eDelivery AS4

9 maart 2023

bsi. ISO/IEC 27001 Information Security Management

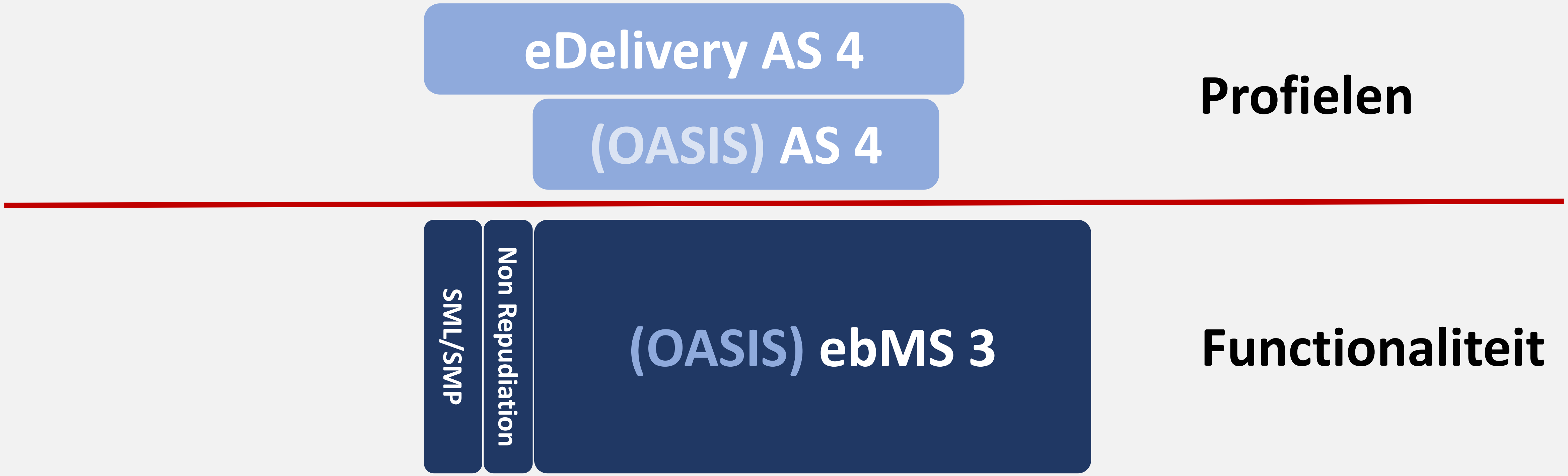
eDelivery AS4

- eDelivery en eDelivery AS4
- Functionaliteit eDelivery AS4
- Toepassing Internationaal en Nationaal
- Verschil in Toepassing
- Nieuwe Ontwikkelingen
- eDelivery AS4 Implementaties
- Digikoppeling

eDelivery en eDelivery AS4

- eDelivery is een door de EU gekozen set van standaarden t.b.v. gegevensuitwisselingen vergelijkbaar met Digikoppeling
- De eDelivery standaard wordt beheerd door DG_DIGIT
- Binnen eDelivery zijn er profielen gedefinieerd voor zowel ebMS3 als voor REST API’s
- eDelivery AS4 is een profiel op basis van ebMS3 AS4:
  - ➢ eDelivery AS4 = ebMS3 AS4 + extensies

