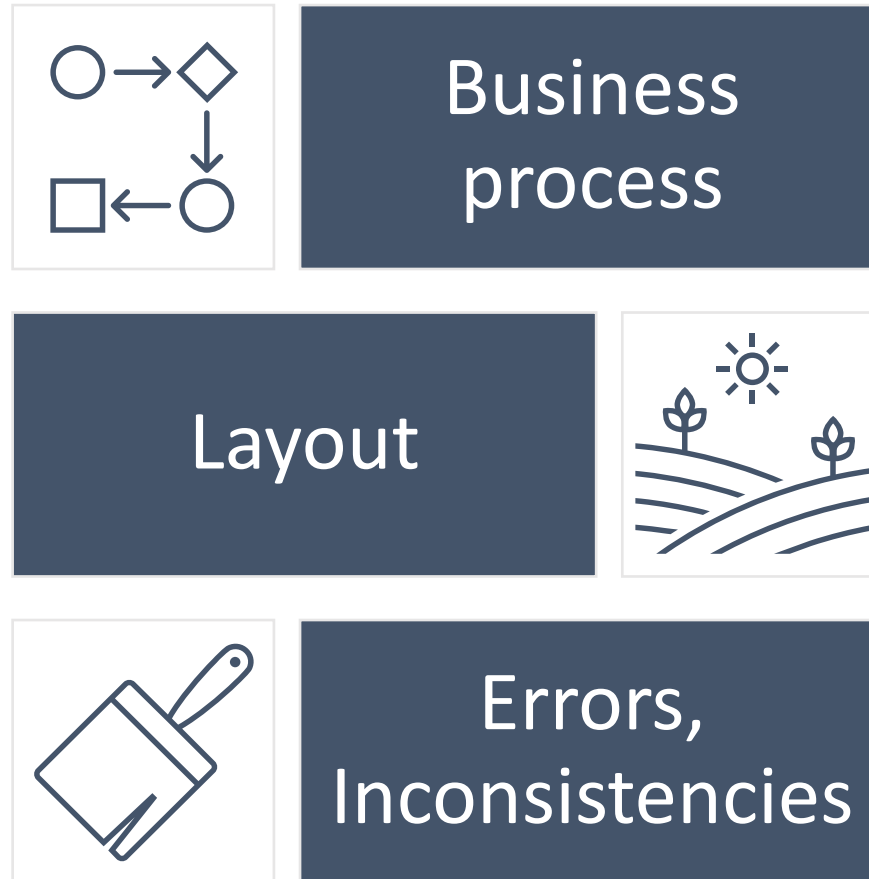
Accurate and timely information on allocated quantities, market positions, and account imbalances is essential for effective portfolio management, enabling compliance with balancing obligations while optimizing asset performance.



MARSIT
Documents

In line with NC BAL.

Document review areas



Review constraint: the schema must remain unchanged

Business Processes

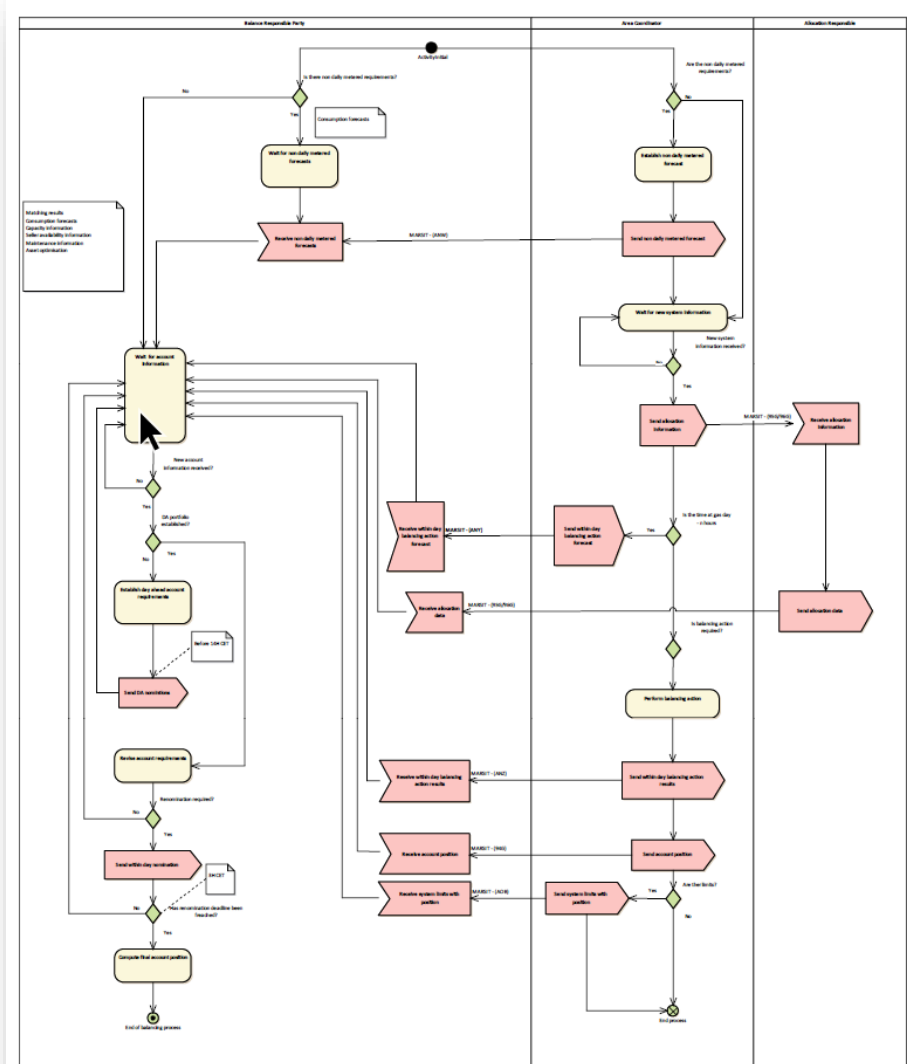
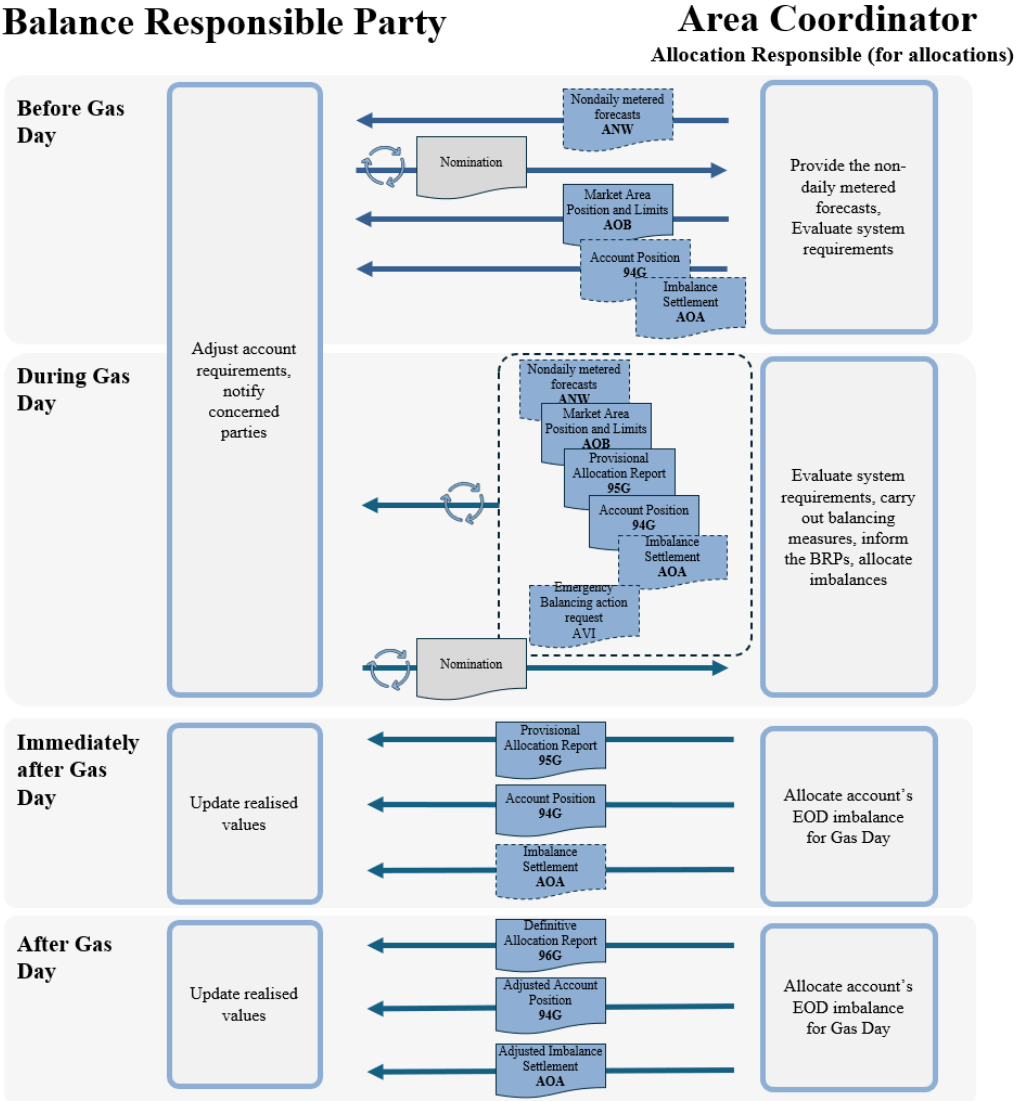


Figure: 2 Balancing workflow



Document Layout

Each business process has a dedicated chapter, including an example of the schema usage.

4 Non-Daily Metered Forecast

4.1 Process Description

If a Balance Responsible Party's account includes non-daily metered consumer sites, the Area Coordinator shall provide forecast updates of the non-daily metered off-takes. This information can be provided at the connection point level or at the Market Area level (aggregated value for all sites).

The frequency and the lead times of the forecast updates depend on the information model in place (according to Balancing Network Code, 3 types of information model are possible to be implemented in a Market Area: base case, variant I and variant II).

4.1.1 Non-Daily Metered Forecast (ANW)

The source of information on non-daily metered off-takes forecast is the forecasting party designated by the regulatory authority (it may be Distribution System Operator, Transmission System Operator or a third party). For the purpose of simplification and taking into account that usually the forecasting party is a system operator, the role of System Operator is used in this document instead of forecasting party.

The System Operator shall provide the Area Coordinator with the forecast of Balance Responsible Party's non-daily metered off-takes. The timing to provide this information to the Area Coordinator shall be sufficient to allow the Area Coordinator to communicate the Balancing Responsible Party with the forecasted quantity and for day-ahead and within-day forecast, it shall not exceed one hour before deadlines defined in Balancing Network Code for a given information model in place.

4.2 Document Structure Overview

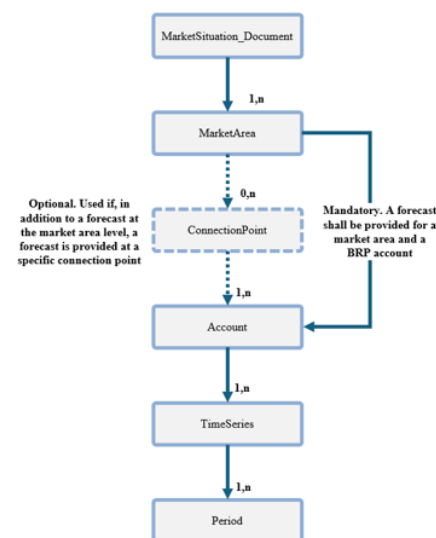
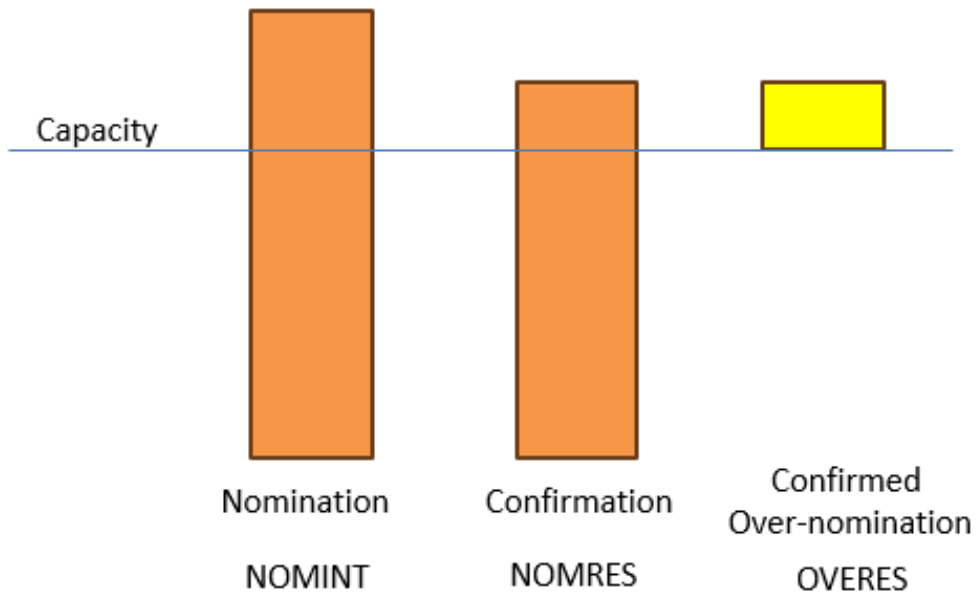


Figure 3 Example structure for Non-Daily metered forecast

Over-nomination



Definition and process:

Over-nomination refers to the act of requesting/nominating more capacity than has been contractually subscribed or allocated.

