eDelivery Interoperability Forum

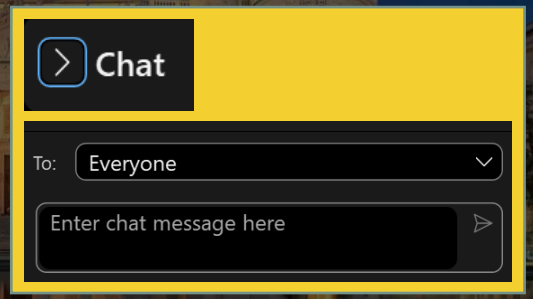
Discussion & feedback

27 June 2023

Reminder

The meeting is not being recorded

Place your Qs in the chat section or



Raise your hand if you want to speak or ask Q

Mute your microphone when you do not speak

Your Privacy

By intervening in the meeting, you agree to share your name, voice and video image with the other participants.

The privacy statement for the meeting is available on the registration page:
https://ec.europa.eu/eusurvey/runner/edeliveryInteroperabilityForum

Lorem

Lorem

Lorem ipsum

Welcome

Maya Madrid

The eDelivery Interoperability Forum

is...

a platform for the eDelivery BB and for solution and service providers to explore together the technical evolution, market opportunities and market needs around eDelivery

and aims to promote knowledge sharing, provide feedback on challenges, needs and preferences, and facilitate the discussion for the way forward

with the objective to...

keep eDelivery solution and services providers up to date with the evolution of the eDelivery building block (e.g., technical specifications)

bring projects and solution/service providers together to facilitate match-making between business needs and service offering

collect input from solution/service providers to guide building block's strategy

convenes...

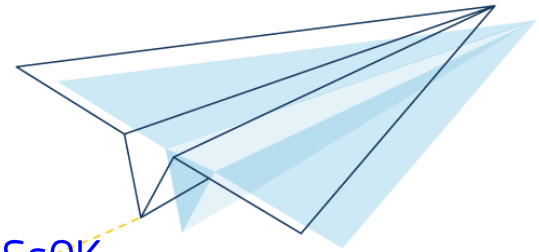
online for one to two hours

2-4 times / year depending on participation, evolution and needs

Public Consultations available

The public consultations for eDelivery specification changes are available now

- **eDelivery AS4 profile 2.0** draft specification: https://ec.europa.eu/digital-building-blocks/wikis/x/dVTZJw
- **eDelivery SMP profile 2.0** draft specification: https://ec.europa.eu/digital-building-blocks/wikis/x/zSs0K



Update roadmap

2023 — **2024** — **2025**

End of public consultation	Discussion in Interop. Forum	Adoption & Publication	Product support	Roll-out in projects
20 October 2023	**28 November 2023**	**End of 2023**	**2024-2025**	**2025 onwards**

eDelivery Conformance Testing Service

New conformance testing platform

The new conformance testing platform is available:

https://as4conftest.edelivery.tech.ec.europa.eu/itb

New display of conformant solutions

Conformant eDelivery AS4, SMP and SML products will be displayed in a new way to make sure recently tested products (and product versions) are clearer to the users.

[Webinar on eDelivery value proposition 28 September (tentative)]

[eDelivery Informal Cooperation Network Meeting 9 November]

[eDelivery Interoperability Forum 28 November]

[Survey to collect the interests to future webinars]

[Archive of past events]

Discussion & Feedback

Bogdan Dumitriu

Overview of the previous meeting

1 eDelivery news (*by Bogdan Dumitriu*)

New market opportunities

eDelivery service offering updates

2 eDelivery profiles updates (*by Pim Van Der Eijk*)

eDelivery AS4 profile 2.0

eDelivery SMP profile 2.0

3 Conformance testing service updates (*by Bogdan Dumitriu & François Gautier*)

New conformance testing platform (demo)

New presentation of conformant solutions

4 Discussion (*all*)

Sharing needs, expectations, feedback, etc

Slides of the previous meeting are available on the eDelivery User Community

https://ec.europa.eu/digital-building-blocks/wikis/x/BQXrJ

Questions and Answers from the previous session

Maya Madrid

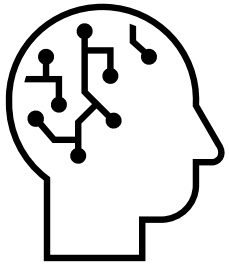
Policy Officer

eDelivery policy officer in CNECT, EC

Francois Gautier

Technical Expert

eDelivery technical expert, conformance testing



Pim Van Der Eijk

Architect

eDelivery technical expert, AS4 and SMP specification changes

Bogdan Dumitriu

Project Officer

Project officer in charge of eDelivery implementation in DIGIT, EC

Please try to limit your intervention at 5 minutes

Guided discussion through last meeting’s topics

Bogdan Dumitriu

Feedback welcome

Guided discussion

We would especially appreciate feedback for slides marked as ‘Feedback welcome’!

