ENTSOG AS4 Frequently Asked Questions

Version 0.2 – 2025-05-22

Disclaimer

THIS DOCUMENT ONLY PROVIDES SPECIFIC TECHNICAL INFORMATION GIVEN FOR INDICATIVE PURPOSES AND, AS SUCH, IT CAN BE SUBJECT TO FURTHER MODIFICATIONS. THE INFORMATION CONTAINED IN THE DOCUMENT IS NON-EXHAUSTIVE AS WELL AS NON-CONTRACTUAL IN NATURE AND CLOSELY CONNECTED WITH THE COMPLETION OF THE APPLICABLE PROCESS FORESEEN BY THE RELEVANT PROVISIONS OF COMMISSION REGULATION (EU) 2015/703 OF 30 APRIL 2015 ESTABLISHING A NETWORK CODE ON INTEROPERABILITY AND DATA EXCHANGE RULES.

NO WARRANTY IS GIVEN BY ENTSOG IN RESPECT OF ANY INFORMATION SO PROVIDED, INCLUDING ITS FURTHER MODIFICATIONS. ENTSOG SHALL NOT BE LIABLE FOR ANY COSTS, DAMAGES AND/OR OTHER LOSSES THAT ARE SUFFERED OR INCURRED BY ANY THIRD PARTY IN CONSEQUENCE OF ANY USE OF -OR RELIANCE ON- THE INFORMATION HEREBY PROVIDED.

Table of contents

1 ENTSOG AS4

1.1 What is AS4?

AS4 is a B2B communication protocol standard. It was designed to meet the functional requirements of B2B electronic business and provides advanced security and reliability features. AS4 was originally developed by the OASIS standards organization and is an international standard, ISO 15000-2. AS4 is a subset of another OASIS standard called ebMS3. Like AS4, ebMS3 is also part of the ISO family as 15000-1.

1.2 What is ENTSOG AS4?

AS4 is a configurable standard that is typically profiled for use in specific contexts in a so-called 'Usage Profile'. ENTSOG AS4 is such a Usage Profile designed for use by TSOs and the broader gas market which addresses the gas market's specific requirements. ENTSOG AS4 defines which features of AS4 are to be used and provides a precise specification on how to use those features. It ensures that the use of AS4 is secure and facilitates interoperability between different implementations.

1.3 Why does ENTSOG use AS4?

The Interoperability Network Code and the data exchange rules published on 30 April 2015 by the European Commission (EC) define three types of data exchange. AS4 is mandated in the regulation as the prescribed data exchange standard for one of the three, namely document-based data exchange.

1.4 What is the relationship between ENTSOG AS4 and Edig@s XML?

ENTSOG AS4 defines how the AS4 standard is to be used and specifies the content of the AS4 message header. AS4 messages can contain payloads of any type. An ENTSOG AS4 message can be used to transport Edig@s XML payloads. For document-based data exchange, the use of Edig@s XML is also mandated in the Interoperability Network Code (Article 21).

2 ENTSOG AS4 v4.0

2.1 What versions of ENTSOG AS4 exist?

The current production version of ENTSOG AS4 is v3.6, which was published in May 2019. The latest version of ENTSOG AS4 v4.0 was published on the 5th May 2025 (here) on the ENTSOG website and is intended to replace v3.6. by 2027.

2.2 Why did ENTSOG create a new AS4 v4.0?

ENTSOG AS4 v3.6 still meets all functional requirements. However, the security profiling of ENTSOG AS4 v3.6 is no longer state-of the-art. v4.0 updates the security section of the profile in accordance with current security best practices. The update of the profile to v4.0 provides continued security for users of ENTSOG AS4 for the coming years. It also provides investment protection, as only the AS4 gateway components are affected, not the interfaces to backend systems.

2.3 Does ENTSOG AS4 v4.0 mean that v3.6 is no longer secure?

No, ENTSOG AS4 v3.6 is still secure. However, it is no longer state-of-the-art and it may not be sufficiently secure for future use. Users of ENTSOG AS4 should start planning their migration to v4.0 in order to maintain security.

2.4 What are the differences between v3.6 and v4.0?

The substantive changes in version v4.0 relate to sections:

- 2.2.3.3, compression is ’Recommended’ instead of ‘Mandatory’ and gateways should store messages to handle non-repudiation disputes.
- 2.2.6.1, the TLS specification has been updated to reflect the state-of-the-art in transport layer security (versions, cipher suites).
- 2.2.6.2, WS-Security using XML signature: Switch to using EdDSA instead of RSA.
- 2.2.6.3, WS-Security using XML Encryption: Encryption now uses X25519 instead of RSA.
- 2.2.6.5, alternative Elliptic Curve option using ECDSA.
- 2.3.4.4, guidelines on Certification Authorities.
- 2.3.4.5, removed the details of (non-mandatory) EASEE-gas certificate profile.
- 2.4.3, some optional extensions added to ebCore Agreement Update.