The **NOMINT** and **NOMRES** messages contain the global flowing request and the operator related confirmation. NOMRES is sent to the Balancing Responsible Party.

The **new OVERES** message contains the allocated over-nominated quantity and associated charge which will be invoiced later.

REMIT reporting

- Table 4 Gas Capacity Allocation Schema will be published in Edig@s 6.1, not in Edig@s 5.1
- Fundamental data schemas (Nomination Monitoring and Contractual Monitoring) will also be migrated to Edig@s 6.1 (Target publication in 2027 and implementation in 2028)



REMIT
Documents

Scorecard

The EASEE-gas Scorecard is a structured evaluation tool designed to promote interoperability, transparency, and usability across European gas market interfaces.

Initial evaluation in 3 main categories, based on a predefined set of evaluation criteria.

1. Connectivity
2. Message Implementation
3. Documentation & Transparency

Category	Score
Connectivity	★★★★☆ (4/5)
Message Implementation	★★★☆☆ (2/5)
Documentation & Transparency	★★★☆☆ (2/5)

Scorecard Objectives

- To provide a **consistent and transparent comparison tool** for TSO's
- To create an opening for the **improvement dialogue** with the TSO, to enable progression more actively in the market via the Edigas WG
- To gather **insights and information** on important topics like connectivity, message implementation and documentation & transparency

Promotion activities

- Conducted workshop with Energy Traders Europe (ETE) for Storage & LNG messages
- Proposed workshop with GIE
- Ongoing talks to ACER about REMIT 6.1
- Today joint workshop with GIE and ENTSOG
- Scorecard approach

03. Roadmap



1. Introduction to EASEE-gas and Edig@s
2. Work done in 2026
 - a) MARSIT documentation rework
 - b) Overnomination Response message
 - c) REMIT version 6.1
 - d) Scorecard process
 - e) Promotion activities
3. **Edig@s Roadmap for 2027**

Roadmap 2027

NC CAM/CMP update

Expect ready Q4 2026.

Implementation 2027 (expect changes in codelist)

NC INT

Assess impact

Further improvements of messages and documentation

ACKNOW

REMIT version 6.1

New ways of documentation

Review all CBP's (Common business practice guides)

Finalise CBP for business continuity management

Edig@s support

The support of Edig@s version 5 will end in **March 2027**.

All market participants are encouraged to implement 6.1.

In case of any questions, please reach out to the MWDWG for support.

THANK YOU



Website
easee-gas.eu/

5. Edig@s validation: XML, XSD & Schematron



Rainer Gnan
Bayernets

Edig@s Validation

XML, XSD & Schematron

bayernets GmbH

Brussels, 14 October 2026

Rainer Gnan :: IT Systems Specialist - Communication Systems

Edig@s Validation | Agenda



Edig@s Validation | Agenda



XML Stack | XML

Well-formedness

A linguistic expression A from a language L is called well-formed if it conforms to the syntactic rules of L:

“Colorless green ideas sleep furiously.”

XML Stack | XML

Well-formedness

An XML document is well-formed if it conforms to the syntactic rules defined by the W3C XML specification:

<Nomination_Document>

 <identification>xml document</identification>

 <colorless green="true">syntactically</colorless>

 <ideas>well-formed</ideas>

</Nomination_Document>

XML Stack | XML

1. XML Parser

- Checks whether the XML is well-formed
 - If yes:
 - can be processed by the receiving system
 - Otherwise:
 - XML processing error

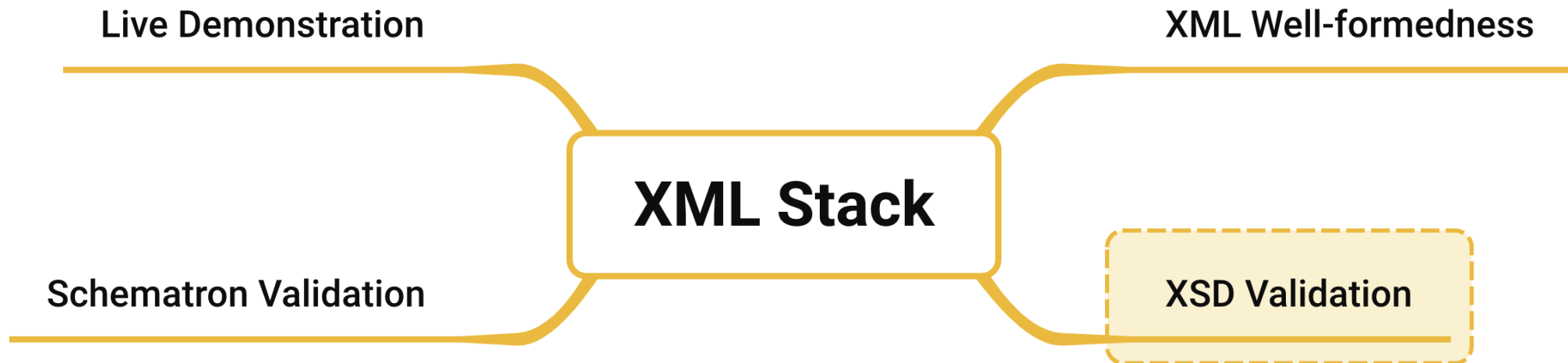
2. XML Syntax Rules

- Elements
 - Names in start and end tag must match exactly
 - Names must begin with a letter or underscore
 - Names may then contain
 - ... letters, underscores, colons, digits
 - ... hyphens and/or periods ...
 - No whitespace immediately after the opening „<„
 - ...
- Attributes
 - ...
- ...

Edig@s Validation | Agenda



Edig@s Validation | Agenda



XML Stack | XSD

1. Structure & Data Types

- Definition of document structure
- Precise distinction between data types
- Support for namespaces

2. Constraints & Limitations

- Definition of permitted value ranges
- Definition of allowed character patterns
- Specification of default values
- Complex dependencies between values cannot be expressed directly

XML Stack | XSD

```
<?xml version="1.0" encoding="UTF-8"?>
<xs:schema xmlns:xs="http://www.w3.org/2001/XMLSchema" >
  <xs:element name="Nomination_Document" type="demo">
    <xs:complexType name="demo">
      <xs:sequence>
        <xs:element name="identification" type="xs:string"/>
        <xs:element name="version" type="xs:string"/>
        <xs:element name="documentCode" type="xs:string"/>
        <xs:element name="creationDateTime" type="xs:string"/>
        <xs:element name="validityPeriod" type="xs:string"/>
        <xs:element name="issuer_MarketPart" type="xs:string"/>
        <xs:element name="issuer_MarketPart" type="xs:string"/>
        <xs:element name="recipient_MarketPart" type="xs:string"/>
        <xs:element name="recipient_MarketPart" type="xs:string"/>
        <xs:element name="Internal_Account" type="xs:string"/>
      </xs:sequence>
      <xs:attribute name="schemaVersion" type="xs:string"/>
    </xs:complexType>
  </xs:element>
</xs:schema>
```

XSD Vocabulary (incomplete list)

- **Elements**
 - <xs:element>
 - <xs:attribute>
- **Types**
 - <xs:simpleType>
 - <xs:complexType>
- **Compositors**
 - <xs:sequence>
 - <xs:choice>
- **Constrains**
 - <xs:restriction>
 - <xs:pattern>

XML Stack | XSD

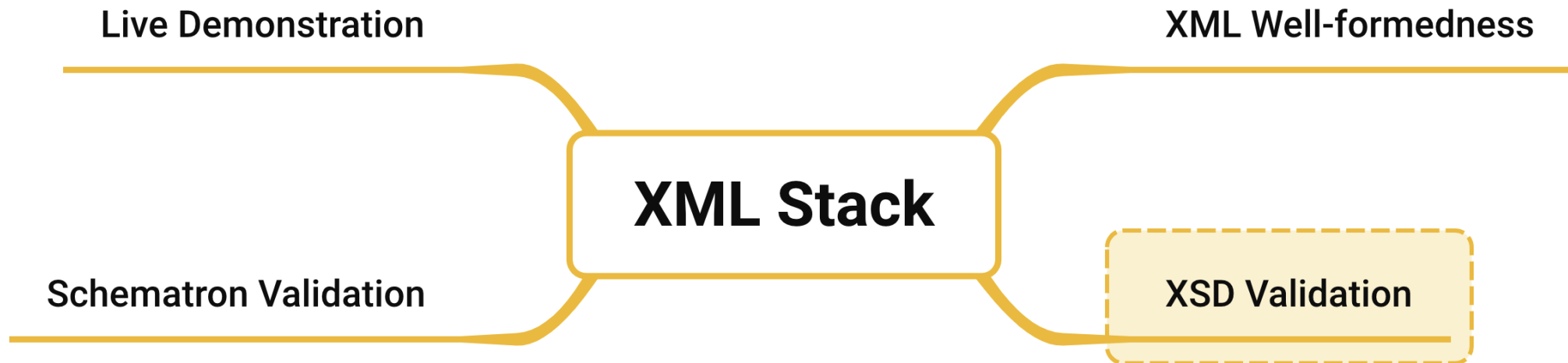
1. XSD Validator

- Reads the XML document
- Reads the corresponding XSD
- Checks whether the XML is valid
 - If yes:
 - Can be processed by the receiving system
 - Can be handed over to the next validation layer
 - Otherwise:
 - Validator reports a validation error

2. XSD

- Elements
 - Required ones are present
 - Appear in the correct order
 - Belong to the correct namespaces
 - ...
- Values
 - Expected data types
 - Expected patterns
 - Expected value range
 - ...

Edig@s Validation | Agenda



Edig@s Validation | Agenda



XML Stack | Schematron

XSD:

„Is the value structurally and type-wise valid?“

Schematron:

“Does the value make sense and comply with the business rules in the specific context?“

XML Stack | Schematron

Business Rules (incomplete list)

- Conditional business rules
 - „If A, then B must apply.“
- Cross-element consistency rules
 - „If A and B are related, then their values must be consistent with each other.“
- ...

XML Stack | Schematron

```
<?xml version="1.0" encoding="UTF-8"?>
<schema xmlns="http://purl.oclc.org/dsdl/schematron">
  <ns uri="urn:easee-gas.eu:edigas:BrpNominationAndI">
  <pattern id="BR-NOMINT-001">
    <rule context="edigas:Period">
      <assert test="
        xs:dateTime(replace(substring-before(
          &gt;=
          xs:dateTime(replace(substring-before(
            and
            xs:dateTime(replace(substring-after(
              &lt;=
              xs:dateTime(replace(substring-after(
            ">
            BR-NOMINT-001: Period/TimeInterval must be
          </assert>
        </rule>
      </pattern>
    </schema>
```

Schematron Vocabulary (incomplete list)

- **Core Elements**

- <ns>
- <pattern>
- <rule>
- <assert>
- <report>
- ...

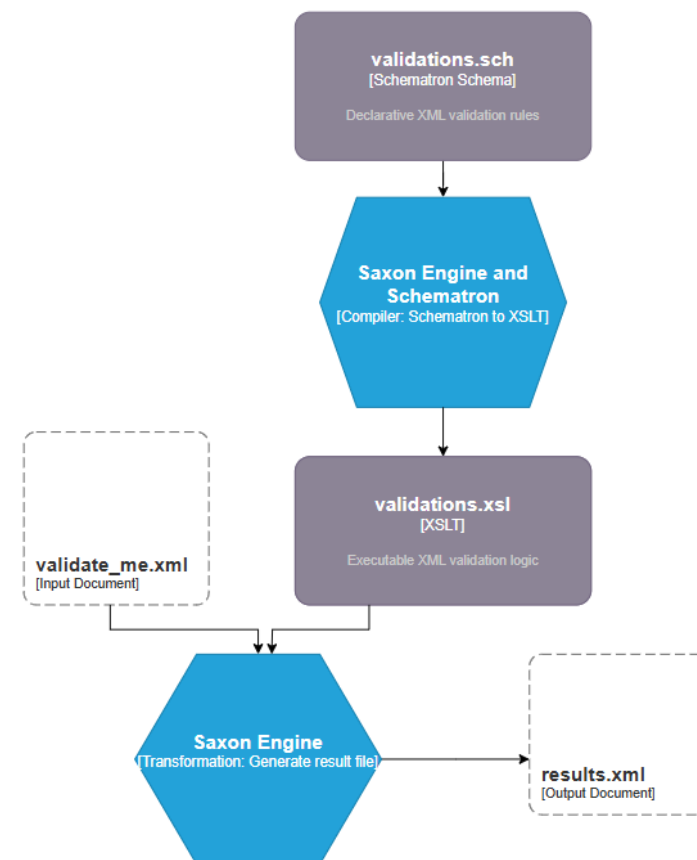
XML Stack | Schematron

Schematron Compilation Process

Schematron compilation transforms a Schematron schema containing declarative validation rules into an executable representation.

