Release Notes Wijziging Digikoppeling 2.0 en 3.0 Standaarddocumentatie

4 april 2016

1 Overzicht van de wijzigingen

Het Technische Overleg Digikoppeling heeft goedkeuring verleend aan de volgende wijzigingsverzoeken

RFC#	Ingediend wijzigingsverzoek	Datum ingediend
1	Verzocht wordt om beveiligingsstandaarden op te nemen in een apart document waarin alleen de actuele versies van de TLS standaard, de SHA standaard en ciphers staan. De koppelvlakspecificaties kunnen naar dit document verwijzen.	11-6-2015
2	Verzocht wordt om requirement "4.1.8 Profile Requirement Item: Timestamp" uit de koppelvlakspecificatie ebMS te verwijderen omdat het formaat van de Timestamp niet configureerbaar is.	7-9-2015
3	Verzocht wordt om in DK 3.0 WUS KVS in paragraaf 2.4.2 het type van de wsa:to aan te passen naar anyURI (in plaats van EndpointReference) om daarmee onderliggende standaarden te volgen.	17-9-2015
4	Bij het samenstellen van het nieuwe Digikoppeling beveiligingsvoorschrift zijn ook referenties naar (wettelijke)regelingen en internationale standaarden bekeken en indien nodig up-to-date gebracht	4-4-2106

Bij de uitvoering van dit wijzigingsverzoek is geconstateerd dat in de Digikoppeling Documentatie nog verwezen werd naar de SHA-1 standaard tbv signing en encryptie. SHA-1 is echter inmiddels niet meer veilig voor dit doel. Bij het opstellen van het Digikoppeling Beveiligingsvoorschrift is daarom de volgende wijziging doorgevoerd

RFC#	Constatering	Datum ingediend
5	SHA-1 wordt gezien als een zwakke cipher voor signing en deze zal in de loop van dit jaar niet langer door de gangbare browsers ondersteund worden. In de beveiligingsrichtlijnen voor Transport Security van het NCSC wordt het gebruik van SHA voor Voor het genereren van een certificaathandtekening onvoldoende bestempeld. Op de "Gangbare Standaarden" lijst van het Forum Standaardisatie wordt naar SHA-2 verwezen.	04-04-2016

Naar aanleiding van deze verzoeken zijn de volgende documenten uit de Digikoppeling Standaard gewijzigd:

Digikoppeling 2.0

- Digikoppeling_2.0_Architectuur_v1.4.docx
- Digikoppeling_2.0_Koppelvlakstandaard_WUS_v2.7.docx
- Digikoppeling_2.0_Koppelvlakstandaard_ebMS_v2.7.docx
- Digikoppeling_2.0_Koppelvlakstandaard_GB_v1.4.docx

Digikoppeling 3.0

- Digikoppeling_3.0_Architectuur_v1.3.docx
- Digikoppeling_3.0_Koppelvlakstandaard_ebMS_v3.1.docx
- Digikoppeling_3.0_Koppelvlakstandaard_GB_v3.1.docx
- Digikoppeling_3.0_Koppelvlakstandaard_WUS_v3.4.docx

Digikoppeling 2.0 en 3.0

- Digikoppeling_Identificatie_en_Authenticatie_v1.3.docx
- Digikoppeling_Gebruik_en_achtergrond_certificaten_v1.4.docx
- Digikoppeling_Beheermodel_v1.4.docx
- Digikoppeling_Beveiligingsstandaarden_en_voorschriften_v2.docx

Daarnaast zijn de XML berichtvoorbeelden uit de Digikoppeling koppelvlakstandaarden WUS 2.0 en 3.0 verwijderd. Deze voorbeelden zullen worden gepubliceerd in een apart document en worden op een later moment opgeleverd.

