Release Notes Wijziging Digikoppeling Standaarddocumentatie

16-05-2019

1 Overzicht van de wijzigingen

1.1 Wijzigingsverzoeken

Het Technisch Overleg Digikoppeling heeft goedkeuring verleend aan de volgende wijzigingen:

RFC#	Ingediend wijzigingsverzoek	Datum
2019-1	WUS: Signing	04-11-2018
2019-2	ebMS: Gebruik van SyncReplyMode verruimd.	07-02-2019

1.2 Gewijzigde documenten

De volgende documenten zijn gewijzigd:

Digikoppeling	actuele versie	vorige versie
Digikoppeling_Koppelvlakstandaard_WUS	3.7	3.6
Digikoppeling_Koppelvlakstandaard_ebMS2	3.3	3.2
Digikoppeling_Best_Practices_ebMS2	3.2	3.1
Digikoppeling Overzicht Actuele Documentatie en Compliance	1.3	1.2

1.3 Wijzigingen per document

1.3.1 Digikoppeling_Koppelvlakstandaard_WUS_v3.7

#	Locatie	Oorspronkelijke tekst	Gewijzigd in	# RfC	Toelichting
1	2.4.2 P10	**wsa:To** Dit wordt gebruikt om de endpoint vast te leggen waar het bericht naar toe dient te gaan. Het element wsa:to is van het type wsa:AttributedURIType - een extensie op het xs:anyUri type- en dient gevuld te worden met een 'Adres' element. De waarde van het adres element kan hetzij een absolute URI zijn of "http://www.w3.org/2005/08/addressing/anonymous". Optioneel kan het To-adres aangevuld te worden met een OIN door het gebruik van querystring parameters (e.g. http://service-end-point?oin=xxxxxx). De waarde van de oin in het adres is	**wsa:To** Dit wordt gebruikt om de endpoint vast te leggen waar het bericht naar toe dient te gaan. Het element wsa:to is van het type wsa:AttributedURIType - een extensie op het xs:anyUri type- en dient gevuld te worden met een 'Adres' element (wsa:Address). De waarde van het adres element kan hetzij een absolute URI zijn of "http://www.w3.org/2005/08/addressing/anonymous". Optioneel kan het To-adres aangevuld te worden met een OIN door het gebruik van querystring parameters (e.g. http://service-end-point?oin=xxxxxx). De waarde van de oin	2019-1	Toegevoegd (wsa:Address)

		het oin nummer van de ontvangende partij.	in het adres is het oin nummer van de ontvangende partij.		
2	2.4.2 p11	**wsa:From** **WS-Addresing request headers** wsa:RelatesTo Indicates relationship to a prior message. Unused in this MEP, but could be included to facilitate longer running message exchanges	**wsa:From** **WS-Addresing request headers** wsa:RelatesTo Indicates relationship to a prior message. Unused in this Message Exchange Pattern (MEP), but could be included to facilitate longer running message exchanges.	2019-1	Toegevoegd Message Exchange Pattern
3	2.4.2 p11	**WS-Addresing response headers** wsa:To Y	**WS-Addresing response headers** wsa:To Y* … * Sommige platformen wijken op dit punt af van de Web Service Addresing 1.0 – Metadata standaard. Het wsa:To veld wordt bij synchrone SOAP verkeer actief uit het antwoordbericht gefilterd. Om hier vanuit de standaard aan tegemoet te komen mag bij het ontbreken van dit veld in het antwoordbericht door de ontvanger de anonymous waarde (http://www.w3.org/2005/08/addressing/anonymous) worden aangenomen.	2019-1	
	2.4.2 p12	**WS-Addresing response headers** wsa:MessageID Y	wsa:MessageID Y ****** **…** ** Hiermee wordt afgeweken van wat de Web Services Addressing 1.0 – Metadata standaard voorschrijft. Volgens deze standaard is de MessageID in response optioneel. Bovenstaande properties kunnen in een aantal gevallen ook gespecificeerd worden door betreffende velden in de header weg te laten (3). (3) 1 Zie WS-addressing 1.0- Core, paragraaf 2.1en paragraaf 3.2; zie ook BP 1.2 paragraaf 3.7.14.	2019-1	
	2.4.4 p14	**WB004** Ondertekenen van bericht onderdelen SOAP:body, SOAP:headers (WS-Addressing headers en Timestamp) is verplicht bij toepassing van End-to-End beveiliging.	**WB004** Ondertekenen van bericht onderdelen SOAP:body, SOAP:headers (WS-Addressing headers en Timestamp) is verplicht bij toepassing van End-to-End beveiliging. Van elk van deze onderdelen dient separaat een digest te worden berekend en te worden opgenomen in het SignedInfo element. De handtekening	2019-1	