This representation is then applied to an XML document to evaluate the rules and produce validation results.

Depending on the implementation, the executable representation may be XSLT, and the validation results may be represented as SVRL or another implementation-specific format.



XML Stack | Schematron

Schematron Validity

An XML document is Schematron-valid when all applicable Schematron rules evaluate successfully. Meaning that all required business, semantic, and cross-element constraints are satisfied.

Edi@s Validation Service implements Edig@s Guideline requirements as executable Schematron business rules.

```
<?xml version="1.0" encoding="UTF-8"?>
<!-- IMPORTANT! ALL comments in this document are provided for better
<Nomination_Document xmlns="urn:easee-gas.eu:edigas:BrpNominationAndl
  <identification>NOMINT-01G-border</identification>
  <version>1</version>
  <documentCode>01G</documentCode>
  <creationDateTime>2020-01-12T19:30:47Z</creationDateTime>
  <validityPeriod>2020-01-13T05:00Z/2020-01-14T05:00Z</validityPer
  <issuer_MarketParticipant.identification codingScheme="305">Issue
  <issuer_MarketParticipant.marketRole.roleCode>ZSH</issuer_Market
  <recipient_MarketParticipant.identification codingScheme="305">Re
  <recipient_MarketParticipant.marketRole.roleCode>ZS0</recipient_
  <Internal_Account>
    <internalAccount codingScheme="ZS0">ACCOUNT</internalAccount>
    <ConnectionPoint>
      <identification codingScheme="305">ConnectionPntEIC</iden
      <measureUnit.unitOfMeasureCode>KW1</measureUnit.unitOfMea
      <NominationType>
        <nominationCode>A02</nominationCode>
        <External_Account>
          <externalAccount codingScheme="ZS0">COUNTERPARTY
          <Period>
```

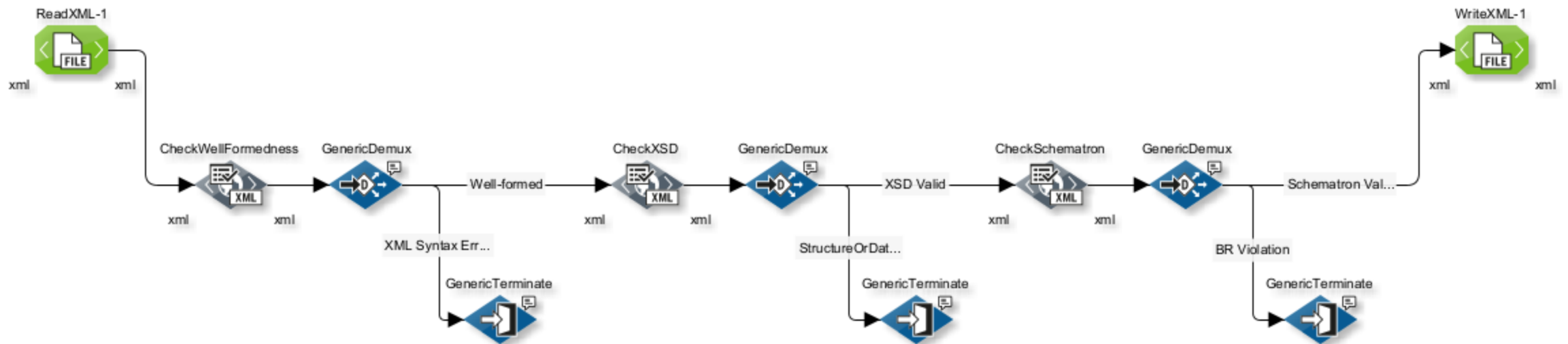
Edig@s Validation | Agenda



Edig@s Validation | Agenda



XML Stack | Live Demonstration



Contact

Rainer Gnan

Telefon: + 49 89 890572-474

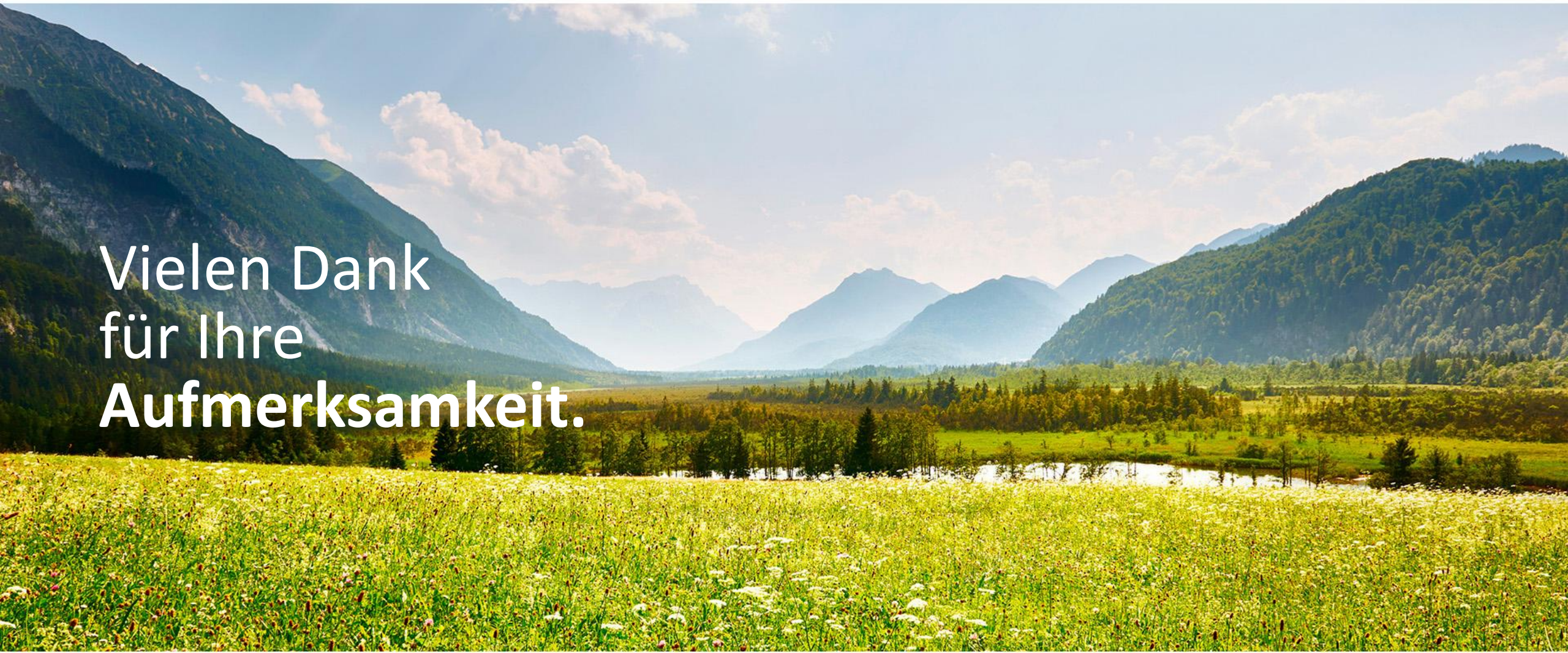
E-Mail: rainer.gnan@bayernets.de

bayernets GmbH

Poccistraße 7

80336 München

www.bayernets.de



Vielen Dank
für Ihre
Aufmerksamkeit.

6. ENTSOG CNOTS: Data exchange validation tool for Edig@s 6.1 and schematron



Pim van der Eijk
Sonnenglanz Consulting

Edig@s

About Edig@s

News

Downloads

EDI Validation Tool

Forms

EIC

Remit

Edig@s: The European message format for the gas market

Edig@s is a comprehensive electronic data interchange (EDI) format for the commercial information exchange by electronic means between partners involved in the European gas industry.

Widely recognised and used by the industry, Edig@s had become the de facto electronic message format for gas information exchange.



The European message format for the gas market

EDIG@S downloads

Edig@s Downloads

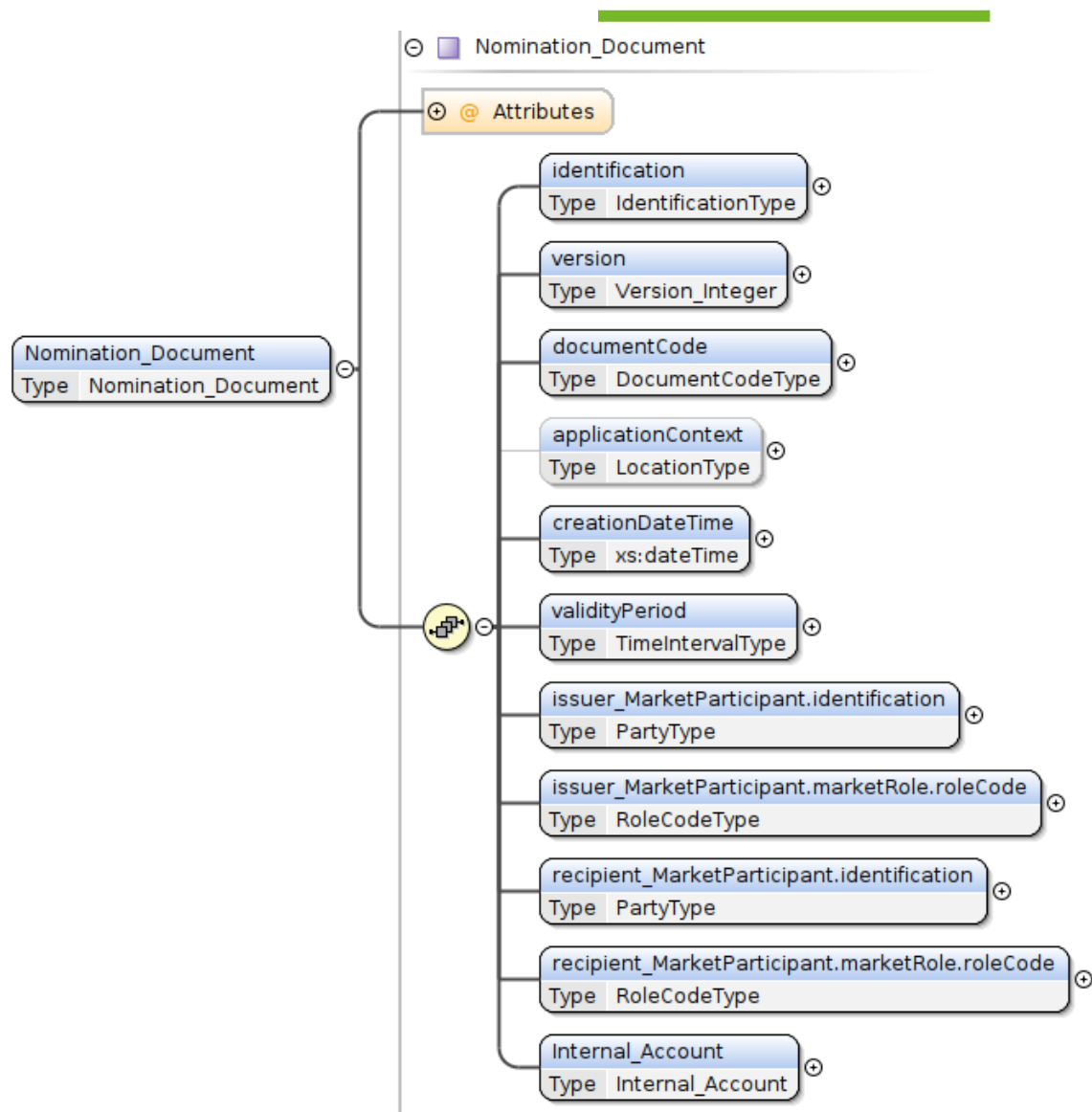
Version 6.1 - Recommended

Title		Size
	<u>Edig@s Version 5.1 and 6.1 Comparison</u>	4 MB
	<u>Deprecated items</u> Version 5 and 6 overview of deprecated items.	110 KB
	<u>Version 6.1: Whole package</u> All Edigas v6.1 documents, examples, XSD's etc. in one zip file.	23 MB
	<u>Edigas 6.1 - Document Overview.xlsx</u>	119 KB