2 Wijzigingen per document

2.1 Digikoppeling 2.0

2.1.1 Digikoppeling_2.0_Architectuur_v1.4.docx

#	Locatie	Oorspronkelijke tekst	Gewijzigd in	# RfC	Toelichting
1	7.2 p28	In Digikoppeling is ervoor gekozen om dat certificaat te gebruiken op het niveau van het communicatie KANAAL (TLS) en (nog) niet op het niveau van het BERICHT (XMLDsigof bijv. x509 token). Dit is in detail uitgewerkt in ' Digikoppeling Identificatie en Authenticatie'.	In Digikoppeling is ervoor gekozen om dat certificaat te gebruiken op het niveau van het communicatie KANAAL (TLS) en ook op het niveau van het BERICHT (XMLDsigof bijv. x509 token). Dit is in detail uitgewerkt in 'Digikoppeling Identificatie en Authenticatie' en 'Digikoppeling Beveiligingsstandaarden en voorschriften'.	4	
2	7.3 p28	Zowel de koppelvlakstandaard van ebMS als van WUS maken gebruik van TLS/SSL v3 (tweezijdig) voor encryptie van berichten. Als in de toekomst versleuteling van de payload opgenomen wordt in de standaarden, zal dat in beide gevallen gebeuren op basis van XML Encryption of mogelijke andere toekomstige standaarden.	Zowel de koppelvlakstandaard van ebMS als van WUS maken gebruik van TLS (tweezijdig) voor encryptie van berichten. Versleuteling van de payload is sinds Digikoppeling 2.0 opgenomen in de koppelvlakstandaarden op basis van XML Encryption of mogelijke andere toekomstige standaarden. Dit is in detail uitgewerkt in 'Digikoppeling Beveiligingsstandaarden en voorschriften'.	1, 4	

2.1.2 Digikoppeling_2.0_Koppelvlakstandaard_WUS_v2.7.docx

#	Locatie	Oorspronkelijke tekst	Gewijzigd in	# RfC	Toelichting
3	1.2p4		Standaardenplaat aangepast	4	
4	2.11p6 3.1p21 Bijl.1-4		De XML voorbeelden zijn verplaatst naar een nieuw nog te publiceren document	4	
5	2.3p11 2.4.4p16	Verwijzing naar specifieke TLS versies Voorschriften WT001, WT003	verwijzing naar [*Digikoppeling beveiligingsstandaarden en voorschriften*]	1	

#	Locatie	Oorspronkelijke tekst	Gewijzigd in	# RfC	Toelichting
6	2.4.4p16	Aangezien er meerdere WS-Addressing specificaties zijn, die onder meer verschillende namespaces kunnen hebben, is er voor gekozen om alleen de specificatie van 2005/08 (http://www.w3.org/TR/2005/CR-ws-addr-core-20050817/) of van 2006/05 (http://www.w3.org/TR/ws-addr-core/) verplicht te stellen in de berichten binnen het Digikoppeling domein. Hieronder wordt de toepassing van de verschillende velden toegelicht.	Aangezien er meerdere WS-Addressing specificaties zijn, die onder meer verschillende namespaces kunnen hebben, is er voor gekozen om alleen de specificatie van 2006/05 (http://www.w3.org/TR/ws-addr-core/) verplicht te stellen in de berichten binnen het Digikoppeling domein. Hieronder wordt de toepassing van de verschillende velden toegelicht.	4	verwijzing naar candidate recommendation verwijderd
7	2.4.2p17	WB007 Technische gegevens ten behoeve van ondertekenen: … DigestMethodAlgorithm SHA-1 (http://www.w3.org/2000/09/xmldsig#sha1) SignatureMethodAlgorithm SHA-1 (http://www.w3.org/2000/09/xmldsig#hmac-sha1 of http://www.w3.org/2000/09/xmldsig#rsa-sha1)	WB007 Technische gegevens ten behoeve van ondertekenen: … DigestMethodAlgorithm zie [*Digikoppeling beveiligingsstandaarden en voorschriften*] SignatureMethodAlgorithm zie [*Digikoppeling beveiligingsstandaarden en voorschriften*]	4, 5	Verplaatst naar *Digikoppeling beveiligingsstandaarden en voorschriften* verwijzingen naar SHA-1 vervangen door SHA-2
8		WB008 Technische gegevens ten behoeve van versleutelen: Data Encryption Algorithms 3DES (http://www.w3.org/2001/04/xmlenc#tripledes-cbc) of AES128 (http://www.w3.org/2001/04/xmlenc#aes128-cb) of AES256 (http://www.w3.org/2001/04/xmlenc#aes256-cbc) Key Transport Algorithms RSA-1_5 (http://www.w3.org/2001/04/xmlenc#rsa-1_5) of RSA-OAEP (http://www.w3.org/2001/04/xmlenc#rsa-oaep-mgf1p)	WB008 Technische gegevens ten behoeve van versleutelen: Data Encryption Algorithms zie [*Digikoppeling beveiligingsstandaarden en voorschriften* Key Transport Algorithms zie [*Digikoppeling beveiligingsstandaarden en voorschriften*] "	4	verplaatst naar *Digikoppeling beveiligingsstandaarden en voorschriften*

