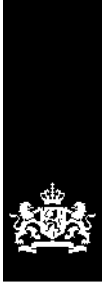


Ministerie van Binnenlandse Zaken en Koninkrijksrelaties

Digikoppeling beveiligingsstandaarden en voorschriften

Versie 1.2

Datum 17-12-2019
Status Definitief

Inhoud

1 Inleiding 5

1.1 Doel en Doelgroep 5

1.2 Digikoppeling 5

1.3 Digikoppeling standaarden 6

2 Identificatie 7

2.1 Wat is identificatie? 7

2.2 Identificerend nummer 7

3 PKIoverheid certificaten 8

3.1 Standaarden 8

3.2 Wat is PKIoverheid? 8
3.2.1 PKIoverheid 8
3.2.2 PKIoverheid certificaat 8

3.3 Voorschriften 8
3.3.1 Digikoppeling voorschriften 8
3.3.2 PKIoverheid programma van eisen 9
3.3.3 Geldigheid 10

3.4 Best practices 10

4 TLS 11

4.1 Standaarden 11

4.2 Digikoppeling voorschriften 11

4.3 Onderbouwing 12

4.4 Overwegingen 12

5 Cipher suites voor TLS, signing en encryptie 13

5.1 TLS Ciphersuites 13

5.2 XML Signing 13
5.2.1 Digikoppeling voorschriften voor XML signing 13
5.2.2 Reden voor vervanging SHA-1 door SHA-2 13

5.3 XML Encryptie 15
5.3.1 Digikoppeling voorschriften voor payload encryptie 15

6 Referenties 16

6.1 Normatieve referenties 16

6.2 Niet-normatieve referenties 17
6.2.1 Block ciphers 17
6.2.2 Secure Hash Standard (FIPS 180-4) 17
6.2.3 Gebruik en achtergronden Digikoppeling certificaten 17
6.2.4 Uitschakelen SSLen upgrade open SSL 17
6.2.5 HTTPS factsheet 17

6.2.6 Digikoppeling Identificatie en Authenticatie 17
6.2.7 Digikoppeling Architectuur..... 17

Colofon

Logius Servicecentrum:
Postbus 96810
2509 JE Den Haag

t. 0900 555 4555 (10 ct p/m)
e. servicecentrum@logius.nl

Documentbeheer

Datum	Versie	Auteur	Opmerkingen
04/04/2016	1.0	Logius	Nieuwe standaarddocument
12/10/2017	1.1	Logius	CSP hernoemd naar TSP Opmerkingen over migratie TLS verwijderd
17/12/2019	1.2	Logius	Aanpassing n.a.v. NCSC TLS Richtlijnen versie 2.0

1 Inleiding

1.1 Doel en Doelgroep

Dit document beschrijft de eisen die Digikoppeling stelt aan de beveiliging van de berichtuitwisseling.

Dit document is bestemd voor architecten en ontwikkelaars van applicaties die gebruik maken van Digikoppeling om berichten tussen systemen veilig uit te wisselen.

Alle Digikoppeling webservices die op WUS of ebMS2 gebaseerd zijn, moeten conformeren aan deze Digikoppeling beveiligingsstandaarden en voorschriften. Deze wordt in dit document gespecificeerd.

Doel van dit document is ontwikkelaars te informeren wat deze beveiligingsvoorschriften precies inhouden, welke standaarden en welke versies toegestaan zijn en partijen zich aan moeten conformeren.

1.2 Digikoppeling

Deze paragraaf bevat zeer beknopt een aantal hoofdpunten uit de overige documentatie.
Digikoppeling biedt de mogelijkheid om op een sterk gestandaardiseerde wijze berichten uit te wisselen tussen serviceaanbieders (service providers) en serviceafnemers (service requesters of consumers).