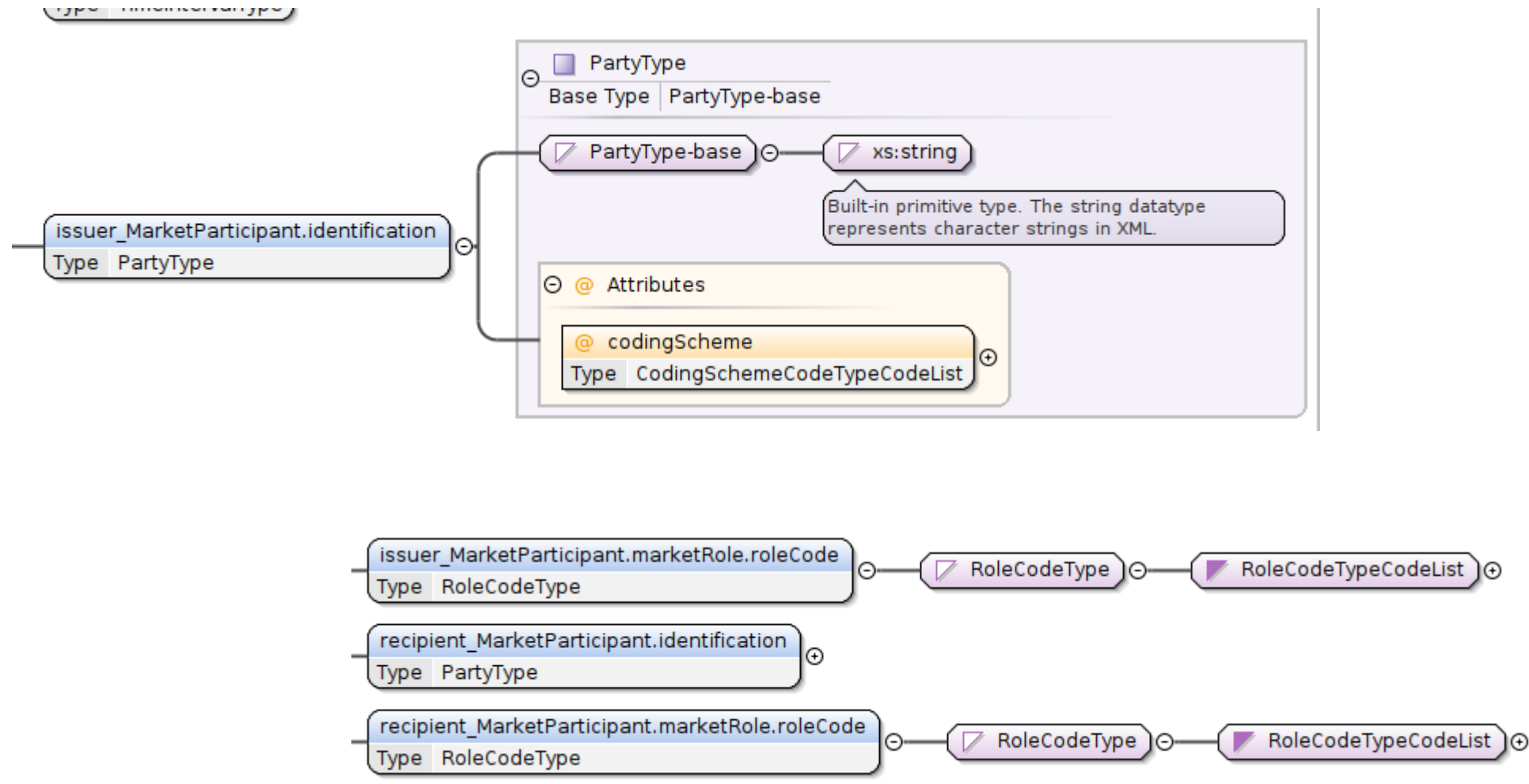
Package content

- **Implementation Guidelines**
 - Ground rules
 - Models for each process
- **Schemas**
 - Document schemas
 - Types and code list schemas
- **Examples**
- **Best practices**
- **Release notes, comparison etc.**

Nomination Document – XML Schema



Nomination Document – XML Schema



Nomination Document – XML Instance



```
<version>1</version>
<documentCode>01G</documentCode>
<creationDateTime>2020-01-12T19:30:47Z</creationDateTime>
<validityPeriod>2020-01-13T05:00Z/2020-01-14T05:00Z</validityPeriod>
<issuer_MarketParticipant.identification codingScheme="305">21X0000000001006T</issuer_MarketParticipant.identification>
<issuer_MarketParticipant.marketRole.roleCode>ZSH</issuer_MarketParticipant.marketRole.roleCode>
<recipient_MarketParticipant.identification codingScheme="305">21X-IT-A-A0A0A-7</recipient_MarketParticipant.identification>
<recipient_MarketParticipant.marketRole.roleCode>ZS0</recipient_MarketParticipant.marketRole.roleCode>
<Internal_Account codingScheme="305">ACCOUNT</Internal_Account>
```

Nomination Document – Decision Table

1.2 Nomination Document

Nomination document	Connection Point	VTP OTC	VTP exchange	Non matching nomination
identification			Mandatory.	
version			Mandatory.	
documentCode	01G = Nomination.	02G = VTP OTC nomination.	03G = VTP exchange nomination.	04G = Non matching nomination.
creationDateTime			Mandatory.	
validityPeriod			Mandatory.	
applicationContext	May be used. Deprecated attribute which will be removed in the next version of Edig@s.			
issuer_MarketParticipant.identification		Mandatory; codingScheme = 305 (EIC Party X code).		
issuer_MarketParticipant.marketRole.roleCode	ZSH = Balance Responsible Party.	ZSH = Balance Responsible Party.	ZUM = Clearing Responsible	ZSH = Balance Responsible Party.
recipient_MarketParticipant.identification		Mandatory; codingScheme = 305 (EIC Party X code).		
recipient_MarketParticipant.marketRole.roleCode	ZSO = System Operator.	ZUK = Area Coordinator.	ZUK = Area Coordinator.	ZSO = System Operator.
Internal_Account.internalAccount	Mandatory; codingScheme = 305 (EIC Account Y code) or ZSO (System Operator).			
Internal_Account.internalAccountTso	Used if the account identification is ambiguous; codingScheme = 305 (EIC Party X code).			
connectionPoint.identification	Mandatory; codingScheme = 305 (EIC Measurement Point Z or Y code) or ZSO (System Operator).			
ConnectionPoint.measureUnit.unitOfMeasureCode		KW1 = Kilowatt-hour per hour (kWh/h). KW2 = Kilowatt-hour per day (kWh/d). A15 = Kilogram per hour (Kg/h)		
NominationType.nominationCode	A01 = Single sided. A02 = Double sided.	A02 = Double sided.	Not used.	Not used.

Collaboration and joint effort of EASEE-gas and ENTSOG

- TSOs requested a tool to help XML instance checking against Edig@s 6.1
- Increase the level of conformance to both Edig@s 6.1 XSDs and document usage decision tables and other guidelines
- Implement the validation logic in a standard: Schematron
- Deploy the logic in a validation portal for ease of case
- (Future, TBC) make Schematron validation rules available to users
- Aims to encourage and facilitate uptake of 6.1 in the gas sector (including new gases)

High level benefits of an Edig@s validation tool

Help market participants validate their Edig@s 6.1

- Encourage market participants to check their implementations against THE standard and also to give tools to help migration to 6.1
- Flag up where there are inconsistencies with a given implementation
- Reduce mistakes in interpretation of the usage of fields (reduce misuse)
- Facilitate upfront counterparty message testing (check before sending test file)

Edig@s 6.1 XML validation portal



edigas.validex.net/en/login



The European message format for the gas market

DISCLAIMER ON RESPONSIBILITY AND LIABILITY

THIS SYSTEM IS PROVIDED "AS IS" WITH NO WARRANTIES WHATSOEVER, EXPRESS OR IMPLIED, INCLUDING ANY WARRANTY OF MERCHANTABILITY, NONINFRINGEMENT, FITNESS FOR PARTICULAR PURPOSE, ACCURACY OR COMPLETENESS, OR ANY WARRANTY OTHERWISE ARISING OUT OF THIS DOCUMENT.

MIDRAN LTD, ENTSG and EASEE-GAS disclaim all liability for any damages arising from any use or misuse of this service, whether special, indirect, consequential, or compensatory damages, and including liability for infringement of any intellectual property rights, relating to use of information in or reliance upon this service.

The service provider makes no commitment to update the information contained herein and retains the right to make changes to this system and its validation artefacts at any time, without notice.

By logging in the user agrees to these terms.

Full disclaimer in 'more details'

[More Info](#)

Sign In

☐ Remember Me [Forgot Password](#)

[Log in](#)

[Don't have a login?](#) [Create account](#)

Simple user interface

1. Select the guideline and upload message

Validation

1) First select type of validation

Show all validations

2) Then enter the test file for validation

Entsog demo

EDIGAS Nomination Document 6.1

PEPPOL BIS Billing (UBL Invoice) v 3

PEPPOL BIS Billing (UBL CreditNote) v 3

Peppol Shared PINT invoice rules

Drag and drop a file here

If you prefer you can also [Browse...](#)

2. Creates a report validated against a schematron file and shows the error with an error message.

Report

View as PDF

Filename: Example NOMINT 01G - Borderpoints_003.xml
Date: 2024-10-24 12:48:32

Document Types

Description	Matched	Info	Warning	Fatal
XML Structural Validation	Yes	0	0	0
XSD schema Entsog test	Yes	0	0	0
Entsog schematron	Yes	0	0	3

Hide Warnings

XML Structural Validation

XSD schema Entsog test

Entsog schematron

Flag	Rule id	Info	Query	Message	Location (click on path to display in XML)	Full Location
	R-EDIGAS-V61-NOMINT-003			If the document code is 01G the recipient must be a ZSO (found ZSH)	/Nomination_Document[1]	
	R-EDIGAS-V61-NOMINT-010			If the coding scheme is 305, the code value has to be an EIC code value of 16 characters (found "21y1000000001006T" with length 17)	/Nomination_Document[1]/Internal_Account[1]/Conn.../Identification[1]	
	R-EDIGAS-V61-NOMINT-011			If the coding scheme is 305, the code value has to be an EIC Party X code value (found "21y1000000001006T")	/Nomination_Document[1]/Internal_Account[1]/Conn.../Identification[1]	

Back-office stats available to admin to show which rules are broken most.

File: Example NOMINT 01G - Borderpoints_003.xml

Location of error

Location: /Nomination_Document[1]/Internal_Account[1]/ConnectionPoint[1]/Identification[1]

Message: If the coding scheme is 305, the code value has to be an EIC Party X code value (found "21y1000000001006T")

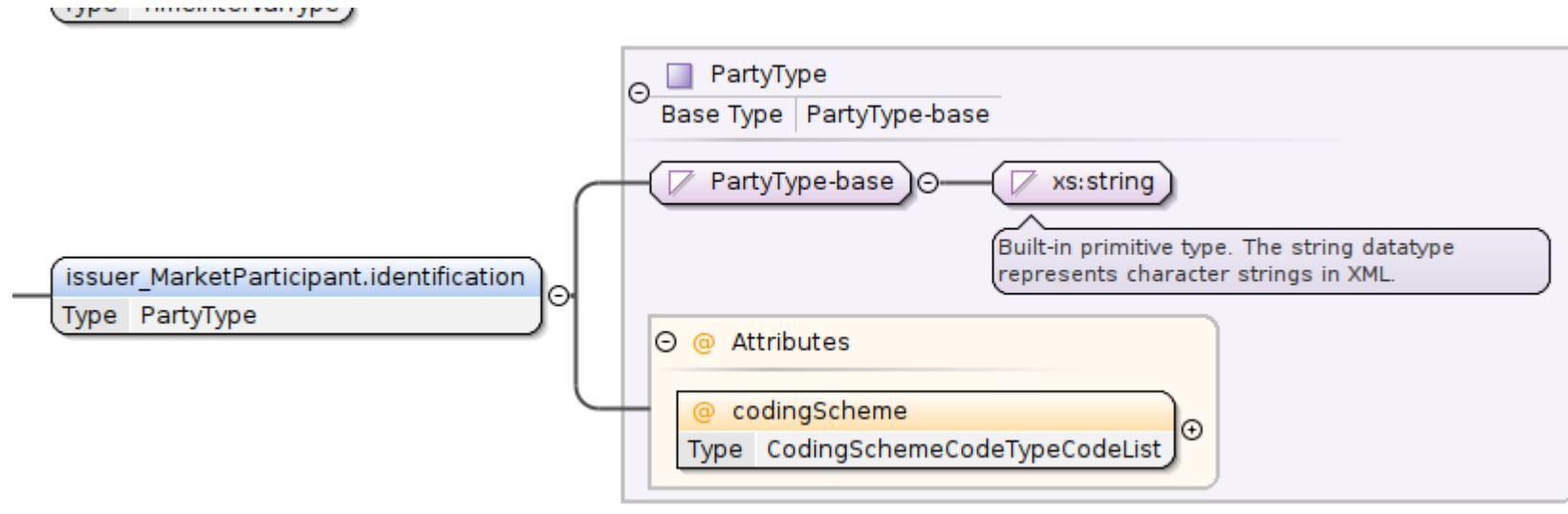
```
<!-- IMPORTANT! All comments in this document are provided for better understanding of the example(-s) provided. None of
<Nomination_Document xmlns="urn:easee-gas.eu:edigas:8rpnominationandmatching:NominationDocument:6:1" schemaVersion="1">
  <identification>NOMINT-01G-border</identification>
  <version>1</version>
  <documentCode>01G</documentCode>
  <creationDateTime>2020-01-12T19:30:47Z</creationDateTime>
  <validityPeriod>2020-01-13T05:00Z/2020-01-14T05:00Z</validityPeriod>
  <issuer_MarketParticipant.identification codingScheme="305">21X000000001006T</issuer_MarketParticipant.identification>
  <issuer_MarketParticipant.marketRole.roleCode>ZSH</issuer_MarketParticipant.marketRole.roleCode>
  <recipient_MarketParticipant.identification codingScheme="305">21X-IT-A-A0A0A-7</recipient_MarketParticipant.identification>
  <recipient_MarketParticipant.marketRole.roleCode>ZSH</recipient_MarketParticipant.marketRole.roleCode>
  <Internal_Account>
    <internalAccount codingScheme="ZSO">ACCOUNT</internalAccount>
    <ConnectionPoint>
      <identification codingScheme="305">21y1000000001006T</identification>
      <manufacturerCode>21</manufacturerCode>
    </ConnectionPoint>
  </Internal_Account>
</Nomination_Document>
```