2.1.3 Digikoppeling_2.0_Koppelvlakstandaard_ebMS_v2.7.docx

#	Locatie	Oorspronkelijke tekst	Gewijzigd in	# RfC	Toelichting
9	1.2p5		Standaardenplaat aangepast	4	
10	2.5p12 4.2.3p37 4.2.6p38 4.11.4p6	Verwijzing naar specifieke TLS versies Voorschriften 4.2.3, 4.2.6, 4.11.4	verwijzing naar [*Digikoppeling beveiligingsstandaarden en voorschriften*]	1	
11	2.4p10 4.1.5p25 4.4.1p43	typo in naam 1.1.1 MessageId en RefTo1.1.1 MessageId	gewijzigd in MessageId, RefToMessageId	4	
12	4.1.5p25	[RFC 2822]	[RFC 5322]	4	
13	4.2.1p39	Payload confidentiality is optional. Whenever used, the	Payload confidentiality is optional.	4	FIPS 179 moet zijn FIPS 197

#	Locatie	Oorspronkelijke tekst	Gewijzigd in	# RfC	Toelichting
		[FIPS 179] standard (AES 256-cbc) is used by the [XML Encryption].	The [*Digikoppeling beveiligingsstandaarden en voorschriften*] describes what security standard must be used.		
14	4.2.1p33	Verwijzing naar SHA-1	verwijzing naar [*Digikoppeling beveiligingsstandaarden en voorschriften*]	5	verwijzingen naar SHA-1 vervangen door SHA-2
15	5.5p72	Message Payload and Flow Profile (zonder paragraaf aanduiding)	5.5 Message Payload and Flow Profile	4	paragraaf aanduiding (5.5) toegevoegd
16	6.1	Normative and Non Normative Referenties	Sommige niet meer gebruikte referenties verwijderd. Referenties bijgewerkt en paden aangepast	4	
17	4.1.8p28 4.1.8p29	Timestamps must include the 'Z' (UTC) identifier.	Requirement has been removed	2	Item is als leeg item gehandhaafd om doornummering niet om te gooien

2.1.4 Digikoppeling_2.0_Koppelvlakstandaard_GB_v1.4.docx

#	Locatie	Oorspronkelijke tekst	Gewijzigd in	# RfC	Toelichting
18	1.2p4		Standaardenplaat aangepast	4	
19	4.2p14 e.v.	Verwijzing naar specifieke TLS versies Voorschriften GB006, GB007	verwijzing naar [*Digikoppeling beveiligingsstandaarden en voorschriften*]	1	
20	5.1p18	Referenties	Sommige niet meer gebruikte referenties verwijderd. Referenties bijgewerkt en paden aangepast	4	

2.2 Digikoppeling 3.0

2.2.1 Digikoppeling_3.0_Koppelvlakstandaard_ebMS_v3.1.docx

#	Locatie	Oorspronkelijke tekst	Gewijzigd in	# RfC	Toelichting
20	1.2p5		Standaardenplaat aangepast	4	Plaat voor DK3
21	2.5p12 4.2.3p37 4.2.6p38 4.11.4p6	Verwijzing naar specifieke TLS versies Voorschriften 4.2.3, 4.2.6, 4.11.4	verwijzing naar [*Digikoppeling beveiligingsstandaarden en voorschriften*]	1	
22	2.4p10 4.1.5p25 4.4.1p43	typo in naam 1.1.1 MessageId en RefTo1.1.1 MessageId	gewijzigd in MessageId, RefToMessageId	4	
23	4.1.5p25	[RFC 2822]	[RFC 5322]	4	
24	4.2.1p39	Payload confidentiality is optional. Whenever used, the [FIPS 179] standard (AES 256-cbc) is used by the [XML Encryption].	Payload confidentiality is optional. The [*Digikoppeling beveiligingsstandaarden en voorschriften*] describes what security standard must be used.	4	FIPS 179 moet zijn FIPS 197
25	4.2.1p33	Verwijzing naar SHA-1	verwijzing naar [*Digikoppeling beveiligingsstandaarden en voorschriften*]	5	verwijzingen naar SHA-1 vervangen door SHA-2
26	5.5p72	Message Payload and Flow Profile (zonder paragraaf aanduiding)	5.5 Message Payload and Flow Profile	4	paragraaf aanduiding (5.5) toegevoegd
27	6.1	Normative and Non Normative Referenties	Sommige niet meer gebruikte referenties verwijderd. Referenties bijgewerkt en paden aangepast	4	
28	4.1.8p28	Timestamps must include the	Requirement has been removed	2	Item is als leeg item

