EUROPEAN COMMISSION
DIRECTORATE-GENERAL FOR DIGITAL SERVICES

Directorate B – Digital Enablers & Innovation
DIGIT.B.3 – Digital Trust

Disposition of Public Review Comments on "eDelivery AS4 2.0 (2023 PR draft)"

13 February 2024

1. INTRODUCTION

In June 2023, the eDelivery team requested public review comments on its first draft ("2023 PR draft") of a new eDelivery AS4 2.0 profile. The new draft specification updated the security section by adopting more state-of-the art protocols and algorithms and proposed two new Profile Enhancements:

- **ebCore Agreement Update**, an OASIS specification for interoperable message-based updating of messaging configurations.
- **Profile Enhancement for supporting alternative curves and algorithms**, supporting ECDSA for signing and ECDH-ES for key agreement based on Brainpool curves in addition to the main curve and algorithm introduce in the Common Profile.

Please consult this page for more details.

The review comments that were received are addressed in this document.

2. DISPOSITION OF COMMENTS

#	Public Consultation Comment(s)	eDelivery Disposition
	Security choices	
1	It is unclear what the benefits are of changing from key transport to key agreement taking into account there is no or very limited support for key agreement in implementations. Instead of improving interoperability this changes rather seems to increase risk of incompatibilities. There are also no [known] security risks with key transport and the current cryptographic algorithm advisories from both NIST and BSI still accept its use based on the RSAES-OEP algorithm.	Our draft profiles are based on the recommendations from the experts in the area of cryptography and XML Security selected by ENISA who responded to our request to provide recommendations that reflect the current state of the art (published here as supporting documents). The objective is for the updated profile to be stable for a longer period which means it has to be leading-edge. When using algorithms that are no longer state-of-the-art, we would risk having to update the updated profile already earlier. By using the specific proposed set of algorithms, we align eDelivery with the current practice for many other recent Internet protocol standards and applications, facilitating trust of new users and better security for existing ones. The current versions of our profiles are expected to co-exist with the new ones in the medium term. The new versions are being prepared in view of the eventual obsolescence of the cryptography still in use today. For this reason, we see it preferable for the new cryptography to follow the state of the art. In addition to the general approach described above, we asked the cryptography expert who provided the initial recommendations to contribute further clarifications regarding the proposal to replace key transport with key agreement. The received reply is included below for information. **Key Transport Algorithm (one-pass) based on RSA encryption** Three are the main problems with RSA based key encryption (using either RSA-PKCS# 1 v1.5, or RSA-OAEP). a) (Perfect) Forward secrecy: it is a feature of key-agreement protocols that gives assurances that session keys will not be compromised even if long-term secrets used in the session key exchange are compromised. This is clearly not the case for RSA based key encryption. When the key is encrypted with the long lived public key, the same private key is used to decrypt the ciphertext and

retrieve the symmetric key. When this key is leaked, the attacker can use it to reveal all previous communications. On the other hand, ephemeral DH key agreement offers forward secrecy, since the private/public key pair is only used for a single message exchange (or session).

b) In the key transport scenario, only one of the communicating entities generates the common key (and sends it using RSA encryption). Thus, the security of the symmetric key based secure channel depends only on one source of randomness.

c) RSA-PKCS# 1 v1.5 is notoriously difficult to implement, it doesn't have a security proof and there are attacks that are still applicable (variants of Bleichenbacher's attack[1], like so the called ROBOT attack[2]). RSA-OAEP is also challenging to implement securely.

d) RSA is less efficient than EC based solutions.

Note: The ECDH key agreement must be combined with an authentication mechanism that usually is based on public key cryptography (a certificate is used for public key retrieval) and the private key is long-term. In case that the attacker retrieves this private key, she is able to mount a man-in-the-middle attack.

Key transport based on RSA public key encryption alternatives

The main alternative to key transport based on RSA public key encryption is the KEM/DEM paradigm (KEM = key encapsulation mechanism, DEM = Data Encapsulation Mechanism). Among the three main KEM protocols, only one doesn't depend on the Diffie-Hellman protocol.

The RSA-KEM has the same security weaknesses (no forward secrecy), but it is considered easier to implement than RSA based encryption.

[1] Chosen Ciphertext Attacks Against Protocols Based on the RSA Encryption Standard PKCS #1, Daniel Bleichenbacher. https://archiv.infsec.ethz.ch/education/fs08/secsem/bleichenbacher98.pdf

[2] The ROBOT Attack https://robotattack.org/

Support for XHE and EndpointParticipantIdentifier		
2	As the SBDH specification is outdated and replaced by the XHE specification, replace the SBDH profile enhancement with an XHE profile enhancement or add an XHE profile enhancement and deprecate the current SBDH one.	We are proposing the removal of SBDH as a profile enhancement in the next version of the draft profile. The SBDH feature originates in the earlier eSENS project, but experience in eDelivery has shown it to be one of the least used profile enhancements. AS4 already provides direct support for messages containing multiple parts as it is based on MIME packaging, as confirmed successfully in several ecosystems that use AS4 without SBDH, so users do not need this enhancement to exchange multiple payloads in a single message. Users can use either SBDH or XHE as a regular payload without any further specifications and we believe that the removal of the SBDH profile enhancement will further clarify this fact. Against this background, we don't currently see a need for an XHE profile enhancement.
3	Require or recommend (depending also on keeping the SBDH enhancement) the usage of the XHE for 4-Corner topologies based on the OASIS AS4 Interoperability Profile for Four-Corner Networks specifications.	This suggestion is rejected as it would be a breaking change for several tens of ecosystems without clear benefits.
4	Also use the EndpointParticipantIdentifier message property defined in the OASIS specification to identify the Access Point that should receive technical response messages as described in section 3 of the OASIS specification.	We have no such requirement to date from users of the eDelivery AS4 profile. We are open to considering it if the business need appears.