eDelivery AS4 and SMP profiles updates

Pim Van Der Eijk

eDelivery AS4 2.0 specification

- **Modernisation of cryptography**
- **Adoption of ebCore Agreement Update**

eDelivery SMP 2.0 specification

- **Support for OASIS SMP version 2.0**
- **Allow publishing multiple certificates**

Rationale and approach for AS4 security update

Cryptography and Internet security continues to evolve

- The security parameters of eDelivery AS4 were high-end when they were selected but have only been marginally updated since 2014
- Current profile is still secure but is no longer leading edge
- New algorithms and key types based on elliptic curve cryptography are commonplace and their use is expected for new applications and protocols
  - IETF RFC 9231 allows their use in XML Security, WS-Security and AS4
- By aligning with state-of-the-art security we provide continuity and investment protection

Rationale and approach for AS4 security update

Approach

- Continue to promote eDelivery as a cross-domain, general purpose solution
- Independent experts (cryptography, info sec) and IETF editor for support

Feedback welcome

eDelivery AS4 2.0 message layer security

Message signing

- Mandatory support (Common Profile) for Ed25519 (elliptic curve signature algorithm using EdDSA and Curve25519)

Message encryption

- Mandatory support for encryption using X25519 (elliptic curve Diffie-Hellman key exchange using Curve25519)

Feedback welcome

eDelivery AS4 2.0 message layer security

Message encryption

- ECDH allows two parties to jointly agree on a shared secret using an insecure channel.
- ECDH-ES mode involves a stable shared recipient public key
- Optional full ephemeral mode in combination with new ebCore Certificate Update (enhancement)

Feedback welcome

eDelivery AS4 2.0 message layer security

Alternative message and encryption

- Optional support (enhancement) for ECDSA (for cryptographic agility and/or interoperability with some MS scheme)
- The consultation is launched with mandatory support for Ed25519 and X25519 and optional support for ECDSA and Brainpool curves
- The specification may yet be revised to mandate support for both options in the Common Profile

eDelivery AS4 2.0 transport layer security

Transport Layer Security

- Support for TLS 1.3
- Modern curves

Feedback welcome

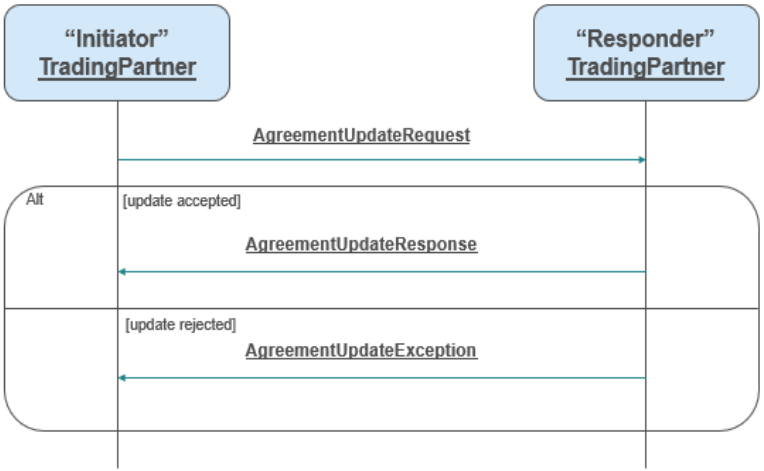
New feature: OASIS ebCore Agreement Update (1/2)

ebCore Agreement Update is an OASIS specification for interoperable message-based updating of messaging configurations.

It is already part of ENTSOG's AS4 profile.

Certificate update

- Signing, encryption, key exchange certificate updates
- Sharing short-lived, partner-specific key exchange public keys



Feedback welcome

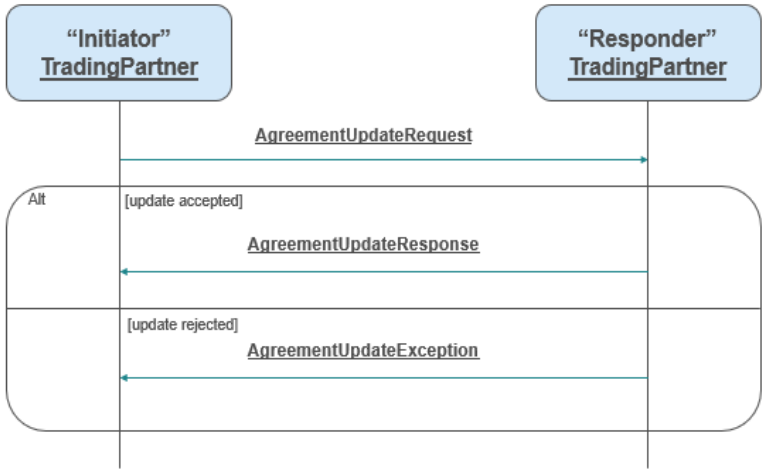
New feature: OASIS ebCore Agreement Update (2/2)

(Optional, future) **endpoint update**

- Endpoint URLs, profile versions, algorithms, network security updates

Benefits

- Automation for direct trust / mutual exchange networks
- No dependency on central services
- Approximates full ephemeral ECDH