De uitwisseling tussen service providers en requesters wordt in drie lagen opgedeeld:

- Inhoud: op deze laag worden de afspraken gemaakt over de inhoud van het uit te wisselen bericht, dus de structuur, semantiek, waardebereiken etc.
  Digikoppeling houdt zich niet met de inhoud bezig, 'heeft geen boodschap aan de boodschap'.
- Logistiek: op deze laag bevinden zich de afspraken betreffende transportprotocollen (HTTP & TLS), messaging (SOAP), beveiliging (authenticatie en encryptie) en betrouwbaarheid. Dit is de laag van Digikoppeling.
- Transport: deze laag verzorgt het daadwerkelijke transport van het bericht (TCP/IP).

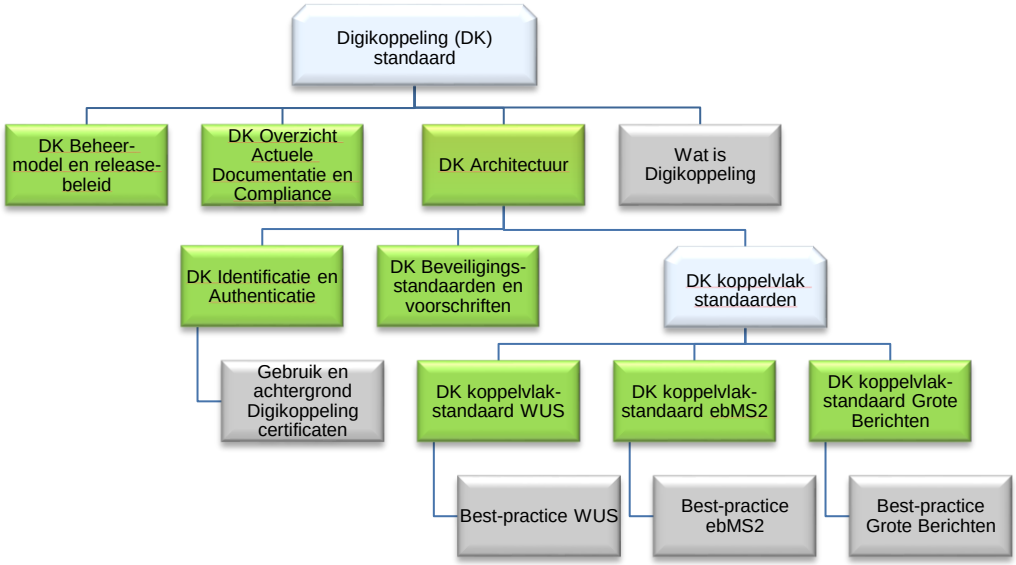
Digikoppeling richt zich dus uitsluitend op de logistieke laag. Deze afspraken komen in de koppelvlakstandaarden en andere voorzieningen.

De koppelvlakstandaarden dienen te leiden tot een maximum aan interoperabiliteit met een minimum aan benodigde ontwikkelinspanning. Daarom is gekozen voor bewezen interoperabele internationale standaarden.

Digikoppeling maakt berichtenuitwisseling mogelijk op basis van de ebXML/ebMS2 en WS* families van standaarden inclusief de daarbij behorende verwante standaarden.

1.3 Digikoppeling standaarden

De Digikoppeling standaarden bestaan uit de volgende documenten (groene blokken zijn onderdeel van de Digikoppeling standaard):



Figuur 1 Overzicht van de Digikoppeling standaard.

Specificatie van de koppelvlakstandaarden
De koppelvlakspecificatie beschrijft de eisen die gesteld worden aan de adapters om interoperabel met elkaar te kunnen communiceren. Digikoppeling gaat over logistiek, dus over de envelop en niet over de inhoud. De hele set informatie die tezamen nodig is voor een complete generieke Digikoppeling koppelvlakdefinitie bestaat uit:

- Interfacedefinitie WUS of ebMS2 met SOAP headers en informatie over velden en hun specifieke inhoud.
- Beveiligingsvoorschriften en standaarden voor de transport laag, signing en encryptie (cipher suites).

2 Identificatie

2.1 Wat is identificatie?

Een goede beveiliging van het berichtenverkeer begint met de identificatie van de partijen en de systemen waarmee zij berichten met elkaar uitwisselen. Identificatie houdt in dat de identiteit van de niet-natuurlijke persoon (organisatie) met grote zekerheid wordt vastgesteld.