#	Locatie	Oorspronkelijke tekst	Gewijzigd in	# RfC	Toelichting
	4.1.8p29	'Z' (UTC) identifier.			gehandhaafd om doornummering niet om te gooien

2.2.2 Digikoppeling_3.0_Koppelvlakstandaard_GB_v3.1.docx

#	Locatie	Oorspronkelijke tekst	Gewijzigd in	# RfC	Toelichting
29	1.2p4		Standaardenplaat aangepast	4	
30	4.2p14 e.v.	Verwijzing naar specifieke TLS versies Voorschriften GB006, GB007	verwijzing naar [*Digikoppeling beveiligingsstandaarden en voorschriften*]	1	
31	5.1p18	Referenties	Sommige niet meer gebruikte referenties verwijderd. Referenties bijgewerkt en paden aangepast	4	

2.2.3 Digikoppeling_3.0_Koppelvlakstandaard_WUS_v3.4.docx

#	Locatie	Oorspronkelijke tekst	Gewijzigd in	# RfC	Toelichting
32	1.2p4	Oude plaat	Standaardenplaat aangepast	4	
33	2.11p6 3.1p21 Bijl.1-4	XML voorbeelden	De XML voorbeelden zijn verplaatst naar een nieuw nog te publiceren document	4	
34	2.3p11 2.4.4p16	Verwijzing naar specifieke TLS versies Voorschriften WT001, WT003	verwijzing naar [*Digikoppeling beveiligingsstandaarden en voorschriften*]	1	
35	2.4.4p16	Aangezien er meerdere WS-Addressing specificaties zijn, die onder meer verschillende namespaces kunnen hebben, is er voor gekozen om alleen de specificatie van 2005/08 (http://www.w3.org/TR/2005/CR-ws-addr-core-20050817/) of van 2006/05 (http://www.w3.org/TR/ws-addr-core/) verplicht te stellen in de berichten binnen het Digikoppeling domein. Hieronder wordt de toepassing van de verschillende velden toegelicht.	Aangezien er meerdere WS-Addressing specificaties zijn, die onder meer verschillende namespaces kunnen hebben, is er voor gekozen om alleen de specificatie van 2006/05 (http://www.w3.org/TR/ws-addr-core/) verplicht te stellen in de berichten binnen het Digikoppeling domein. Hieronder wordt de toepassing van de verschillende velden toegelicht.	4	verwijzing naar candidate recommendation verwijderd
36	2.4.2p17	WB007 Technische gegevens ten behoeve van ondertekenen: … DigestMethodAlgorithm SHA-1 (http://www.w3.org/2000/09/xmldsig#sha1) SignatureMethodAlgorithm SHA-1 (http://www.w3.org/2000/09/xmldsig#hmac-sha1 of http://www.w3.org/2000/09/xmldsig#rsa-sha1)	WB007 Technische gegevens ten behoeve van ondertekenen: … DigestMethodAlgorithm zie [*Digikoppeling beveiligingsstandaarden en voorschriften*] SignatureMethodAlgorithm zie [*Digikoppeling beveiligingsstandaarden en voorschriften*]	4, 5	Verplaatst naar *Digikoppeling beveiligingsstandaarden en voorschriften* verwijzingen naar SHA-1 vervangen door SHA-2
37		WB008 Technische gegevens ten behoeve van versleutelen: Data Encryption Algorithms 3DES (http://www.w3.org/2001/04/xmlenc#tripledes-cbc) of AES128 (http://www.w3.org/2001/04/x	WB008 Technische gegevens ten behoeve van versleutelen: Data Encryption Algorithms zie [*Digikoppeling beveiligingsstandaarden en voorschriften]* Key Transport Algorithms zie [*Digikoppeling beveiligingsstandaarden en*	4	verplaatst naar *Digikoppeling beveiligingsstandaarden en voorschriften*