Functionaliteit eDelivery AS4



eDelivery AS 4

(OASIS) AS 4

Profielen

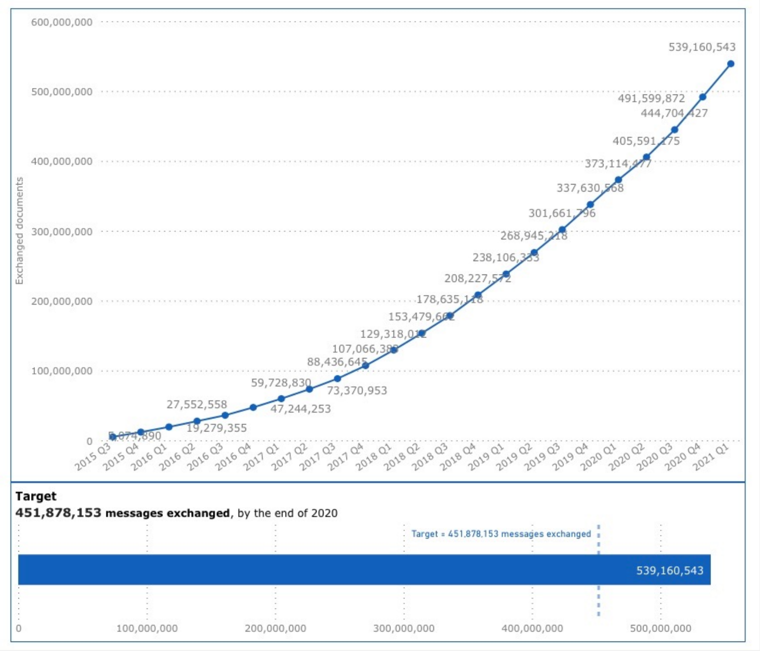
SML/SMP

Non Repudiation

(OASIS) ebMS 3

Functionaliteit

Gebruik Internationaal en Nationaal



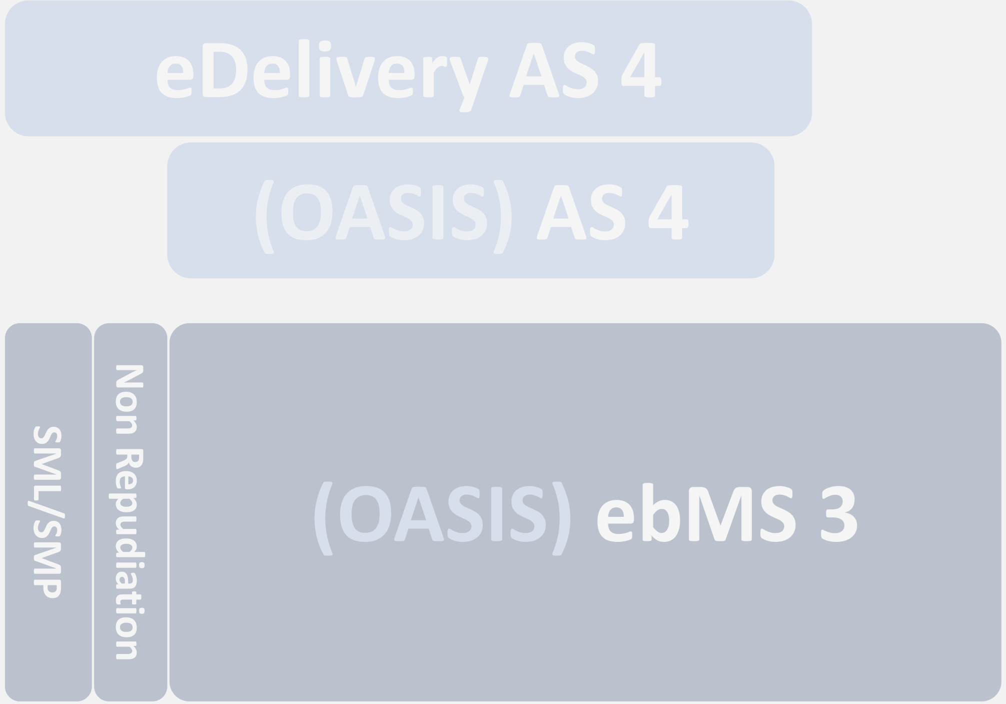
https://ec.europa.eu/digital-building-blocks/wikis/display/CEFDIGITAL/eDelivery+dashboard

- eDelivery AS4 is binnen EU de standaard voor internationaal gegevensuitwisseling, basis bouwblok voor vele grote EU projecten (b.v. SDG/OOTS)

- Voorbeelden Internationale toepassing:
  - E-CODEX
  - EESSI
  - BORIS
  - PEPPOL
  - ECHA
  - ENTSOG
  - EPREL
  - TACHOnet
  - ICS2
  - …

- Voorbeelden Nationale toepassing:
  - Energie Sector (EDSN)
  - EDI4Steel
  - eProcurement (PEPPOL)

Verschil in Toepassing



eDelivery AS 4

(OASIS) AS 4

SML/SMP

Non Repudiation

(OASIS) ebMS 3

- E-CODEX:
  - Point-to-Point
  - Statische Configuratie
- PEPPOL:
  - Point-to-Point
  - SML/SMP (Discovery)
  - Eigen (PEPPOL) PKI
- EESSI:
  - Point-to-Point (Via Nationale Access Points)
  - CSN (Registratie, Distributie)
  - TESTA PKI voor verkeer tussen AP’s
  - ‘Publieke’ PKI voor nationale applicaties
- BORIS:
  - Ster Netwerk (Centraal Register)