De Digikoppeling standaarden schrijven voor hoe de berichtuitwisseling tussen systemen van verschillende organisaties plaats moet vinden. Deze organisaties en systemen worden geauthenticeerd aan de hand van een PKIoverheid certificaat met daarin een uniek identificerend nummer, het OIN.

2.2 Identificerend nummer

Het organisatie identificatienummer (OIN) is het identificerende nummer voor organisaties die gebruik maken van Digikoppeling. De partijen identificeren elkaar op basis van dit nummer.

De bron voor identificatie van organisaties is een erkend register dat is opgenomen in het OIN beleid. In de meeste gevallen is dit het Handelsregister. Het OIN kan worden opgezocht in het OIN Register.

Zie *Digikoppeling Identificatie en Authenticatie* voor meer informatie.
Het OIN register is bereikbaar op *https://portaal.digikoppeling.nl* .

3 PKIoverheid certificaten

3.1 Standaarden

Standaarden	Status	Genoemd in
PKIoverheid certificaten & CRL Profile	Verplicht	PKIoverheid Programma van Eisen

3.2 Wat is PKIoverheid?

3.2.1 PKIoverheid

PKIoverheid is de public key infrastructure in Nederland waarmee PKIoverheid certificaten worden uitgegeven en toegepast conform afspraken die zijn vastgelegd in het PKIoverheid Programma van Eisen. Zie ook het document *'Gebruik en achtergronden Digikoppeling certificaten'* en www.logius.nl/pkioverheid

3.2.2 PKIoverheid certificaat

Digitale certificaten zijn een onmisbare schakel in beveiligd internetverkeer. Een certificaat is een legitimatiebewijs van een website of ICT-systeem. Daarnaast bevat het gegevens die nodig zijn voor beveiligd internetverkeer.[1]

Digikoppeling vereist dat de communicatiepartners PKIoverheid certificaten gebruiken met een OIN om op een vertrouwelijke wijze gegevens uit te wisselen.

3.3 Voorschriften

3.3.1 Digikoppeling voorschriften

Nr	Voorschrift	Toelichting
PKI001	Gebruik OIN in subject serial number veld is verplicht	Dit is afgesproken met de TSPs in de Digikoppeling Overeenkomsten. Zij verstrekken PKIoverheid certificaten met het OIN in het subject.serialnumber field conform de OIN systematiek als het een certificaat betreft dat voor Digikoppeling wprdt gebruikt.
PKI002	PKIoverheid certificaat moet geldig zijn (het mag niet zijn verlopen of ingetrokken)	
PKI003(WT004)	De geldigheid van het certificaat wordt getoetst met betrekking tot de geldigheidsdatum en de Certificate	

[1] Bron: https://www.logius.nl/diensten/pkioverheid/

	Revocation List(CRL) die voldoet aan de eisen van PKI-overheid.
PKI004 (WT005)	De betreffende CRL dient zowel voor de versturende als ontvangende partij te benaderen zijn.

3.3.2 PKIoverheid programma van eisen

1. Een PKIoverheid certificaat dient conform de eisen van het PKIoverheid PvE te worden uitgegeven door de Trust Service Providers (TSP).

2. De te gebruiken certificaten in de productie omgeving voldoen aan de eisen van PKIoverheid (PvE 3b) en de inhoud van de identificerende velden in het certificaat dienen te voldoen aan de afspraken zoals gesteld in de functionele eisen in het document [Digikoppeling Identificatie en Authenticatie]. Met het toepassen van PKIoverheid-certificaten die Digikoppeling compliant zijn, wordt hieraan voldaan.

3. Certificaten voor productie wijken af van certificaten voor test doordat zij op verschillende 'roots' zijn gebaseerd, respectievelijk 'PKI root Staat der Nederlanden' en 'PKI TRIAL root'.