#	Locatie	Oorspronkelijke tekst	Gewijzigd in	# RfC	Toelichting
		mlenc#aes128-cb) of AES256 (http://www.w3.org/2001/04/xmlenc#aes256-cbc) Key Transport Algorithms RSA-1_5 (http://www.w3.org/2001/04/xmlenc#rsa-1_5) of RSA-OAEP (http://www.w3.org/2001/04/xmlenc#rsa-oaep-mgf1p)	*voorschriften*] "		
38	2.4.2/15	De wsa:To is van het type wsa:EndPointReferenceType en dient gevult te worden met een 'Adres' element.	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.	3	
39	2.4.2/15	De elementen wsa:To, wsa:ReplyTo en wsa:From zijn allen van de type 'wsa:EndPointReferenceType	De elementen wsa:ReplyTo en wsa:From zijn beiden van de type 'wsa:EndPointReferenceType'. Het EndPointReferenceType stelt enkel het element 'Address' verplicht. De overige velden van EndPointReferenceType zijn optioneel en zijn om compatibiteitsredenen niet toegestaan binnen Digikoppeling. Voor wsa:to komt deze restrictie dus te vervallen	3	
40	2.4.2/15	verwijzing naar candidate version verwijderd (https://www.w3.org/TR/2005/CR-ws-addr-core-20050817/)	https://www.w3.org/TR/ws-addr-core/	4	
41	2.4.3/16	idem	idem	4	
42	2.4.3	verwijzing naar SHA-1 en XMLDSIG	verwijderd en verplaatst naar *Digikoppeling beveiligingsstandaarden en voorschriften*	5	
43	2.4.3	SHA-1 (http://www.w3.org/2000/09/xmldsig#hmac-sha1 of http://www.w3.org/2000/09/xmldsig#rsa-sha1)	Verwijderd, vervangen door SHA-2 en verplaatst naar *Digikoppeling beveiligingsstandaarden en voorschriften*	5	
44	2.4.3	3DES (http://www.w3.org/2001/04/xmlenc#tripledes-cbc) of AES128 (http://www.w3.org/2001/04/xmlenc#aes128-cbc) of AES256 (http://www.w3.org/2001/04/xmlenc#aes256-cbc)	verwijderd en verplaatst naar *Digikoppeling beveiligingsstandaarden en voorschriften*	4,5	
44	2.4.3		Opgenomen als referenties: RSA-1_5 (http://www.w3.org/2001/04/xmlenc#rsa-1_5) of RSA-OAEP (http://www.w3.org/2001/04/xmlenc#rsa-oaep-mgf1p		

2.2.4 Digikoppeling_3.0_Architectuur_v1.3.docx

#	Locatie	Oorspronkelijke tekst	Gewijzigd in	# RfC	Toelichting
45		Geen inhoudelijke uitleg beveiliging/security/TLS/SHA/PKI/referenties	'Digikoppeling Beveiligingsstandaarden en voorschriften' en plaat met documenten aanpassen		

2.3 Digikoppeling 2.0 en 3.0

2.3.1 Digikoppeling_Identificatie_en_Authenticatie_v1.3.docx

NB: er is geen aparte RFC maar gaat om verouderde teksten die zijn geactualiseerd.

#	Locatie	Oorspronkelijke tekst	Gewijzigd in	# RfC	Toelichting
46	7.1/28	Zolang dat nog niet het geval is, zal voor gebruik op Digikoppeling de gewenste identiteit vastgelegd worden binnen Digikoppeling in het Digikoppeling Service Register.	Zolang dat nog niet het geval is, zal voor gebruik op Digikoppeling de gewenste identiteit vastgelegd worden binnen het OIN register, onderdeel van het Digikoppeling Service Register.	4	
47	Bijlage 1: WBP/17	bijlage WBP 1	verwijderd ivm verouderde en niet relevante tekst (WBP is gewijzigd)	4	
48	1.2/4	Dit document gaat over de bedrijfsarchitectuur.	Dit document gaat over de bedrijfsarchitectuur op landelijk niveau, en specifiek over de identificatie en authenticatie van organisaties	4	
49	1.3/4		Dit document is onderdeel van de Digikoppeling standaarden. (inclusief plaat)	4	
50	2.0/6	Als een overheidsorganisatie	Als een (overheids)organisatie	4	
51	2.0/6	NORA principe P5 stelt: Burgers, bedrijven en maatschappelijke instellingen beschikken over één identiteit die bruikbaar is voor alle contacten met organisaties in het publieke domein en die afhankelijk van de soort dienstverlening ook nodig is en gevraagd moet worden. Dit ongeacht de keuze voor een kanaal. Een en ander komt neer op één administratieve identiteit (één identificatienummer). Deze administratieve identiteit dient afgebeeld te worden op een (ook digitaal toepasbaar) identiteitsbewijs.	vervangen door AP37 (tabel)	4	
52	2.0/6	Dit principe moet ook van toepassing zijn op de overheidsorganisaties.	Dit principe is ook van toepassing op (overheids)organisaties.	4	
53	5.0/15	De inhoud van het NHR is (ten aanzien van overheidsorganisaties) nog onzeker.	De inhoud van het HR is door de Wet op het Handelsregister uitgebreid met rechtspersonen met een publieke taak.	4	
54	5.0/15	Het niveau rechtspersoon met als identificatienummer het Fi-nummer. Het NHR heeft aangegeven, dat dat niveau, en dus dat nummer, in principe het	Het niveau rechtspersoon met als identificatienummer het Rechtspersonen en Samenwerkingsverbanden Identificatie Nummer (RSIN).	4	

