Release Notes Wijziging Digikoppeling Standaarddocumentatie

17-12-2019

1 Overzicht van de wijzigingen

1.1 Achtergrond

NCSC heeft beveiligingsrichtlijnen voor TLS uitgebracht (ICT Beveiligingsrichtlijnen voor Transport Layer Security (TLS) versie 2.0). In deze release van de Digikoppeling standaard zijn de Digikoppeling beveiligingsstandaarden en voorschriften bijgewerkt conform deze nieuwe NCSC richtlijnen en adviezen. Daarnaast is ook het onderdeel XML encryption in het voorschrift geactualiseerd en voorzien van meer toelichting.

1.2 Gewijzigde documenten

De volgende documenten zijn gewijzigd:

Digikoppeling	actuele versie	vorige versie
Digikoppeling Beveiligingsstandaarden en Voorschriften	1.2	1.1
Digikoppeling Overzicht Actuele Documentatie en Compliance	1.4	1.3

1.3 Wijzigingen per document

Digikoppeling_Beveiligingsstandaarden_en_voorschriften_v1.2

#	Locatie	Oorspronkelijke tekst	Gewijzigd in	# RfC	Toelichting
	4.1	TLS 1.2 (RFC5246) Verplicht	TLS 1.2 (RFC5246) Verplicht(*) TLS 1.3 (RFC8446) Optioneel(*)	NCSC	
1	4.2 p11	TLS003 De TLS implementatie mag niet op SSL v3 terug kunnen vallen. Backward compatibility mode voor SSL3 dient te worden uitgezet.	TLS003 De TLS implementatie mag niet op SSL v3 en eerdere versies terugvallen Backward compatibility mode voor SSL v3 en eerdere versies dient te worden uitgezet.	NCSC	
2	4.2 p11	TLS004 TLS 1.0 en TLS 1.1 zijn niet meer toegestaan Niet meer toegestaan vanaf 10-9-2016	TLS004 Een Serviceaanbieder is verplicht TLS versie 1.2 te ondersteunen, daarnaast is het aanbevolen voor een Serviceaanbieder om TLS versie 1.3 te ondersteunen. Als een Serviceaanbieder TLS versie 1.3 aanbiedt dan is het aanbevolen voor Serviceafnemers om TLS 1.3 te gebruiken NCSC geeft aan: "De beste bescherming wordt momenteel geboden door de meest	NCSC	

			recente TLS versie: TLS 1.3" Zie [NCSC ICT-beveiligingsrichtlijnen voor TLS] TLS 1.0 en TLS 1.1 zijn niet meer toegestaan Niet meer toegestaan binnen de Digikoppeling standaard vanaf 10-9-2016		
3	4.2 p11	TLS005 Voor communicatie over HTTPS wordt port 443 gebruikt.	TLS005 Het is verplicht voor communicatie over HTTPS port 443 te gebruiken Port 443 is standaard poort voor HTTPS verkeer	NCSC	
4	4.2 p11	(geen)	TLS006 Het is verplicht te voldoen aan de NCSC ICT-beveiligingsrichtlijnen voor TLS	NCSC	
5	5.1.1 p12	TLSCIPH001 Minimaal verplicht De onderstaande TLS encryptie algoritmen en sleutellengtes MOETEN minimaal worden ondersteund: •TLS_RSA_WITH_AES_256_CBC_SHA •TLS_RSA_WITH_AES_128_CBC_SHA	TLSCIPH001 De gebruikte TLS cryptografische algoritmen moeten de NCSC classificatie 'voldoende' of 'goed' hebben. TLS cryptografische algoritmen met de NCSC classificatie 'uit te faseren' dienen zo spoedig mogelijk maar uiterlijk 01-01-2021 te worden uitgefaseerd.	NCSC	
6	5.1.1	TLSCIPH002 Sterk aanbevolen Ondersteuning van de volgende aanvullende algoritmen en sleutellengtes wordt sterk aanbevolen om interoperabiliteit en veiligheid in de toekomst zeker te stellen: •TLS_RSA_WITH_AES_256_CBC_SHA256 •TLS_RSA_WITH_AES_128_CBC_SHA256	Vervalt	NCSC	
9	5.3.1	ENC003 (oorspronkelijke tekst vervalt)			
10		ENC004 De ondersteunde data encryption (data versleuteling) algoritmen zijn: [3DES] of [AES128] of [AES256] [XML Encryption]	ENC003 De ondersteunde data encryption (data versleuteling) algoritmen zijn: 3DES AES128 AES256 [XML Encryption]	XML encryption	Nummering Aangepast

		(Gebruik GCM mode indien beschikbaar anders CBC mode in combinatie met een signature) [AES128-CBC], [AES128-GCM], [AES256-CBC], [AES256-GCM]	
1 **1**	ENC005 Het Key transport algorithm maakt gebruik van de RSA1_5 of RSA-OAEP algorithmen. [RSA1_5] [RSA-OAEP] [XML Encryption]	ENC004 Het Key transport algorithm maakt gebruik van de RSA-OAEP algoritmen. [RSA-OAEP] [XML Encryption]	XML encryption

1.4 Overzicht releases

Document	Normatief	Release 23-07-2018	Release 21-08-2018	Release 16-05-2019	Release 17-12-2019
Wat is Digikoppeling		1.1.1	1.1.1.	1.1.1	1.1.1
DK Beheermodel en releasebeleid		1.5	1.5	1.5	1.5
DK Architectuur	X	1.5.1	1.5.1	1.51	1.51
DK Koppelvlakstandaard WUS	X	3.5	3.6	3.7	3.7
DK Koppelvlakstandaard EBMS2	X	3.2	3.2	3.3	3.3
DK Koppelvlakstandaard Grote Berichten	X	3.2	3.2	3.2	3.2
DK Identificatie en Authenticatie	X	1.4	1.4	1.4	1.4
DK Beveiliging standaarden en voorschriften	X	1.1	1.1	1.1	1.2
DK Overzicht Actuele Documentatie en Compliance	X	1.1	1.2	1.3	1.4
DK Best Practices WUS		1.10	1.10	1.10	1.10
DK Best Practices EBMS2		3.1	3.1	3.2	3.2
DK Best Practices Grote Berichten		3.1	3.1	3.1	3.1
DK Gebruik en achtergrond certificaten		1.5	1.5	1.5	1.5

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