De volgende eisen uit het [PvE PKIoverheid] (deel 3b) zijn van toepassing op certificaatgebruikers:

RFC	Nr PvE	Eis
RFC 3647	4.5.2 Gebruik van publieke sleutel en certificaat door vertrouwende partij 4.5.2-pkio51	In de gebruikersvoorwaarden die aan de vertrouwende partijen ter beschikking worden gesteld dient te worden opgenomen dat de vertrouwende partij wordt geacht de geldigheid te controleren van de volledige keten van certificaten tot aan de bron (stamcertificaat) waarop wordt vertrouwd. Daarnaast dient te worden opgenomen dat de abonnee zelf zorg draagt voor een tijdige vervanging in het geval van een naderende afloop geldigheid, en noodvervanging in geval van compromittatie en/of andere soorten van calamiteiten met betrekking tot het certificaat of van bovenliggende certificaten. Van de abonnee wordt verwacht dat hij zelf adequate maatregelen neemt om de continuïteit van het gebruik van certificaten te borgen.
	Opmerking	De geldigheid van een certificaat zegt niets over de bevoegdheid van de certificaathouder een bepaalde transactie namens een organisatie c.q. uit hoofde van zijn of haar beroep te doen. De PKI voor de overheid regelt geen autorisatie; daarvan moet een vertrouwende partij zichzelf op andere wijze overtuigen.
RFC 3647	4.9.2 Wie mag een verzoek tot intrekking doen 4.9.2-pkio53	De volgende partijen mogen in een verzoek tot intrekking van een eindgebruikercertificaat doen: • de certificaatbeheerder; • de certificaathouder; • de abonnee;

RFC	Nr PvE	Eis
		• de TSP; ieder andere, naar het oordeel van de TSP, belanghebbende partij/persoon.
RFC 3647	4.9.6 Controlevoorwaarden bij raadplegen certificaat statusinformatie	Een eindgebruiker die de certificaat statusinformatie raadpleegt, dient de authenticiteit van deze informatie te verifiëren door de elektronische handtekening waarmee de informatie is getekend en het bijbehorende certificatiepad te controleren.
RFC 3647	4.9.9 Online intrekking/statuscontrole	Ter verbijzondering van het in {16} IETF RFC 2560 gestelde is het gebruikt van vooraf berekende OCSP responses (precomputed responses) niet toegestaan.

3.3.3 Geldigheid

De geldigheid van het certificaat wordt getoetst met betrekking tot de geldigheidsdatum en de Certificate Revocation List(CRL) die voldoet aan de eisen van PKI-overheid. Zie eis PKI002 en PKI003

De betreffende CRL dient zowel voor de versturende als ontvangende partij te benaderen zijn. Zie eis PKI004 (WT005)

Een certificaat dient te worden ingetrokken als de organisatie niet meer bestaat of als de private sleutel gecompromitteerd is.

3.4 Best practices

De best practices voor inrichting en gebruik zijn beschreven in *Gebruik en achtergronden Digikoppeling certificaten*.

4 TLS

4.1 Standaarden

Standaarden	Status	Bron
TLS 1.2 (RFC5246) TLS 1.3 (RFC8446)	Verplicht(*) Optioneel(*)	NCSC NCSC
HTTP over TLS Transport Layer Security (RFC2818, RFC5785, RFC7230)	Informational	IETF

4.2 Digikoppeling voorschriften

Nr	Voorschrift	Toelichting
TLS001	Authenticatie is verplicht met TLS en PKIoverheid certificaten	
TLS002	Tweezijdig TLS is verplicht	Digikoppeling schrijft het gebruik van twee-zijdig TLS voor en verplicht dit voor alle vormen van berichtuitwisseling via Digikoppeling.
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.
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 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
TLS005	Het is verplicht voor communicatie over HTTPS port 443 te gebruiken	Port 443 is de standaard poort voor HTTPS verkeer
TLS006	Het is verplicht te voldoen aan de NCSC ICT-beveiligingsrichtlijnen voor TLS	Zie H3 van [NCSC ICT-beveiligingsrichtlijnen voor TLS]

4.3 Onderbouwing

Zowel de Digikoppeling-koppelvlakstandaard ebMS2 als de Digikoppeling-koppelvlakstandaard WUS en Digikopppeling-koppelvlakstandaard Grote Berichten schrijven het gebruik voor van (tweezijdig) TLS om de berichtenstroom te beveiligen. Het protocol TLS heeft betrekking op het communicatiekanaal. De Digikoppeling-koppelvlakstandaarden stellen deze eis dus aan de transportlaag en aan de authenticatie van organisaties.