		dient te worden gegenereerd op basis van de inhoud van het SignedInfo element.	
2.4.4 P15	**WB010** Publieke sleutel dat gebruikt is voor het signing proces dient meegeleverd te worden met het bericht via een 'Direct security token' reference. Overwegingen: Het certificaat wordt in het bericht meegestuurd. Hiermee kan de ontvanger door middel van het meegeleverd certificaat de handtekening controleren. Het certificaat dient uiteraard wel vertrouwd te zijn via een truststore configuratie	**WB010** Publieke sleutel welke gebruikt is voor het signing proces dient meegeleverd te worden met het bericht via een 'Direct security token' reference. Overwegingen: Het certificaat wordt in het bericht meegestuurd. Hiermee kan de ontvanger door middel van het meegeleverd certificaat de handtekening controleren. Het certificaat dient uiteraard wel vertrouwd te zijn via een truststore configuratie waarin het PKIoverheid stamcertificaat alsmede de intermediair certificaten en Trusted Servicer Provider certificaten zijn opgenomen. Zie hiervoor https://cert.pkioverheid.nl/. (een vereiste voor veel platformen om de validatie van het bericht aan te vangen).	2019-1
2.4.4 P15	(nieuw)	**WB013** Indien WS-Security wordt toegepast, is het controleren van de signature door de ontvangende partij verplicht. Overwegingen: Het ondertekenen van berichten is alleen zinvol als de ontvanger van het bericht ook daadwerkelijk de signature valideerd. Indien de validatie mislukt, dient het bericht afgewezen te worden en een foutmelding als antwoord te worden verstuurd.	2019-1
2.4.4 P15	(nieuw)	**WB014** Indien WS-Security wordt toegepast dient het responsebericht de signature van het requestbericht als onderdeel van het SignatureConfirmation element op te nemen (WS-Security 1.1). Overwegingen: Door het herhalen van de ondertekening van het requestbericht kan de ontvanger van het responsebericht valideren dat het oorspronkelijke requestbericht in onaangetaste staat is ontvangen en verwerkt.	2019-1

1.3.2 Digikoppeling_Koppelvlakstandaard_ebMS_v3.3

#	Locatie	Oorspronkelijke tekst	Gewijzigd in	# RfC	Toelichting
1	Par 2.3/P9	Reliable Messaging: asynchrone uitwisseling met ontvangst bevestigingen en duplicaateliminatie door de ontvangende message handler	Aan deze zin is een voetnoot toegevoegd: *In bepaalde gevallen mag een acknowledgement synchroon verstuurd worden. Zie par 4.4*	2019-2	
2	Par 2.3/P9	De berichtenuitwisseling is asynchroon: een business request wordt in een eigen synchrone HTTP request/response sessie verzonden, terwijl de acknowledgement en optionele business response via een separaat HTTP request/response sessie verzonden worden.	De berichtenuitwisseling is *in principe* asynchroon: een business request wordt in een eigen synchrone HTTP request/response sessie verzonden, terwijl de acknowledgement en optionele business response via een separaat HTTP request/response sessie verzonden worden. In bepaalde gevallen (zie **Fout! Verwijzingsbron niet gevonden.**) mag een acknowledgement of een error synchroon verstuurd worden, Business*responses* worden altijd asynchroon, in een separaat HTTP sessie verzonden.	2019-2	
3	Par 3.1/P12	**SyncReply Module** [ebMS 2.0] Section 4.3 Best effort & Reliable Messaging & End-to-End Security SyncReply is never used in these profiles. All messages, including acknowledgments and error messages, are sent asynchronously.	**SyncReply Module** [ebMS 2.0] Section **Fout! Verwijzingsbron niet gevonden.** Opgesplitst in 3 kolommen: **Best effort** Never used in this profile **Reliable Messaging** Optional used in this profile. All messages, including acknowledgments and error messages, are sent asynchronously, with the exception of cases as described in par 4.4.1. Only in specific cases can MSH signals (acknowledgements, errors) sent synchronously. See 4.4.1 for conditions. **End-to-End Security** Optional in this profile. See profile Best Effort or profile Reliable Messaging for details	2019-2	
4	Par 3.1/P12	[Name and Reference] Asynchronous messaging does not preclude fast response times, as is required to support interactive applications. Asynchronous messaging supports higher levels of scalability and supports	[Notes] Asynchronous messaging does not preclude fast response times, as is required to support interactive applications. Asynchronous messaging supports higher levels of scalability and supports scenarios where a response message may be	2019-2	Tekst is ongewijzigd. De alinea is verplaatst naar de Notes