ENTSOG has published a comparison document that shows the changes between v3.6 and v4.0. In practice, the main impact on applications are the changes to WS-Security and certificates used.

2.5 What is the current status of v4.0?

Version 4.0 has been published on the ENTSOG website since the 5th May 2025. The profile can be found (here).

2.6 What version of Edig@s XML can I use with ENTSOG AS4?

You can use v3.6 or v4.0 of ENTSOG AS4 with any version of Edig@s XML, including but not limited to Edig@s version 6.1.

3 Relation to eDelivery AS4

3.1 What is eDelivery and how does ENTSOG AS4 relate to eDelivery AS4?

The European Commission maintains several Digital Building Blocks. One of them is eDelivery which provides technical specifications based on open standards, installable software and ancillary services to allow projects to create a network of nodes for secure digital data exchange. By building with eDelivery, public and private organisations from different sectors can easily create a safe and interoperable channel to transfer documents and data among each other over a public or private network. One of the open standards used in eDelivery is AS4. Like ENTSOG, the Commission provides a usage profile for AS4, called eDelivery AS4.

3.2 What versions of eDelivery exist and how do they relate to ENTSOG AS4?

The current deployed version of eDelivery AS4 is eDelivery AS4 1.15, which has been superseded by a new version 2.0. (Published in Dec 2024). The 1.15 version is closely aligned to ENTSOG AS4 in its 'Common Profile' which uses the same profiling as ENTSOG's AS4 profile for security, reliability and compression, however, it does not support Agreement Update. It is compatible with the gas domain profiling (use of Edig@s, profiling of ebMS header).

In addition to its Common Profile, eDelivery has several optional 'Profile Enhancements'. In eDelivery AS4 v2.0, ebCore Agreement Update, which was already included in ENTSOG AS4 v3.6 and is also in v4.0, was added to eDelivery.

Like ENTSOG AS4, eDelivery AS4 has been updated to align with advances in the state-of-the-art in security. eDelivery AS4 v2.0 fully aligns with ENTSOG AS4 v4.0. It also adds the ebCore Agreement Update as an optional Profile Enhancement.

Finally, ENTSOG AS4 adds some domain-specific profiling in the use of values for message headers, which are compatible with eDelivery AS4 but are not covered by eDelivery AS4 as it is a domain neutral profile.

3.3 Why is it beneficial for ENTSOG AS4 to be aligned with eDelivery AS4?

ENTSOG has benefited from the expertise available in the eDelivery community. The teams responsible for AS4 in ENTSOG and in the Commission have been in close touch and have aimed to align and collaborate on the evolution of their specifications. As a result of this collaboration, the domain-independent profiling of ENTSOG AS4 v4.0 is the same as eDelivery AS4 v2.0. Users of ENTSOG AS4 have access to the network of competing solution providers offering services and solutions for eDelivery AS4.

4 Security related questions for ENTSOG AS4 v4.0

4.1 What is EdDSA and how is it used in v4.0?

In v3.6, ENTSOG AS4 uses RSA-based security for message signature. In the v4.0, a different algorithm is used called Ed25519, one of the EdDSA algorithms. Ed25519 is a modern, secure and widely used algorithm. EdDSA algorithms are also asymmetric algorithms, like RSA. Instead of RSA public/private key pairs, EdDSA requires a different kind of public/private key pairs.

4.2 Why was EdDSA selected as the preferred signature algorithm in ENTSOG AS4?

EdDSA was recommended as the algorithm to use as the replacement for RSA by independent cryptographic experts. It is supported in all modern security toolkits and programming languages. Several, but not yet all, Certification Authorities support EdDSA based certificates. It is expected that support for EdDSA will become more widespread in the coming years.

4.3 What is key agreement? Why did you select X25519?

In v3.6, ENTSOG AS4 uses RSA-based security for message encryption. In the v4.0, a different algorithm is used called X25519 which is a modern, best practice key agreement algorithm. The agreed keys established using X25519 are used to encrypt the message payload parts. X25519 is a modern, secure and widely used algorithm. EdDSA is also an asymmetric algorithm. Instead of RSA public/private key pairs, EdDSA requires a different kind of public/private key pair.

4.4 In ENTSOG AS4, why do I need to use different keys for signing and encryption?

The public/private Ed25519 key pair can only be used for signature. The public/private X25519 key pair can only be used for key agreement. Therefore, communication partners need to exchange two public keys rather than just one.

4.5 Why did you add an alternative Elliptic Curve Cryptography option?

In addition to the updated profiling based on Ed25519/X25519, the v4.0 specification supports an alternative Elliptic Curve Cryptography option. This option is also used on signing and encryption using key agreement but uses ECDSA instead. The reason is that as of 2025, there is less support for EdDSA (and X25519) than for ECDSA amongst Certification Authorities. In certain situations where this is a blocker for implementers, ECDSA may be used as fallback.