In Digikoppeling is ervoor gekozen om PKIoverheid certificaten te gebruiken op het niveau van het communicatiekanaal (TLS) om de directe communicatiepartners te authenticeren. TLS kan niet toegepast worden om end-to-end authenticatie uit te voeren in een multi-hop (voor ebMS2) omgeving; zie daarvoor berichtniveau beveiliging in de [Digikoppeling Architectuur] documentatie.

4.4 Overwegingen

Het NCSC adviseert om TLS altijd te configureren op basis van de [ICT-beveiligingsrichtlijnen voor Transport Layer Security].

5 Cipher suites voor TLS, signing en encryptie

5.1 TLS Ciphersuites

Nr	Voorschrift	Toelichting
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.	Zie [ICT-beveiligingsrichtlijnen voor TLS] van NCSC

5.2 XML Signing

5.2.1 Digikoppeling voorschriften voor XML signing

Nr	Voorschrift	Toelichting
SIGN001	Signing met SHA-2 is verplicht.	Minimaal SHA-224 of SHA-256.
SIGN002	Signing conform XMLDSIG is verplicht	Zie de koppelvlakstandaarden signed profielen
SIGN003	Het DigestMethod Algorithm moet gebruik maken van een van de volgende algoritmen: [SHA-224] [SHA-256] [SHA-384] [SHA-512]	Zie ook de koppelvlakstandaard WUS Zie ook https://www.w3.org/TR/xmldsig-core1/#sec-DigestMethod Zie Normatieve referenties in 6.1
SIGN004	Het SignatureMethod Algorithm kan gebruik maken van een van de volgende algoritmen: [SHA-224] [SHA-256] [SHA-384] [SHA-512]	Zie ook de koppelvlakstandaard WUS Zie ook https://www.w3.org/TR/xmldsig-core1/#sec-DigestMethod voor voorbeelden Zie Normatieve referenties in 6.1

5.2.2 Reden voor vervanging SHA-1 door SHA-2

Certificaten met SHA-1 als hashfunctie worden vervangen door certificaten met hashfuncties uit de SHA-2-familie: SHA-256, SHA-384 en SHA-512. Certificaten met MD5 als hashfunctie zijn enkele jaren geleden al vervangen. MD5 is de voorloper van SHA-1. [HTTPS- factsheet NCSC]

PKIoverheid stelt SHA-2 als eis. Alle certificaten die onder de root Staat der Nederlanden worden uitgegeven moeten voldoen aan SHA-2. In de [ICT beveiligingsrichtlijnen voor TLS] van het NCSC wordt SHA-1 nog wel als 'voldoende' bestempeld voor hashing binnen een applicatie, maar voor signing is het onvoldoende.

In plaats daarvan is het dus wenselijk om gebruik te maken van een algoritme dat als ‘goed’ is aangemerkt, dus:

- SHA-512,
- SHA-384 of
- SHA-256

5.3 XML Encryptie

5.3.1 Digikoppeling voorschriften voor payload encryptie

Nr	Voorschrift	Toelichting
ENC001	Indien er gebruik wordt gemaakt van XML encryption op payload niveau dient de FIPS 197 standaard (AES) te worden gebruikt.	[FIPS 197]
ENC002	Encryptie conform XML versleuteling [XML Encryption] is verplicht (http://www.w3.org/TR/xmlenc-core/)	[XML Encryption]
ENC003	De ondersteunde data encryption (data versleuteling) algoritmen zijn: 3DES AES128 AES256	[XML Encryption] (Gebruik GCM mode indien beschikbaar anders CBC mode in combinatie met een signature) [AES128-CBC], [AES128-GCM], [AES256-CBC], [AES256-GCM]
ENC004	Het Key transport algorithm maakt gebruik van de RSA-OAEP algoritmen.	[RSA-OAEP] [XML Encryption]

6 Referenties

6.1 Normatieve referenties

De normatieve referenties zijn de verplichte standaarden waar Digikoppeling aan refereert. Voor de juiste uitleg van deze standaarden verwijzen wij naar de vindplaats van de gehanteerde standaard.