3. Click link to error position in message

Text here

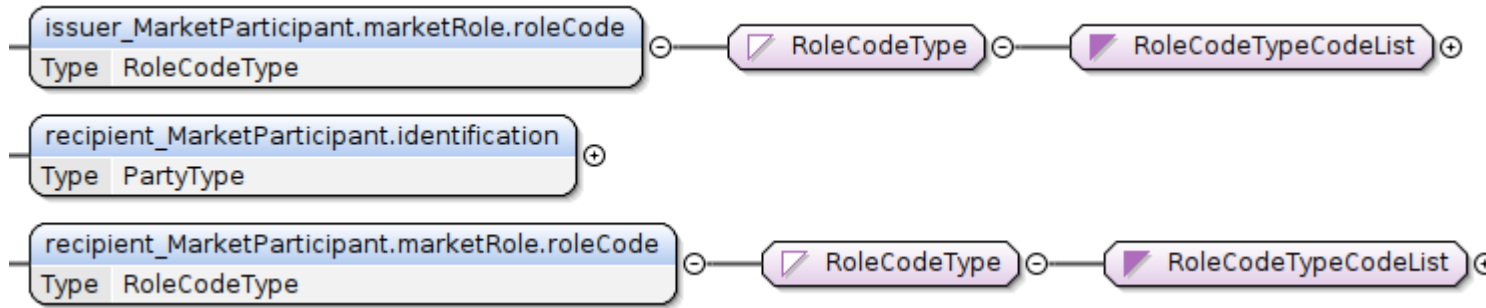
73

Under the hood ...



```
<sch:rule context="/nomint:Nomination_Document/nomint:issuer_MarketParticipant.identification">
  <sch:let name="cs" value="@codingScheme" />
  <sch:let name="code-value" value="text()" />
  <sch:assert id="R-EDIGAS-A16-NOMINT-008A"
    test="$cs='305'">The coding scheme for issuer market participant must be 305; found scheme: <sch:value-of
      select="$cs" />
  </sch:assert>
  <sch:assert
    test="matches(normalize-space($code-value),'^\\d\\dX','i')" id="R-EDIGAS-A16-NOMINT-008B"
    >The code for issuer market participant must be an EIC Party X code; found code: "<sch:value-of
      select="$code-value"/>" </sch:assert>
</sch:rule>
```

Under the hood ...



```

<sch:rule context="/nomint:Nomination_Document/nomint:issuer_MarketParticipant.marketRole.roleCode">
  <sch:let name="ic" value="text()" />
  <sch:let name="dc" value="/nomint:Nomination_Document/nomint:documentCode/text()" />

  <sch:assert id="R-EDIGAS-A16-NOMINT-009A" test="$dc != '01G' or $ic = 'ZSH'"
    >If the document code is 01G (Nomination) the issuer must be a ZSH (Balance responsible party); found <sch:value-of
      select="$ic"/>
  </sch:assert>

  <sch:assert id="R-EDIGAS-A16-NOMINT-009B" test="$dc != '02G' or $ic = 'ZSH'"
    >If the document code is 02G (VTP OTC Nomination) the issuer must be a ZSH (Balance responsible party); found <sch:value-of
      select="$ic"/>
  </sch:assert>

  <sch:assert id="R-EDIGAS-A16-NOMINT-009C" test="$dc != '03G' or $ic = 'ZUM'"
    >If the document code is 03G (VTP exchange nomination) the issuer must be a ZUM (Clearing Responsible); found <sch:value-of
      select="$ic"/>
  </sch:assert>

  <sch:assert id="R-EDIGAS-A16-NOMINT-009D" test="$dc != '04G' or $ic = 'ZSH'"
    >If the document code is 04G (Non matching nomination) the issuer must be a ZSH (Balance responsible party); found <sch:value-of
      select="$ic"/>
  </sch:assert>
</sch:rule>
  
```

Status of support for EASEE-gas in validation portal

Currently Deployed

- NOMINT – Nomination
- NOMRES – Nomination Response
- DELORD – Delivery Order
- DELRES – Delivery Response
- METRED – Management Information Overview
- LIMITS – Limits
- INVENT – Inventory Position
- STOREQ – Storage Action Request
- STOCON – Storage Action Confirmation

Roadmap

- ACKNOW– Acknowledgment
- OFFERS– Gas Purchase or Sale Offers
- REQUEST – Offtake request to seller
- REQRES – Request response
- ...

(Future new Edig@s document types)

Lessons learned

Schematron mapping operationalizes the decision tables

- From documentation for designers to executable validation logic
- Decision tables are an excellent starting point for rule development

Rules reflect and require a deep understanding of the domain logic

- Schematron developer needs to be complemented by an expert with deep Edig@s experience
- Formalizing the rules as Schematron is a good sanity check on the documentation
- The service helps start debate between implementers
- Ideally, for new document types, ENTSOG/EASEE-gas would provide the Schematron with the release
- An exhaustive test set (valid / invalid sample for each document and rule) would help

Lessons learned

There are many common patterns across document types

- Supporting a new document can often reuse logic already defined for previous documents

Overall, Schematron is a good fit for the problem

- There is a direct mapping from decision tree table structure (column, row, cell values) to Schematron assertions
- It is possible to write helpful error messages (XSD errors can be cryptic / deeply technical)

Some logic cannot be captured easily, for example:

- Some rules refer to gas day, which depends on Daylight Saving
- There are XPath functions for date, but not for "Last Sunday of March"

Sharing Schematron rules (Future)

- Schematron rules provide the logic
 - Native
 - Compiled XSLT (as used by the Validex service)
- Potential applications for Schematron outside Validex:
 - Desktop XML development tools (oXygen XML Editor, Altova XMLSpy, etc.), B2B integration middleware
 - Testing including batch regression testing
 - Runtime validation

7. Coffee break: 14:40 - 15:05



8. AS4: ENTSOE AS4 v4.0 from development to deployment



Pim van der Eijk
Sonnenglanz Consulting

ENTSOG AS4: from development to deployment

ENTSOG AS4 v4.0 specification is approved, published and ready to be used, however

To migrate, TSOs also need

- Solution providers to update their solutions to version 4.0
- Certificates of a different type than they use today with 3.6
- A joined-up migration strategy



ENTSOG
AS4 PROFILE
Version 4.0

2025

Solutions for v4.0 and interoperability

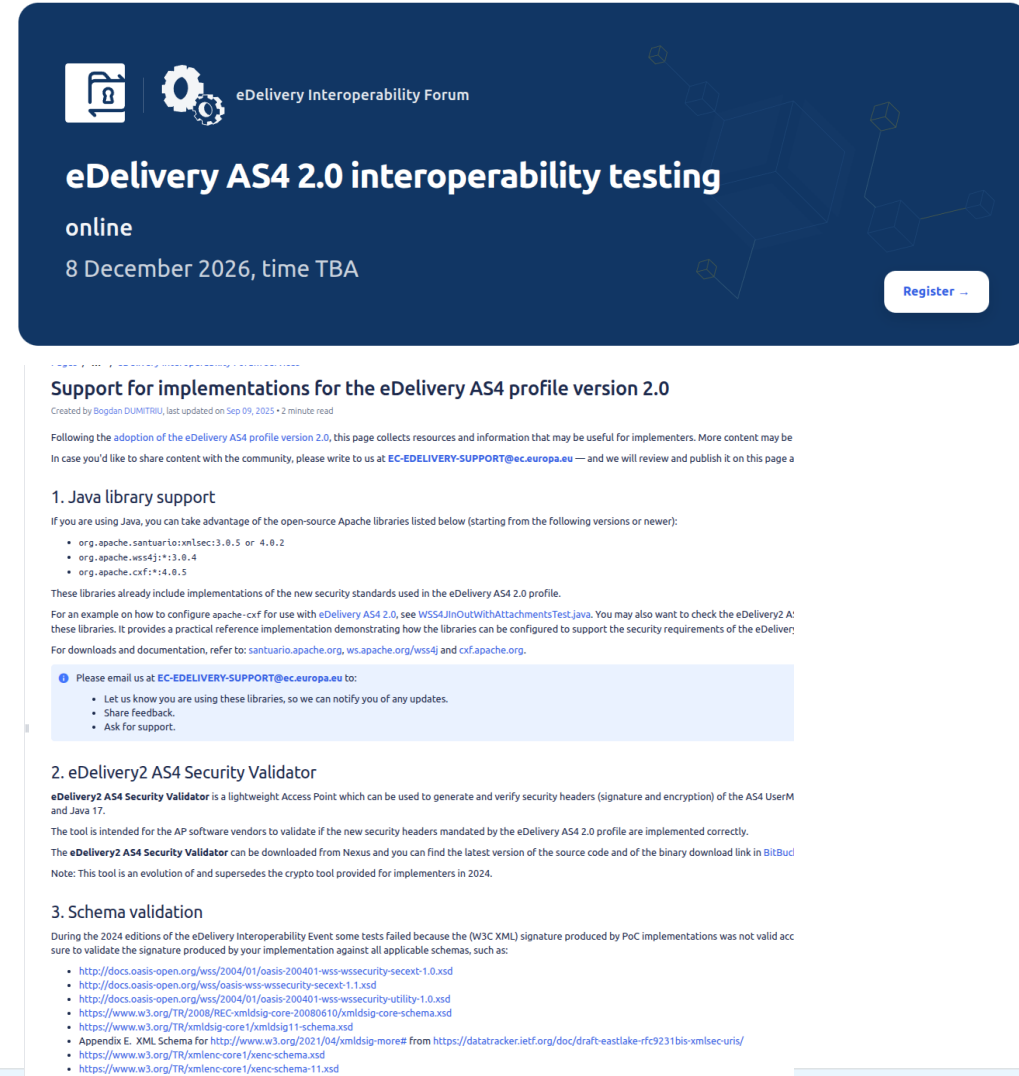
EC is doing another eDelivery interoperability testing event in December 2026

- Registration at <https://ec.europa.eu/digital-building-blocks/sites/spaces/EDELCOMMUNITY/pages/964165805/eDelivery+AS4+2.0+interoperability+testing+8+December+2026>
- Known to be very useful for improving products and their interoperability

ENTSOG has actively promoted this event

- Many service providers active in the gas market have informally confirmed their intention to participate

More information from EC presentation later today



The banner features the eDelivery Interoperability Forum logo and a map of Europe. Below it, the text reads: "eDelivery AS4 2.0 interoperability testing online", "8 December 2026, time TBA", and a "Register" button.

Support for implementations for the eDelivery AS4 profile version 2.0
Created by Bogdan DUMITRU, last updated on Sep 09, 2025 • 2 minute read

Following the adoption of the eDelivery AS4 profile version 2.0, this page collects resources and information that may be useful for implementers. More content may be in case you'd like to share content with the community, please write to us at EC-EDELIVERY-SUPPORT@ec.europa.eu — and we will review and publish it on this page

1. Java library support
If you are using Java, you can take advantage of the open-source Apache libraries listed below (starting from the following versions or newer):

- `org.apache.santuario:xmlsec:3.0.5` or `4.0.2`
- `org.apache.wss4j:*.3.0.4`
- `org.apache.cxf:*.4.0.5`

These libraries already include implementations of the new security standards used in the eDelivery AS4 2.0 profile.

For an example on how to configure apache-cxf for use with eDelivery AS4 2.0, see `WSS4JInOutWithAttachmentsTest.java`. You may also want to check the eDelivery 2 AS4 these libraries. It provides a practical reference implementation demonstrating how the libraries can be configured to support the security requirements of the eDelivery. For downloads and documentation, refer to: santuario.apache.org, ws.apache.org/wss4j and cxf.apache.org.

Please email us at EC-EDELIVERY-SUPPORT@ec.europa.eu to:

- Let us know you are using these libraries, so we can notify you of any updates.
- Share feedback.
- Ask for support.

2. eDelivery2 AS4 Security Validator
eDelivery2 AS4 Security Validator is a lightweight Access Point which can be used to generate and verify security headers (signature and encryption) of the AS4 UserM and Java 17.

The tool is intended for the AP software vendors to validate if the new security headers mandated by the eDelivery AS4 2.0 profile are implemented correctly.