Nieuwe Ontwikkelingen

The eDelivery AS4 profile is being updated. Its main changes relate to the security algorithms used. The profile will introduce ECC-based signing and encryption as its nominal model and downgrade RSA-based signing to legacy status, in line with other AS4 profiles in Europe. It will separate:

- *Long-lived certificates used for signing and encrypting messages, normally issued by Certification Authorities*
- *Short-lived (ephemeral) encryption keys. These keys are generated by the parties directly and shared bilaterally rather than via a registry as they are specific to an individual counterparty.*
- *It will also add a new feature for updates of security tokens based on OASIS ebCore Agreement Update. This protocol supports using secure messages for securely updating both long-lived and short-lived security tokens, similar to modern security protocols as used in IM apps like Signal.*
- *It allows an approach similar to management of user accounts in enterprises: an initial process to be onboarded to an organization (usually involving some approval steps, initial setup of passwords and/or tokens) after which the user can self-manage (periodically changing passwords etc.), except for exceptional situations like forgotten or expired passwords that may trigger a re-onboarding.*

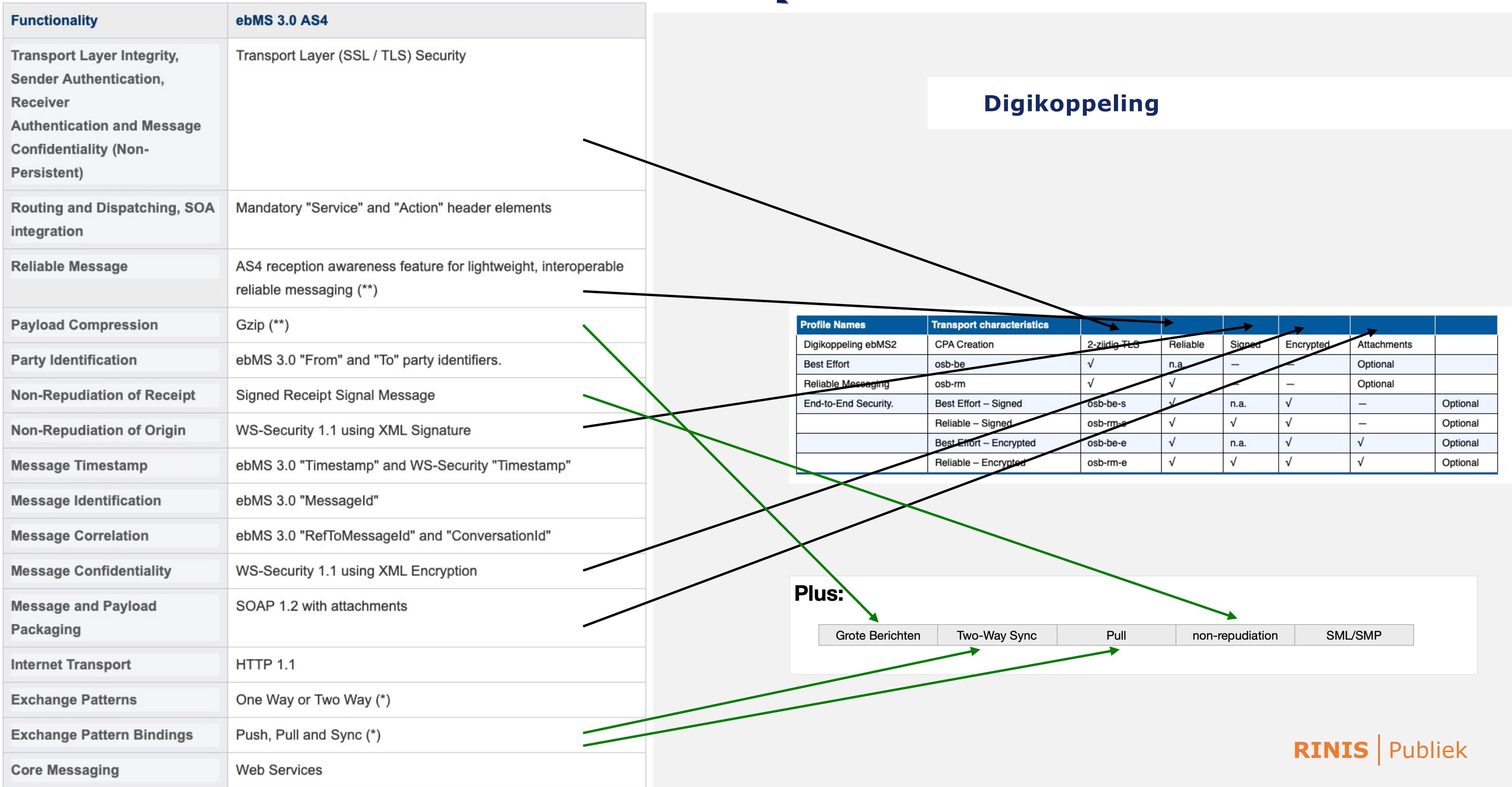
The updated eDelivery profile specifications will first go through a public review. Products implementing eDelivery need to be adapted to support the new functionality. It will therefore only become relevant for future versions, well after December 2023.