4.6 Why does your Elliptic Curve Cryptography option allow ECC curves other than Brainpool?

The BDEW AS4 profile also uses ECDSA, like the alternative ECC option in ENTSOG AS4. However, in BDEW AS4 it is limited to specific curves, called Brainpool. This limitation is not followed in ENTSOG AS4. The reason is that other curves, in particular NIST curves, are more widely used and easier to implement than Brainpool. BDEW AS4 uses Brainpool due to a requirement to support a legacy PKI. This requirement does not apply in other countries and would therefore be too limitative for ENTSOG AS4.

4.7 Can I use my existing ENTSOG AS4 3.6 certificate with ENTSOG v4.0?

No, your current certificate will be an RSA certificate. ENTSOG AS4 v4.0 requires different, incompatible (to RSA) types of keys (Ed25519 and X25519 or, in the alternative ECC option, ECDSA).

5 Migration

5.1 Is there a particular date by which we must implement ENTSOG AS4 4.0?

There is no specific implementation date for implementation of ENTSOG AS4 v4.0. As RSA is no longer state-of-the-art, ENTSOG recommends that the new profile should be implemented by the end of 2027.

5.2 Some of our partners want to adopt ENTSOG AS4 4.0 but others are not ready. Can we run both 3.6 and 4.0 in parallel?

Just as today, for v3.6, AS4 products already allow you to configure certificates and URLs for different communication partners, they should support dual-protocol support in their product and allow you to use one or the other depending on configuration. Implementations may differ in the details for how this is done (for example, whether or not a single URL can be used for v3.6 and v4.0 exchanges). It is also similar to how (in the past when AS4 was first introduced) AS2 and AS4 were used in parallel. There is no need to postpone implementation of v4.0 until all parties are v4.0 capable.

5.3 Does ENTSOG AS4 require us to use Edig@s 6.1? Our company still uses Edig@s 5 with some of our partners.

ENTSOG AS4 v4.0 can be used with all three of the versions 4, 5 and 6.1 of Edig@s.

5.4 Our company is becoming active in new gases. Can we use ENTSOG AS4 v4.0 for these applications?

The legal mandate for ENTSOG AS4 v4.0 is linked to the natural gas networks. In practice, the profile could be used without any modification for any exchange between parties identified using EIC codes supported by Edig@s.

5.5 We implemented BDEW AS4. Does that mean we are ENTSOG AS4 v4.0 compliant?

No, there are several differences including the use of different algorithms and different key types for signing and key agreement. The alternative ECC option is closer to BDEW AS4, however, it is less restricted in supported curves and certification authorities and uses a different key derivation algorithm. Nevertheless, a product that today already supports BDEW AS4 would not require many changes to support ENTSOG AS4.

5.6 Are the certificates for ENTSOG AS4 v4.0 the same as those for BDEW AS4?

No, Ed25519 and X25519 keys are not ECDSA keys. Any ECDSA certificates used for the alternative ECC option may use different curves than the one used for BDEW AS4.

6 Implementation support

6.1 How is ENTSOG going to help TSOs implement ENTSOG AS4?

TSOs can obtain assistance from ENTSOG by contacting the Interoperability & Data Exchange team. ENTSOG will also support implementations via dedicated Webinars and the annual ENTSOG Data Exchange workshop.

6.2 Are solution providers already implementing ENTSOG AS4 v4.0?

Yes, solution providers are already implementing ENTSOG AS4 v4.0. Some are now offering it in products and services and others are known to have prototype implementations with several having expressed intentions to support it after 2025.

6.3 What is interoperability testing and why should my solution provider get involved?

Interoperability testing is a test involving multiple independent implementations exchanges AS4 messages according to the specifications. In 2024, the eDelivery team of the European Commission organized some interoperability testing (as part of validation of their eDelivery v2.0 profile) and they intend to do further interoperability testing going forward. ENTSOG will support this work.

6.4 What is conformance testing and why should my solution provider get involved?

Conformance testing is a testing involving an implementation of AS4 executing test scenarios against a conformance testing solution where the conformance of exchanged messages is validated against the specification. For their earlier v1.15 profile, the eDelivery team operates a conformance testing service. This service will be updated for their v2.0. Solutions that pass this conformance testing service are also applicable for ENTSOG AS4 v4.0 due to its overlap to eDelivery v2.0.

6.5 My solution provider wants assistance from ENTSOG in implementing v4.0. Where can they get help?

ENTSOG does not have a mandate and/or resources to support private companies implementing the new profile but will provide help when resource is available on a best effort basis.

6.6 Can EASEE-Connect help with migration?

The EASEE-Connect service of EASEE-gas allows parties to register their connection parameters and to establish connections with counterparties. It supports registration of supported versions of the ENTSOG profile (v3.6 or v4.0) and supports the different types of data which are stored and shared for the different profile versions.