The **eDelivery2 AS4 Security Validator** can be downloaded from Nexus and you can find the latest version of the source code and of the binary download link in [BitBucket](#).

Note: This tool is an evolution of and supersedes the crypto tool provided for implementers in 2024.

3. Schema validation
During the 2024 editions of the eDelivery Interoperability Event some tests failed because the (W3C XML) signature produced by PoC implementations was not valid according to the signature produced by your implementation against all applicable schemas, such as:

- <http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurity-secext-1.0.xsd>
- <http://docs.oasis-open.org/wss/oasis-wss-wssecurity-secext-1.1.xsd>
- <http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurity-utility-1.0.xsd>
- <https://www.w3.org/TR/2008/REC-xmlsig-core-20080610/xmlsig-core-schema.xsd>
- <https://www.w3.org/TR/xmlsig-core1/xmlsig11-schema.xsd>
- Appendix E. XML Schema for <http://www.w3.org/2021/04/xmlsig-more#> from <https://dataretriever.ietf.org/doc/draft-eastlake-ietf-c9231bis-xmlsec-uris/>
- <https://www.w3.org/TR/xmlenc-core1/xenc-schema.xsd>
- <https://www.w3.org/TR/xmlenc-core1/xenc-schema-11.xsd>

ENTSOG 3.6: RSA for signing and encryption

- Owner **signs** using private key, everyone can verify using public key
- Everyone can **encrypt** using public key, only owner can decrypt using private key
- Can be used for two usages.

ENTSOG 4.0 Ed25519 for signing

- Owner **signs** using private key, everyone can verify using public key
- Cannot be used for key agreement

ENTSOG 4.0 X25519 for key agreement

- Everyone can **encrypt** using public key, only owner can decrypt using private key
- Cannot be used for signing

AS4 algorithms now supported in ENISA algorithm catalog



Draft v3.0 of ECCG Agreed Cryptographic Mechanisms - version 3 - draft for public review adds algorithms needed for ENTSG AS4 v4.0

https://certification.enisa.europa.eu/publications/eucc-guidelines-cryptography_en

Agreed Digital Signature Schemes.

Primitive	Scheme	R/A	Notes
RSA	PSS (PKCS#1v2.1) [RFC8017, PKCS1, ISO9796-2]	A	52-QuantumThreat
FF-DLOG	KCDSA [ISO14888-3]	A	50-DSARandom, 52-QuantumThreat
	Schnorr [ISO14888-3]	A	
	DSA [FIPS186-5, ISO14888-3]	A	
EC-DLOG	ECKCDSA [ISO14888-3]	A	50-DSARandom, 52-QuantumThreat
	ECDSA [FIPS186-5, ISO14888-3]	A	
	ECGDSA [TR-03111]	A	
	ECSchnorr [ISO14888-3]	A	
	Deterministic ECDSA [FIPS186-5]	A	
	EdDSA [RFC8032]	A	52-QuantumThreat, 51-DeterministicSignatures
LWE	ML-DSA [FIPS204]	R	53-Hybridization, 58-ML-DSA Parameters
HASH	XMSS [SP800-208]	R	55-OptionalHybridization, 56-StateManagement,
	LMS [SP800-208]	R	57-XMSS-LMS-Parameters
	SLH-DSA [FIPS205]	R	54-SLH-DSAParameters, 55-OptionalHybridization
RSA	PKCS#1v1.5 [RFC8017, PKCS1, ISO9796-2]	A	49-PKCSFormatCheck, 52-QuantumThreat

Agreed Key Establishment and Key Encapsulation Schemes.

Primitive	Scheme	R/A	Notes
FF-DLOG	DH [SP800-56A, ISO11770-3]	A	60-KE-Auth, 61-DHSubgroupAttacks 62-QuantumThreat
	DLIES-KEM [ISO18033-2]	A	
EC-DLOG	EC-DH [SP800-56A, ISO11770-3]	A	60-KE-Auth, 61-DHSubgroupAttacks, 62-QuantumThreat
	ECIES-KEM [ISO18033-2]	A	
	X25519, X448 [RFC7748]	A	60-KE-Auth, 62-QuantumThreat
LWE	ML-KEM [FIPS203]	R	60-KE-Auth, 63-Hybridization, 64-ML-KEM Parameters
	FrodoKEM [FRODO-KEM]	R	60-KE-Auth, 63-Hybridization, 65-FrodoKEM Parameters

General Notes.

Agreed Elliptic Curve Parameters.

Curve Family	Curve	R/A	Notes
Brainpool [RFC5639]	BrainpoolP256r1	A	
	BrainpoolP384r1	A	
	BrainpoolP512r1	A	
NIST [FIPS186-5, Appendix D.1.2]	NIST P-256	A	40-SpecialP
	NIST P-384	A	
	NIST P-521	A	
Edwards curves [RFC7748]	Curve25519	A	40-SpecialP
	Curve448	A	
FR [JORF]	FRP256v1	A	

Text here

EdDSA is enabled in EU electronic signature standards for Certification Authorities

- ETSI TS 119 312 (June 2026)
- https://www.etsi.org/deliver/etsi_ts/119300_119399/119312/02.01.01_60/ts_119312v020101p.pdf

ETSI TS 119 312 V2.1.1 (2026-06)



Electronic Signatures and Trust Infrastructures (ESI);
Cryptographic Suites

6.2.1 General

The list of signature algorithms given in Table 2 shall be used. The algorithms shall be implemented as per the reference listed in Table 2 and shall follow the recommendations provided in the ECCG Agreed Cryptographic Mechanisms [14], where applicable. The present document provides additional recommendations and requirements in the following clauses.

Table 2: Digital Signature Algorithms

Short signature algorithm name	References	R/L
RSA-PKCS#1v1_5	IETF RFC 8017 [3]	L
RSA-PSS	IETF RFC 8017 [3]	R
DSA	FIPS Publication 186-5, ISO/IEC 14888-3 [4]	R
ECDSA	FIPS Publication 186-5 [2]	R
EdDSA	IETF RFC 8032 [23]	R (see note 1)
ML-DSA	NIST FIPS Publication 204 [26]	R
SLH-DSA	NIST FIPS Publication 205 [27]	R
EC-SDSA-opt	ISO/IEC 14888-3 [4]	L
LMS	IETF RFC 8554 [28]	R (conditional, see note 2)
XMSS	IETF RFC 8391 [29]	R (conditional, see note 2)

NOTE 1: EdDSA is not an agreed digital signature scheme under the ECCG Agreed Cryptographic Mechanisms [14]. The "R" status assigned to EdDSA in Table 2 reflects the recommendation of the present document independently of the ECCG ACM.

Certificate and Certificate Signing Request (CSR)

- X509 certificate
 - Data structure holding only public data: public keys and public metadata
 - Issuer signs the certificate; recipient can verify using issuers included public key
 - User can use the subject public key for verification or encryption
- Self-signed certificate
 - Certificate where the issuer and subject are the same
 - Proves the issuer=subject has the private key associated with its public key
- Certificate Signing Request (CSR)
 - Like a self-signed certificate, but is created by user to make a request to an issuing certification authority

```
Certificate:
Data:
  Version: 3 (0x2)
  Serial Number:
    36:c8:af:bb:f4:6f:1c:09:a0:27:92:13:98:74:50:a9:8a:12:d0:91
  Signature Algorithm: sha256WithRSAEncryption
  Issuer: C = DE, O = QuoVadis Trustlink Deutschland GmbH, CN = QuoVadis
  Validity
    Not Before: Oct 31 08:18:41 2023 GMT
    Not After : Oct 31 08:13:00 2026 GMT
  Subject: C = BE, OU = Transporters, OU = EASEE-Gas, O = Fluxys Belgium
  Subject Public Key Info:
    Public Key Algorithm: rsaEncryption
    RSA Public-Key: (2048 bit)
    Modulus:
      Exponent: 65537 (0x10001)
  X509v3 extensions:
    X509v3 Authority Key Identifier:
      keyid:DC:08:90:B2:1E:E6:BB:60:EC:EA:3B:47:B5:46:89:71:EA:73:FC

    Authority Information Access:
      CA Issuers - URI:http://trust.quovadisglobal.com/quovadiseurop
      OCSP - URI:http://ocsp.quovadisglobal.com

    X509v3 Certificate Policies:
      Policy: 1.3.6.1.4.1.8024.1.100
      CPS: http://www.quovadisglobal.com/repository

    X509v3 Extended Key Usage:
      TLS Web Client Authentication, E-mail Protection
    X509v3 CRL Distribution Points:

      Full Name:
        URI:http://crl.quovadisglobal.com/quovadiseuropeadvancedcag2

    X509v3 Subject Key Identifier:
      F5:09:E5:9B:40:CD:2F:48:6C:0E:67:28:ED:F8:6C:48:31:54:EC:F0
    X509v3 Key Usage: critical
      Digital Signature, Non Repudiation, Key Encipherment
  Signature Algorithm: sha256WithRSAEncryption
```

Certification Authority

- Trusted party, validated by audits, certification, following standards and legislation
- Validates the CSR (confirm the requester holds the private key)
- Perform identity verification of the issuer
- Quality checks on certificates (e.g. algorithms, key size used)
- Custom checks (e.g. membership of EASEE-gas)
- Provides revocation service

EdDSA and Certification Authorities

Workflow for EdDSA is the same as for RSA and ECDSA

- Request initiated based on CSR
- Different key type, but otherwise similar validation
- EdDSA is an approved EU signature algorithm, CAs can offer it

Possibility to start without an (intermediary) root for EdDSA

- CA may need new hardware (Hardware Security Module) or software (PKI software) for full EdDSA chain compatibility
- CA can re-use an existing non-EdDSA root (e.g.: ECDSA) with EdDSA leaf certificates

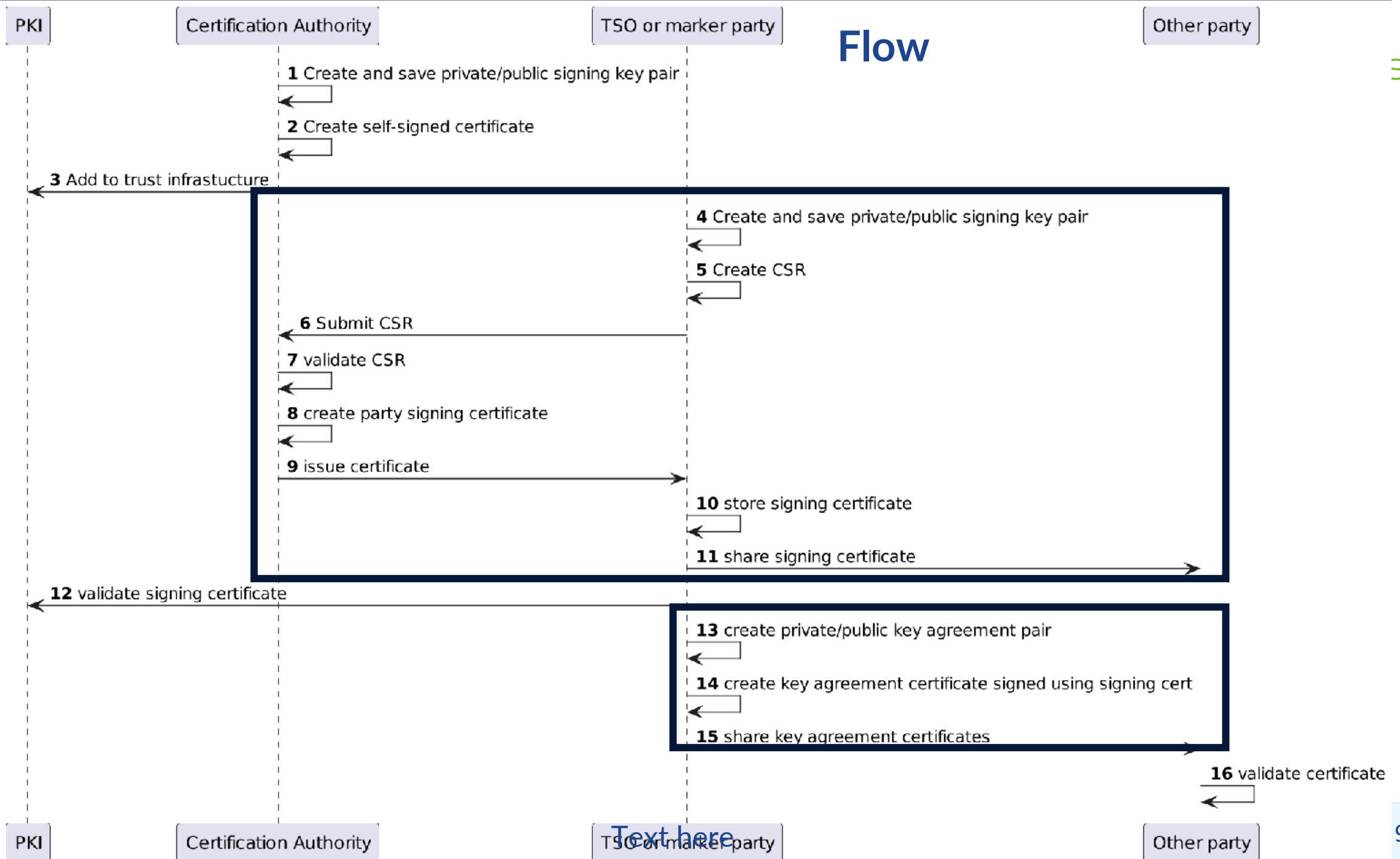
Difference from current workflow

- No option for self-signed certificates or CSR as X25519 is encryption-only
- The public key can be exchanged and ownership proven in other ways, but this is different from the current workflow

Alternative

- Exchange X25519 keys as certificates signed by Ed25519 leaf certificates, not by a CA.
- Avoids the cost and overhead of the CA, compatible with more frequent updates

Flow



Text here

Use signing certificate (+ private key),
as starting point

- Issued by CA

Then generate key agreement
certificates

- Signed using the signing
certificate
- Name etc. fields copied

Share with partners for deployment in
AS4 communication gateway

ITC KG proof-of-concept

- Python PoC script
- Uses a production-grade cryptography
library
<https://cryptography.io/en/latest/> for
asymmetric crypto and X509

OpenSSL command line

- Available and likely widely used
- Command line

AS4 solutions could add value by providing
built-in support, with a professional admin
interface

Obtaining Certificates: Summary

Ed25519 certificate (signature)

- Complies with all relevant legislation (EU Digital Identity) and technical standards (ETSI) for trust services.
- Certification Authorities provide trust
- As it was recently added, Ed25519 is not yet very widely available, but frontrunners have started offering it
- Example: Microsec (HU), <https://www.microsec.hu/en>.