#	Locatie	Oorspronkelijke tekst	Gewijzigd in	# RfC	Toelichting
		meest geschikt is om voor identificatie op Digikoppeling te gebruiken.	Dit is inhoudelijk gelijk aan het Fiscaal-nummer. Het HR heeft aangegeven, dat dat niveau, en dus dat nummer, in principe het meest geschikt is om voor identificatie op Digikoppeling te gebruiken.		
55	Bijlage 1/17	Bijlage 1 WBP is vervallen	Nieuwe bijlage OIN en HRN)	4	
56	Bijlage 1/17	Logius maakt voor overheidsorganisaties primair gebruik van het fiscale nummer van de Belastingdienst dat ook is/wordt opgenomen in het NHR. In die gevallen waar een overheidsorganisatie nog geen fiscaal nummer heeft, kan worden uitgeweken naar alternatieven.	Logius maakt voor overheidsorganisaties primair gebruik van het RSIN uit het HR. In die gevallen waar een overheidsorganisatie nog geen RSIN heeft, kan worden uitgeweken naar alternatieven.	4	
57	Bijlage 1/17	Prefix 00000001 Fi-nummer van Belastingdienst (9 posities). Dit wordt het RSIN uit het NHR.	Prefix 00000001: RSIN uit het Handelsregister (9 posities)	4	
58	Bijlage 1/17	Prefix 00000005: Niet toegewezen (DigiD)	Prefix 00000005: Niet toegewezen	4	
59	Bijlage 1/17	Prefix 00000006: Reservering (vestigingsnummer KvK)	Prefix 00000006: Niet toegewezen	4	
60	Bijlage 1/17	Prefix 00000007: Niet toegewezen (BRIN)	Prefix 00000007: Gereserveerd voor BRIN	4	
61	Bijlage 1/17	Het Fi-nummer (RSIN) wordt opgegeven door de aanvrager en bij Belastingdienst (dan wel in het NHR) gecontroleerd door Logius	Het RSIN wordt opgegeven door de aanvrager en bij het HR gecontroleerd door Logius	4	

2.3.2 Digikoppeling_Gebruik_en_achtergrond_certificaten_v1.4.docx

#	Locatie	Oorspronkelijke tekst	Gewijzigd in	# RfC	Toelichting
62	1.2/4	Achtergrond Een belangrijk aspect voor beveiliging van Digikoppeling is de juiste identificatie, authenticatie en autorisatie van organisaties. Digikoppeling maakt hiervoor gebruik van een PKI-infrastructuur met certificaten. Voor Digikoppeling is daarbij gekozen om certificaten toe te passen die voldoen aan de eisen van PKIoverheid .	Achtergrond Een belangrijk aspect voor beveiliging van Digikoppeling is de juiste identificatie, authenticatie en autorisatie van organisaties. Voor Digikoppeling is daarbij gekozen om certificaten toe te passen die voldoen aan de eisen van PKIoverheid.	1	
63	1.4 (nieuw)/4		Wijzigingen tov versie 1.3.1	1	
64	1.6 (was 1.5)	Samenhang met andere documenten (tabel). Alle DK documenten plus PKIoverheid.	alinea verwijderd en hernoemd Referenties	1	
65	2	Ontwerpen van de aansluiting op Digikoppeling met een Digikoppeling adapter (hoofdstuk 2).	• Uitleg over PKIoverheid (hoofdstuk 2) • Ontwerpen van de aansluiting op Digikoppeling met een Digikoppeling adapter (hoofdstuk 3).	1	
66	2.2/7	Digikoppeling identificeert organisaties zoveel mogelijk in lijn met de Staatsalmanak.	Digikoppeling identificeert organisaties zoveel mogelijk aan de hand van OIN. Zie		