eDelivery AS4 Implementaties

eas.x
edicomas server
PAGERO
edata arc
[OXALIS]
FLAME
SEEBURGER
Business Integration
mendelson
e-commerce gmbh
ion-AP
Galaxy
GATEWAY
axway
babelway
Bizbrains
Integration accomplished.
AS4.NET
linQsupply®
IDA INFRONT
ADDNODE GROUP
data interchange
Harmony
eDelivery Access
phase4
OSS
iFENIX
GENESIS IT
IBM®
Cleo
... never stops
navitasoft
IP systems
UM
nota
software AG
HOLODECK B2B
DESCARTES
AdValvas
europe
b2brouter
qvalia
DOCUMENT CENTRIC SOLUTIONS

https://ec.europa.eu/digital-building-blocks/wikis/display/DIGITAL/eDelivery+AS4+conformant+solutions

Digikoppeling



Functionality	ebMS 3.0 AS4
Transport Layer Integrity, Sender Authentication, Receiver Authentication and Message Confidentiality (Non-Persistent)	Transport Layer (SSL / TLS) Security
Routing and Dispatching, SOA integration	Mandatory "Service" and "Action" header elements
Reliable Message	AS4 reception awareness feature for lightweight, interoperable reliable messaging (**)
Payload Compression	Gzip (**)
Party Identification	ebMS 3.0 "From" and "To" party identifiers.
Non-Repudiation of Receipt	Signed Receipt Signal Message
Non-Repudiation of Origin	WS-Security 1.1 using XML Signature
Message Timestamp	ebMS 3.0 "Timestamp" and WS-Security "Timestamp"
Message Identification	ebMS 3.0 "MessageId"
Message Correlation	ebMS 3.0 "RefToMessageId" and "ConversationId"
Message Confidentiality	WS-Security 1.1 using XML Encryption
Message and Payload Packaging	SOAP 1.2 with attachments
Internet Transport	HTTP 1.1
Exchange Patterns	One Way or Two Way (*)
Exchange Pattern Bindings	Push, Pull and Sync (*)
Core Messaging	Web Services

Profile Names	Transport characteristics					
Digikoppeling ebMS2	CPA Creation	2-zijdig TLS	Reliable	Signed	Encrypted	Attachments
Best Effort	osb-be	√	n.a.	–	–	Optional
Reliable Messaging	osb-rm	√	√	–	–	Optional
End-to-End Security.	Best Effort – Signed	osb-be-s	√	n.a.	√	–	Optional
	Reliable – Signed	osb-rm-s	√	√	√	–	Optional
	Best Effort – Encrypted	osb-be-e	√	n.a.	√	√	Optional
	Reliable – Encrypted	osb-rm-e	√	√	√	√	Optional

Plus:

Grote Berichten	Two-Way Sync	Pull	non-repudiation	SML/SMP

Links

DG DIGIT: https://commission.europa.eu/about-european-commission/departments-and-executive-agencies/informatics_en
eDelivery: https://ec.europa.eu/digital-building-blocks/wikis/display/DIGITAL/eDelivery
OASIS: https://www.oasis-open.org
ICN eDelivery: https://ec.europa.eu/digital-building-blocks/wikis/display/EDELCOMMUNITY/Informal+Cooperation+Network+for+eDelivery

BETROUWBAAR

GEGARANDEERD

VEILIG

www.rinis.nl

bsi.
ISO/IEC
27001
Information Security
Management