X25519 certificate (key agreement)

- X25519 certificates can be created and exchanged directly between market partners or using EASEE-connect

Future options or alternatives

RFC 9883, An Attribute for Statement of Possession of a Private Key

- Defines an adaptation to CSR process and format, signed using a party's signature key containing key agreement key
- Two stage flow like our proposal, but with CA and not peer-to-peer
- Not yet widely implemented by CAs or in libraries or tooling

RFC 9925, Unsigned X.509 Certificates

- Would allow sharing an X25519 key in a certificate that is not signed; certificate is just a container format
- Misses the benefit of the EdDSA signature

Migrating towards new profile

- Define an approach to migrate TSOs and communication partners
 - Identify approach, dependencies, timelines
- Phased approach
 - Network Code requires AS4, not a specific version
 - "Big bang" migration is both unrealistic and unnecessary
 - Parties to add complementary v4.0 capabilities (software and config upgrade)
 - Migrate existing v3.6 partner connections to v4.0
 - Once all migrated, v3.6 can be phased out
 - Similarly to how AS4 originally replaced AS2

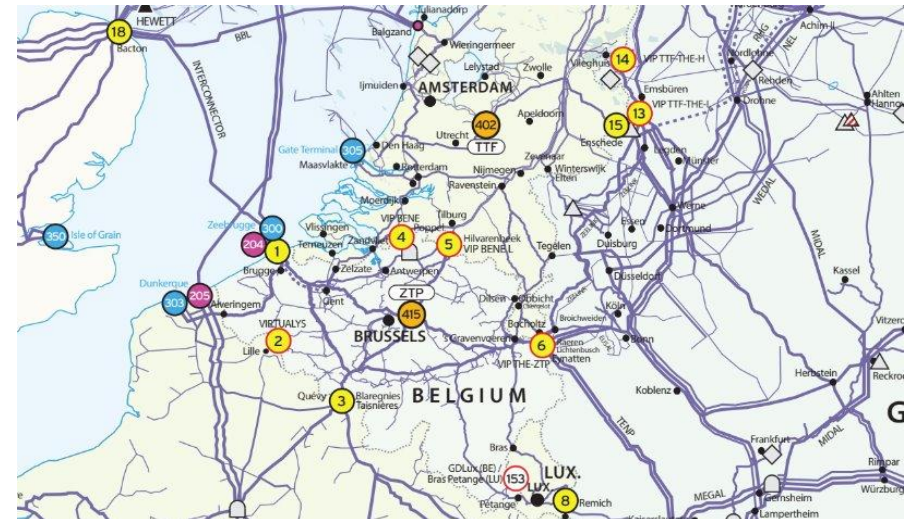
Cluster approach to migration

Cluster-based approach

- Start small: small number of companies (adjacent TSOs and/or key market partners) in a particular region and corresponding gas flows
- Similar levels of readiness, resource availability and agreement to align on them
- Solution providers that support, or are working on, implementing ENTSG AS4v4.0.
- Scale out from there and interconnect

ENTSG, ITC KG to support:

- Answer technical questions; facilitate interop testing; knowledge sharing, liaison to EC eDelivery



AS4 cluster questionnaire



Introduction

Version 4.0 of the ENTSOG AS4 profile specification was published in May 2025. This specification is an evolution of the currently used version 3.6, but introduces more modern security algorithms and security keys that are not compatible with the ones used in v3.6. ENTSOG has already been supporting the migration towards the new profile by working with solution providers, certification authorities, EASEE-gas and the European Commission to help create an ecosystem supporting ENTSOG members and other market parties deploy the new solution.

To further promote and support the migration towards v4.0, **ENTSOG proposes to further coordinate and facilitate the migration**. As there is no fixed legal deadline for migration, the migration will not be a “big bang” migration but rather an iterative process where TSOs deploy v4 on their AS4 communication gateways, then gradually and incrementally switch communication partners from v3.6 to v4.0.

To organize this incremental migration, **ENTSOG proposes to identify logical “migration clusters”**. Members of a cluster are each other’s top communication partners. A migration cluster consists of one or more adjacent TSOs and the key market parties that represent the bulk of their data exchanges. Members in a cluster have a similar implementation readiness and coordinate the deployment. Clusters correspond to natural groupings based on geography, gas flows, technical readiness and business priorities. Identifying clusters makes it easier and more efficient to plan and execute migration.

– [ENTSOG AS4
v4.0 Migration
and Adoption
Questionnaire –
Fill out form](#)

AS4 cluster questionnaire

ENTSOG AS4 v4.0 Migration and Adoption Questionnaire

This questionnaire collects information about your organization's readiness to migrate to ENTSOG AS4 profile version 4.0, solution-provider capabilities, interoperability, counterparties, and certification requirements. The information will help ENTSOG identify and support migration clusters aiming to implement AS4 v4.0 during 2027.

When you submit this form, it will not automatically collect your details like name and email address unless you provide it yourself.

* Required

1. Company name *

2. Name of the contact person for ENTSOG AS4 v4.0 *

https://forms.cloud.microsoft/Pages/ResponsePage.aspx?id=_YQFgflpN0GmocDjMoCxXBpNIDBHxTxAp7WVYdlxgjdUMFNXUDRGWDQwTjRRSVM0R1BCMTFIRUIaWS4u

9. AS4: Migration of Certificates



Dirk Serruys (Fluxys)
Chair TSWG EASEE-gas



Secure continuity. Future-ready interoperability.

MoC2026 success and preparation of EASEE-gas certificates for the ENTSOG AS4 V4 profile

01.

The story in one view



Two linked journeys, managed separately

1 MoC2026

Protect continuity now

Coordinated renewal

- Existing AS4 V3.6-compatible certificates
- One orchestrated go-live on 22 September 2026
- Company-specific switch-over plans
- Central support and hourly reporting

2 AS4 V4 readiness

Modernise security progressively

New certificate model

- Separate signing and key-agreement credentials
- Ed25519 for signatures and X25519 for key agreement
- CA, profile, tooling and interoperability preparation
- Phased adoption rather than another big bang

Continuity was protected without delaying the next security step



MoC 2026

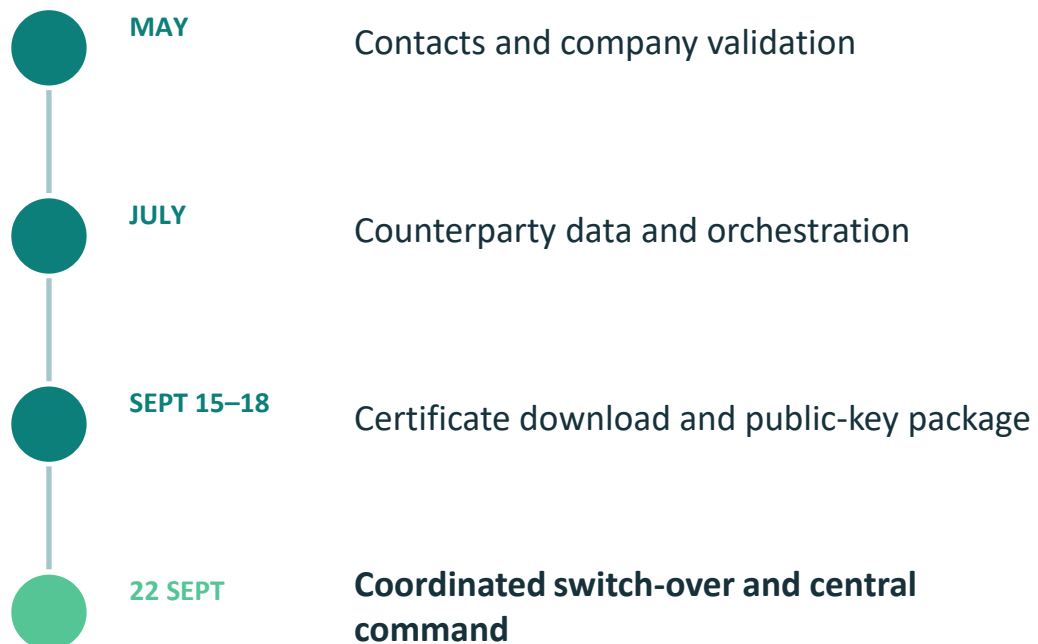
Migration of Certificates 2026

02.

MoC2026



MoC2026: coordinated execution delivered continuity



GO-LIVE COMPLETE

Success was engineered through preparation, sequencing and shared operational discipline.



Continuity protected

The market moved to renewed credentials through a controlled schedule, without mixing the migration with the V4 technology change.

A repeatable operating model

Central coordination, individual switch-over plans, public-key packaging and defined escalation channels reduced ambiguity.

Issues contained and resolved

Operational exceptions were handled through the central command structure and bilateral technical follow-up.

Trust preserved

Certificates remain valid for three years and continue to support current AS4 V3.6 communication.



AS4 V4 readiness

EDDSA Certificates in support of the new AS4 V4 profile

03.

AS4 V4 Readiness



From one certificate to two cryptographic roles

V4 separates message signing from key agreement. That improves cryptographic agility, but changes certificate issuance, platform configuration and operational lifecycle management.

The preparation challenge is not only technical. It spans policy, CA capability, product support, trust distribution and migration governance.

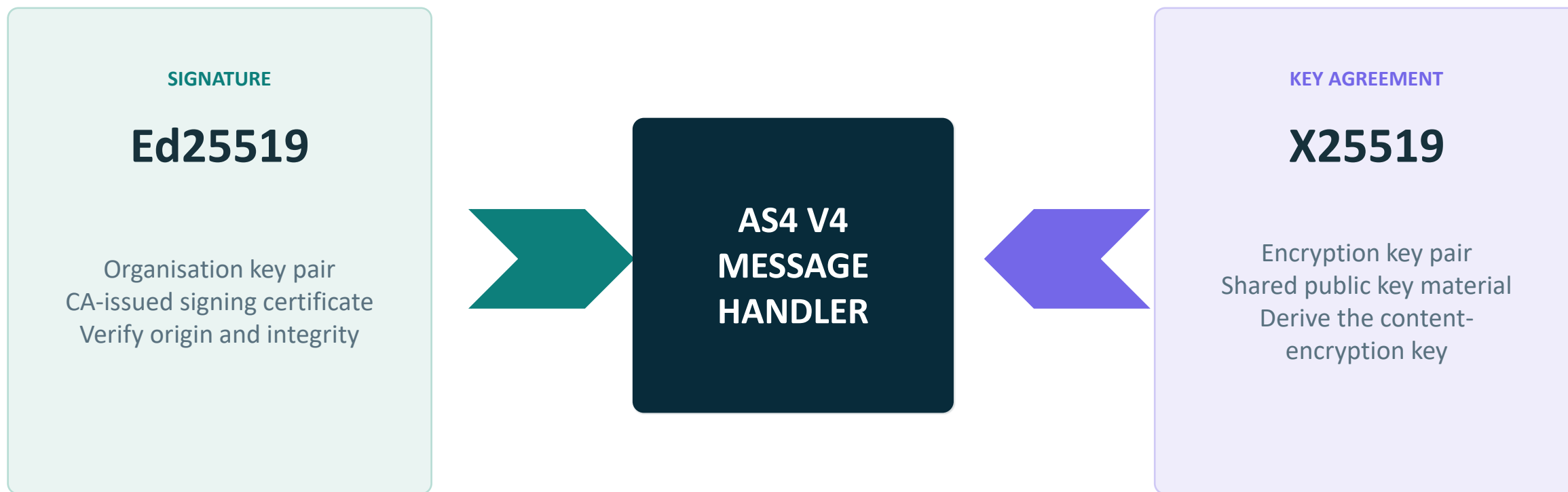


03.