		scenarios where a response message may be sent minutes, hours or days after the initial request message. Asynchronous messaging may be combined transparently with store-and-forward intermediaries.	sent minutes, hours or days after the initial request message. Asynchronous messaging may be combined transparently with store-and-forward intermediary		
5	Par 3.2/P16 Mult-hop Module	These profiles use asynchronous communication for business messages, acknowledgments and error messages. This protocol is therefore compatible with asynchronous, transparent, store-and-forward ebXML Messaging (or other SOAP-based) intermediaries. However, this document only specifies functionality between ebXML Message endpoints. (See also caveat in the section 'Reliable Messaging Module' in this chapter.)	[verwijderd]	2019-2	Multi-hop wordt niet gebruik binnen Digikoppeling. Dan is deze toelichting over het gebruik van *asynchronous messaging* niet relevant.
6	Par 4.4.1/P40 Name and Reference	[ebMS 2.0] Section 4.3 SyncReply Best effort & Reliable Messaging & End-to-End Security	Opgesplitst in 3 kolommen: (zie #7)		
7	Par 4.4.1/P40 Profiling (a)	(leeg)	**Best effort** Not applicable. **Reliable Messaging** SyncReply is restricted to **none** (default) or **mshSignalsOnly** (on condition) Condition for usage of msghSignalsOnly mode is: • both parties MSH are able to activate syncReplyMode=msghSignalsOnly see also [Best Practice]**End-to-End Security** See profile Best Effort or profile Reliable Messaging for details		
8	Par 4.4.1/P40 Profiling (b) If SyncReply mode is used, are MSH	(leeg)	**Best effort** Not applicable. **Reliable Messaging** If SyncReply mode used only MSH signals are expected synchronously **End-to-End Security** See profile Best Effort Reliable Messaging for details		

	signals, business messages or both expected synchronously?		
9	Par 4.8.1/P50	In case Reliable messaging is used: This profile uses end-to-end reliable messaging. This allows the Digikoppeling to recover from any temporary processing failures at the level of intermediaries. Upcoming versions of the Digikoppeling may support store and forward ebXML intermediaries at an infrastructure level. The functionality of these intermediaries is likely be limited to fully transparent, asynchronous store-and-forward routing of ebXML Messages. In that case, no special processing is required of endpoints in the presence of any such intermediaries, as compared to direct point-to-point connections, other than supporting connection to/from the URL and client and server TLS authentication details for the intermediary rather than the "true" sender/recipient.	In case **Reliable messaging** is used: This profile uses end-to-end reliable messaging. This allows the Digikoppeling to recover from any temporary processing failures at the level of intermediaries. Upcoming versions of the Digikoppeling **may** support store and forward ebXML intermediaries at an infrastructure level. The functionality of these intermediaries is likely be limited to fully transparent, asynchronous store-and-forward routing of ebXML Messages, with the exception of cases as described in par 4.4.1. In the default asynchronous case, no special processing is required of endpoints in the presence of any such intermediaries, as compared to direct point-to-point connections, other than supporting connection to/from the URL and client and server TLS authentication details for the intermediary rather than the "true" sender/recipient.
10	6.1 Non-Normative References		Toegevoegd: **[Best Practice]** Digikoppeling Best Practices ebMS2 URL https://www.logius.nl/sites/default/files/public/bestanden/diensten/DigiKoppeling/Standaarden/Digikoppeling-Best-Practices-ebMS2.pdf
11	Hele document		Een paar kleine typo's verwijderd

1.3.3 Digikoppeling_Best_Practices_ebMS2v3.2 (Niet Normatief)

Best Practice EB015 over SyncReply toegevoegd

1.4 Overzicht releases

Document	Normatief	Release 23-07-2018	Release 21-08-2018	Release 16-05-2019
Wat is Digikoppeling		1.1.1	1.1.1.	1.1.1
DK Beheermodel en releasebeleid		1.5	1.5	1.5
DK Architectuur	X	1.5.1	1.5.1	1.51
DK Koppelvlakstandaard WUS	X	3.5	3.6	3.7
DK Koppelvlakstandaard EBMS2	X	3.2	3.2	3.3
DK Koppelvlakstandaard Grote Berichten	X	3.2	3.2	3.2
DK Identificatie en Authenticatie	X	1.4	1.4	1.4
DK Beveiliging standaarden en voorschriften	X	1.1	1.1	1.1
DK Overzicht Actuele Documentatie en Compliance	X	1.1	1.2	1.3
DK Best Practices WUS		1.10	1.10	1.10
DK Best Practices EBMS2		3.1	3.1	3.2
DK Best Practices Grote Berichten		3.1	3.1	3.1
DK Gebruik en achtergrond certificaten		1.5	1.5	1.5

Met arcering is aangegeven welke onderdelen zijn gewijzigd in de release.