#	Locatie	Oorspronkelijke tekst	Gewijzigd in	# RfC	Toelichting
		Voor Digikoppeling is van belang of organisatie(onderdelen) taken hebben in een wettelijk kader en hun bestuurders tekenbevoegd zijn. Soms identificeert Digikoppeling daarom onderdelen van organisaties.	Digikoppeling Identificatie en Authenticatie.		
67	2.2/7	Voor de unieke identificatie en authenticatie van deze organisaties is er door PKIoverheid gekozen (zie PKIoverheid Programma van Eisen 3b) om het OIN toe te voegen aan een PKIoverheid certificaat in het zogenaamde Subject.serialNumber-veld.	Voor de unieke identificatie en authenticatie van deze organisaties wordt het OIN opgenomen in een PKIoverheid certificaat in het zogenaamde Subject.serialNumber-veld door de CSP. Voetnoot: Indien er sprake is van een twintigcijferig nummer is dit altijd het OIN (of HRN).		
68	nieuw hoofdstuk 2		nieuw hoofdstuk met Inleiding PKIoverheid certificaten		
69	nieuw hoofdstuk 2				
70	5.2 (was 4.2)/12	Achtergrond Beveiliging van de privésleutel kan plaatsvinden door deze op een smartcard (in PKI-termen een Secure User Device of afgekort SUD) te plaatsen. Een dergelijke fysieke beveiliging wordt vaak gecombineerd met een userid/password. Als alternatief kan de privésleutel ook in een password-beveiligde keystore opgeslagen worden. De eerste optie (SUD) heeft de voorkeur van PKIoverheid. Er zijn extra maatregelen nodig als er geen SUD gebruikt wordt. Het programma van eisen dat PKIoverheid aan CSP's oplegt bevat de verplichting aan CSP's om over de juiste beveiliging van sleutels door gebruikers te waken inclusief de mogelijkheid tot audit (zie kader).	staat niet meer in PvE van PKIoverheid dus alinea en kader zijn verwijderd. Kader verwees naar een oude versie van PvE van PKIo en is in zijn geheel verwijderd.		
71	7.3.2/21		Nieuw: 7.3.2 TLS Offloading Door het gebruik van TLS offloading zijn er minder afhankelijkheden van certificaten in CPA's. Daardoor kan de geldigheid van een CPA langer zijn dan de geldigheid van het certificaat. Voorbeeld van hoe certificaat gegevens doorgegeven kunnen worden.		
72	Bijlage 4		Verplaats naar Digikoppeling Identificatie en Authenticatie		
73	1.2/4	Achtergrond Een belangrijk aspect voor beveiliging van Digikoppeling is	Achtergrond Een belangrijk aspect voor beveiliging van Digikoppeling is		

#	Locatie	Oorspronkelijke tekst	Gewijzigd in	# RfC	Toelichting
		de juiste identificatie, authenticatie en autorisatie van organisaties. Digikoppeling maakt hiervoor gebruik van een PKI-infrastructuur met certificaten. Voor Digikoppeling is daarbij gekozen om certificaten toe te passen die voldoen aan de eisen van PKIoverheid .	de juiste identificatie, authenticatie en autorisatie van organisaties. Voor Digikoppeling is daarbij gekozen om certificaten toe te passen die voldoen aan de eisen van PKIoverheid . .		

2.3.3 Digikoppeling_Beheermodel_v1.4.docx

#	Locatie	Oorspronkelijke tekst	Gewijzigd in	# RfC	Toelichting
74		Geen inhoudelijke uitleg beveiliging/security/TLS/SHA/PKI/ referenties	'Digikoppeling Beveiligingsstandaarden en voorschriften' en plaat met documenten aanpassen		

2.3.4 Digikoppeling_beveiligingsstandaarden_en_voorschriften_v2.docx

Dit is een nieuw document met de verplichte Digikoppeling beveiligingsstandaarden en voorschriften, dat onderdeel wordt van de standaard. Zie bovenstaande wijzigingen voor RFCs 1, 4 en 5.