Feedback welcome

Updates to dynamic sender enhancement

eDelivery SMP 2.0

- Support for OASIS SMP version 2.0
- Allows publishing multiple certificates (signing, encryption, key exchange) for a transport
- Supports eDelivery AS4 1.15 and 2.0

No change needed in BDXL

Status and next steps

Status

- eDelivery AS4 profile 2.0 draft specification:
  - Consultation page: https://ec.europa.eu/digital-building-blocks/wikis/x/dVTZJw
  - Specification page: https://ec.europa.eu/digital-building-blocks/wikis/x/NabXGw
- eDelivery SMP profile 2.0 draft available:
  - Consultation page: https://ec.europa.eu/digital-building-blocks/wikis/x/zSs0K
  - Specification page: https://ec.europa.eu/digital-building-blocks/wikis/x/xqfXGw

Feedback welcome

Status and next steps

Next steps:

- Provide feedback to public consultations by the 20th of October 2023
- Proof-of-concept implementations (one company already implemented the new security algorithms)
- Engage with Certification Authorities on provision of certificates

Conformance testing service updates

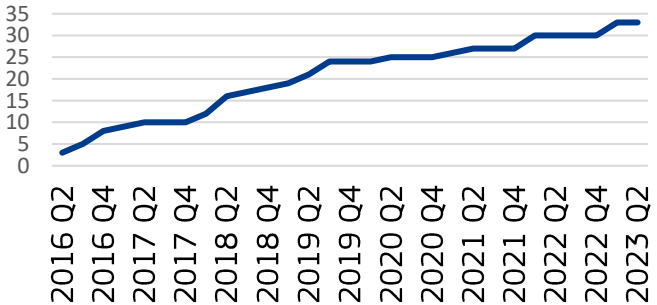
Bogdan Dumitriu
François Gautier

eDelivery AS4 conformant solutions

More information on Digital Europe

Conformant Solutions >

Evolution of eDelivery AS4 conformant solutions (2016-2023)



SMP conformant solutions

More information on Digital Europe

Conformant Solutions >

- Datainterchange - EPIC
- eConnect – Procurement Service Bus (PSB)
- Edicom SMP
- eefacta server
- Galaxy Gateway
- Harmony eDelivery Access
- Ion SMP
- phoss
- Qvalia
- SMP (EC sample software)

Feedback welcome

New presentation of conformant solutions

Multi-level presentation of solutions

Solutions will be grouped based on the eDelivery AS4 or SMP profile version they support, followed by the conformance testing methodology

Product versions will be displayed

The stable version of the tested product will be displayed (not including the patch version)

Conformance testing methodology will be displayed

As the conformance testing methodology (test suite) will evolve more rapidly over time, a versioning system will be introduced and displayed. Products will be grouped based on the version of the methodology.

User feedback

Users will be invited to provide feedback concerning issues encountered with a particular product. The feedback will be critically reviewed by the eDelivery team and not displayed on the web site but may inform changes to the conformance testing methodology.

eDelivery conformance testing

- eDelivery AS4 profile (based on OASIS/ISO ebMS3/AS4)
  - Common profile
  - Profile enhancements

- eDelivery SMP profile (based on OASIS SMP)

Conformance testing platform

- Current solution (Minder) allows conformance testing of:
  - eDelivery AS4 profile v1.15
    - Common profile
    - 3 (out of 6) profile enhancements
    - + ENTSOG usage profile
  - eDelivery SMP profile v1.10

New conformance testing platform

- The new conformance testing solution:
  - Is based on Interoperable Europe's GITB (Generic Interoperability Test Bed);
  - Will be launched on 19 May 2023;
  - Will initially contain the same tests and conformance statements present in the current platform for eDelivery AS4;
  - Will evolve over the next year to support the 3 missing profile enhancements and eDelivery AS4 and SMP 2.0 specifications.

New conformance testing platform

- The new conformance testing solution:
  - Will allow you troubleshoot a lot more independently;
  - Will be more modern, user-friendly and will allow the project team to expand the test suite much faster in the future;
  - Will allow you to easily upgrade the conformance statement when the conformance testing methodology or the eDelivery specifications evolve.

The eDelivery symbiosis

Building block

Promote and facilitate the use of eDelivery in the European digitalisation

Ensure long-term custodianship of eDelivery specifications and baseline services

Provide level playing field for projects/users to learn about solution and service providers

Solution and service providers

Provide eDelivery service offerings in response to market needs

Evolve services in line with specifications and provide tailored and user-friendly support

Learn and address customer needs

What are the best practices and expectations that would help support the development of a vibrant market for eDelivery software vendors and service providers?

Your feedback is important to us! The feedback survey

https://europa.eu/!cDX47x

Have a question?

eDelivery

Exchange data and documents online reliably and securely

Bogdan Dumitriu

To continue the conversation, contact our team via email

Emails:
EC-digital-building-blocks@ec.europa.eu
EC-eDelivery-support@ec.europa.eu

Thank you

& stay in touch