AS4 V4 Readiness



Target certificate model for AS4 V4



Open design point: CA-issued X25519 certificate versus securely shared, signing-certificate-backed key material

03.

AS4 V4 Readiness



Readiness is a six-workstream programme

1

Certificate profile

Subject naming, EIC representation, key usage, extensions and validity.

2

CA capability

Ed25519 issuance, trust chain, validation and operational support.

3

X25519 lifecycle

Generation, storage, distribution, rotation and revocation model.

4

AS4 products

V4 support, dual profiles, UI/configuration and HSM compatibility.

5

Interoperability

Peer pilots, EC testing, negative tests and operational runbooks.

6

Migration governance

Coalitions of willing, partner sequencing, support and communication.

Principle: prove the ecosystem first, then scale adoption partner by partner

03.

AS4 V4 Readiness



Next moves

NOW

Freeze the certificate profile

Confirm Ed25519 subject fields, usages, extensions and certificate validity policy.

NEXT

Select and prove issuance models

Complete CA proof of concept and decide the X25519 trust/distribution model.

PILOT

Test the complete chain

Validate at AS4 product, HSM, EASEE-connect, peer and EC interoperability levels.

SCALE

Migrate in clusters

Start with willing counterparties and mature solutions; retain controlled V3.6 coexistence.



THANK YOU

Feel free to ask any questions!



Website
easee-gas.eu/

10. EASEE-connect updates



Jean-Francois van Snick (Fluxys)
GSConnect Analyst
EASEE-gas TSWG

What is Easee-Connect?

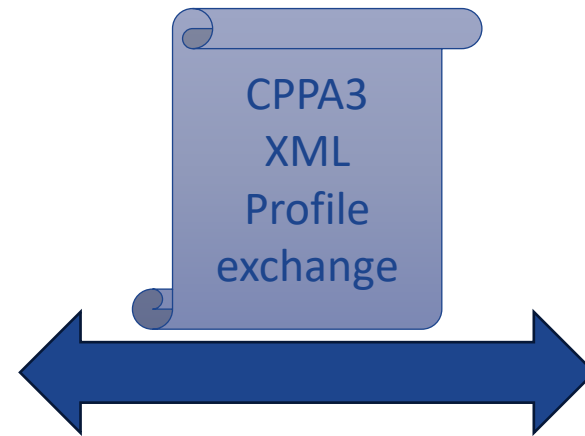


Easee-Connect is an online platform for operators and stakeholders in the gas industry.

It allows the secure storage and exchange of AS2 and AS4 connection parameters.

Facilitates communication and electronic data exchange between business partners in the gas industry.

Easee-Connect Features



Your Communication Tool



Why Use Easee-Connect?



- ⌘ Simplifies the management of electronic exchanges in the gas industry.
- ⌘ Ensures compliance with security and communication standards (AS2/AS4), including new ENTSOG profiles management.
- ⌘ Reduces the risk of errors during connection parameter configuration.
- ⌘ Improves communication between operators, minimizing service interruptions.
- ⌘ Facilitator in the Certificate Renewal Processes

Platform Evolution



EASEE-connect

New features in development, including integration of additional communication protocols and new certificates algorithms.

Ongoing improvements in platform security and efficiency.

Increased interoperability with other data management systems in the gas industry.

Open-minded system to your suggestions for future evolutions.



11. AS4: eDelivery AS4 v2.0 updates



Bogdan Dumitriu
EC eDelivery
Directorate-General for
Informatics (DIGIT)

eDelivery 2.0 Latest Updates

Bogdan Dumitriu
DIGIT, European Commission

14 October 2026
6th Joint Data Exchange and Cybersecurity workshop



EDELIVERY SPECIFICATIONS – NEXT GENERATION

The eDelivery 2.0 specifications were published on 5 December 2024, with eDelivery SMP 2.1 updated on 1 December 2025.

eDelivery AS4 Profile 2.0 Modern cryptography (elliptic curve cryptography based on EdDSA or ECDSA) More flexible Dynamic Discovery (search by C3 PartyId) Support for ebCore Agreement Update	eDelivery SMP Profile 2.1 Upgrade to the latest OASIS SMP 2.0 standard (multiple certificates) Compatible with eDelivery AS4 v2.0 SMP access control feature – eDelivery SMP 2.1	eDelivery BDXL Profile 2.0 Support for publication of SMP 2.0 URLs	eDelivery ebCore Party Id Profile 2.0 Clarified use Aligned with updates to other eDelivery specifications
--	--	---	---

eDELIVERY 2025 INTEROPERABILITY EVENT

What?

Online sessions to test connectivity between implementations of eDelivery AS4 2.0 specifications.

Timing: December 2025 – January 2026

Participants: EC + four companies

Results: by the end, all tests successful

Interoperability issue #1

Different implementations used different X.509 certificate reference mechanisms (Subject Key Identifier, Binary Security Token, Issuer and Serial Number).

Recommendation: Implement all three options for referencing a security token.



scan me

<https://ec.europa.eu/digital-building-blocks/sites/spaces/EDELCOMMUNITY/pages/952470251/eDelivery+AS4+2.0+security+interoperability+testing+2025+-+post-event+report>

eDELIVERY 2025 INTEROPERABILITY EVENT

What?

Online sessions to test connectivity between implementations of eDelivery AS4 2.0 specifications.

Timing: December 2025 – January 2026

Participants: EC + four companies

Results: by the end, all tests successful

Interoperability issue #2

Some messages included an EncryptedKey element even when no payload encryption was performed.

Recommendation: *Sending* implementations should not include unused security tokens; *receiving* implementations should ignore unused tokens for robustness.



scan me

<https://ec.europa.eu/digital-building-blocks/sites/spaces/EDELCOMMUNITY/pages/952470251/eDelivery+AS4+2.0+security+interoperability+testing+2025+-+post-event+report>

eDELIVERY 2025 INTEROPERABILITY EVENT

What?

Online sessions to test connectivity between implementations of eDelivery AS4 2.0 specifications.

Timing: December 2025 – January 2026

Participants: EC + four companies

Results: by the end, all tests successful

Interoperability issue #3

Some implementations signed the Signal Message in response to a User Message with a different algorithm.

Recommendation: Consider hybrid use of cryptography between sender and recipient – sender should not automatically assume that recipient will respond with same cryptography



scan me

<https://ec.europa.eu/digital-building-blocks/sites/spaces/EDELCOMMUNITY/pages/952470251/eDelivery+AS4+2.0+security+interoperability+testing+2025+-+post-event+report>

eDELIVERY 2026 INTEROPERABILITY EVENT

What?

Online sessions to test connectivity between implementations of eDelivery AS4 2.0 specifications.

Timing: 8 December 2026

Participants: over 10 companies/products already signed up



scan me

STANDARDS ALIGNMENT / MARKET SUPPORT

Purpose

Support market availability of EdDSA certificates.
For the EU market, CAs follow ETSI TS 119 312.

ETSI TS 119 312

Following a change request from eDelivery, [ETSI TS 119 312 V2.1.1 \(2026-06\)](#): *Cryptographic Suites* includes the electronic signature algorithm introduced in eDelivery AS4 2.0 (EdDSA).

ETSI TS 119 522

A new version of [Draft ETSI EN 319 522-4-1 \(2026-06\)](#): *Message delivery bindings* aligns the ETSI AS4 profile to the eDelivery AS4 2.0 profile (ECDSA only).

ECCG Agreed Cryptographic Mechanisms

Following a change request from eDelivery, the [Draft ECCG Agreed Cryptographic Mechanisms version 3](#) includes the cryptographic algorithms introduced in eDelivery AS4 2.0 (EdDSA & X25519).

HOW CAN ENTSGO LEVERAGE EDELIVERY FURTHER?

Services, tools and events

eDelivery Interoperability Forum

A platform to support the collaboration between the eDelivery Building Block and providers of **eDelivery-conformant solutions**.

Membership based, Peppol members welcome!

Learn more:
<https://ec.europa.eu/digital-building-blocks/sites/x/-AR7Jg>

eDelivery Interoperability Event

Online sessions to **test connectivity** between implementations of eDelivery AS4 2.0 specifications.

We are open for joint events!

Learn more:
<https://ec.europa.eu/digital-building-blocks/sites/x/UoPFO>

AS4 2.0 Security Header Validation Tool

A tool to generate and **verify the security headers** (signature and encryption) used in AS4 messages.

Learn more:
<https://ec.europa.eu/digital-building-blocks/code/projects/EDELIVERY/repos/edelivery2-as4-security-validator>

eDelivery Conformance Testing

The service offered by the eDelivery Building Block for providers of eDelivery-conformant solutions to **demonstrate conformance**.

Testing of eDelivery AS4 2.0 available by November!

Learn more:
<https://ec.europa.eu/digital-building-blocks/sites/x/CKrXGw>

EDELIVERY CONFORMANCE TESTING

2026-06
Strengthened testing of eDelivery common profile (used by ENTSOG) with 32 new test cases

2026-11
Support for eDelivery AS4 2.0 expected in early November 2026



<https://ec.europa.eu/digital-building-blocks/sites/x/CKrXGw>

Product	Testing	Conformance	Reports	Actions
CData Arc	Tested on 13 Nov 2025 Conformant since 13 Jan 2017	eDelivery AS4 2025 09 1.15 4C SB DR DS PF EG	Download report Previous versions	
IP Works EDI 2024	Tested on 13 Nov 2025 Conformant since 16 Aug 2024	eDelivery AS4 2025 09 1.15 4C SB DR DS PF EG	Download report Previous versions	
Descartes	Tested on 15 Sep 2022 Conformant since 15 Sep 2022	eDelivery AS4 2023 06 1.15 4C SB DR DS PF EG	Download report Previous versions	
Domibus 5.1.x (EC sample implementation)	Tested on 4 Jun 2025 Conformant since 17 Jul 2019	eDelivery AS4 2023 06 1.15 4C SB DR DS PF EG	Download report Previous versions	

DOMIBUS 5.2 / 6.0

Domibus 5.2 supports REST API-based integration

Domibus 6.0 will support eDelivery 2.0

- EdDSA & ECDSA
- HSM (tested with simulators only)
- ... and several new features unrelated to eDelivery 2.0

Timeline

Domibus 6.0 expected in Q2 2027



<https://ec.europa.eu/digital-building-blocks/sites/spaces/DIGITAL/pages/467110244/Domibus>

Email us:

EC-EDELIVERY@ec.europa.eu
EC-EDELIVERY-SUPPORT@ec.europa.eu



© European Union 2026

Reuse of this presentation authorised under the CC BY 4.0 license.

12. Round-up, Questions & Answers



Douglas Walker Hill
Interoperability & Data Exchange
ENTSOE

Round up

– Take-ways:

- We have put in place an Edi@s XML validation tool free to use
- Schematron validation artefacts, increase adherence to the guidelines
- EASEE-gas AS4 MoC in planning
- ENTSOG AS4 v4 is a non-backward compatible change – increased ebSecurity core features
- You should go way with a conceptual understanding of AS4 v4 PKI and schematron/XSLT validation artefacts
- DE session slides will be made available on the WKSP event page
- Tomorrow's Cybersecurity session will start at 09:30

Tomorrow's session: Cybersecurity 09:30-13:00



CYBERSECURITY DAY 2

Resilience of Europe's
Gas Sector

15 OCTOBER 2026

BRUSSELS, BELGIUM



PROGRAMME – DAY 2

15 OCTOBER 2026 | BRUSSELS, BELGIUM

TIME	SESSION	PRESENTER	AFFILIATION
09:30	Welcome	Dr. Andrea Chittaro	SNAM (Task force Chair)
09:35	Agenda	Douglas Hill	ENTSOG
09:40	Cybersecurity situational update – energy sector	Sofia Signori	ENISA
10:00	Stress tests in the gas sector	Ricardo de Sousa Figueiredo	ENISA
10:20	Smart energy expert group updates & a review of the study on cybersecurity in gas	Felipe Castro	DG ENER
10:45	2026 edition NIS2 360 review	Jurgita Skritaite	ENISA
11:05	Break	–	ALL
11:30	TSO cyber readiness review – a TSO perspective	Fabrizio Zucca	SNAM
11:50	CSA2 updates	Matus Baliak	DG CNECT
12:10	Cybersecurity ISAC updates	Aurelio Blanquet	EE-ISAC
12:30	Positioning Physical and Cybersecurity in the gas sector	Brigadier General (Ret.) Ioannis Chatzialexandris	EDA
12:50	Wrap up, Next steps in Cybersecurity, Q&A	Douglas Hill	ENTSOG



Thank you for your attention
Tomorrow's cybersecurity session starts at 09:30 hrs

Douglas Walker Hill,
Interoperability & Data Exchange Adviser
douglas.hill@entsog.eu

ENTSOG - European Network of Transmission System Operators for Gas
Avenue de Cortenbergh 100, 1000 Bruxelles
www.entsog.eu | info@entsog.eu