[FIPS 180-4] Announcing Approval of Federal Information Processing Standard (FIPS) Publication 180–4, Secure Hash Standard, a Revision of FIPS 180–3, Secure Hash Standard. URL http://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.180-4.pdf

[FIPS 197] NIST FIPS 197. Advanced Encryption Standard (AES). URL http://csrc.nist.gov/publications/fips/fips197/fips-197.pdf. of http://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.197.pdf

[ICT beveiligingsrichtlijnen voor TLS] ICT-beveiligingsrichtlijnen voor Transport Layer Security (TLS) (versie 2.0) https://www.ncsc.nl/documenten/publicaties/2019/mei/01/ict-beveiligingsrichtlijnen-voor-transport-layer-security-tls

[PKI-CA] PKI Overheid toegetreden certificatiehouders. URL https://www.logius.nl/ondersteuning/pkioverheid/aansluiten-als-tsp/toegetreden-tsps/

[PKI-PvE] PKI Overheid Programma van Eisen Deel 3b. URL https://www.logius.nl/ondersteuning/pkioverheid , zoekterm “deel 3b”.

[RFC 3447] Public-Key Cryptography Standards (PKCS) #1: RSA Cryptography Specifications Version 2.1, FEBRUARY 2003 http://www.ietf.org/rfc/rfc3447.txt.
[RFC 3447] vervangt [RFC 2437] die niet meer geldig is.

[RFC 5322] Internet Message Format. IETF RFC 5322. http://www.ietf.org/rfc/rfc5322.txt.

[XMLDSIG] Joint W3C/IETF XML-Signature Syntax and Processing specification. http://www.w3.org/TR/2002/REC-xmldsig-core-20020212/. NB: *FIPS-180-3 is vervangen door FIPS 180-4. XMLDSIG verwijst nog naar FIPS 180-3.*

[XML Encryption] XML Encryption Syntax and Processing. W3C Recommendation. http://www.w3.org/TR/xmlenc-core/ beschrijft de volgende algoritmen:

- **[RSA1_5]** http://www.w3.org/2001/04/xmlenc#rsa-1_5
- **[RSA-OAEP]** http://www.w3.org/2001/04/xmlenc#rsa-oaep-mgf1p
- **[SHA-2]** http://www.ietf.org/rfc/rfc4051.txt
- **[SHA-224]** http://www.w3.org/2001/04/xmldsig-more#sha224
- **[SHA-256]** http://www.w3.org/2001/04/xmlenc#sha256
- **[SHA-384]** http://www.w3.org/2001/04/xmldsig-more#sha384

- **[SHA-512]** http://www.w3.org/2001/04/xmlenc#sha512
- **[3DES]** http://www.w3.org/2001/04/xmlenc#tripledes-cbc
- **[AES128-CBC]** http://www.w3.org/2001/04/xmlenc#aes128-cbc
- **[AES128-GCM]** http://www.w3.org/2009/xmlenc11#aes128-gcm
- **[AES256-CBC]** http://www.w3.org/2001/04/xmlenc#aes256-cbc
- **[AES256-GCM]** http://www.w3.org/2009/xmlenc11#aes256-gcm

6.2 Niet-normatieve referenties

De volgende referenties zijn hier opgenomen als bron maar zijn geen onderdeel van de door Digikoppeling vereiste standaarden.

6.2.1 Block ciphers

NCSC onderkent zowel AES als triple DES (block ciphers) als encryptie algoritmen. Deze laatste zijn hier opgenomen:

[TDEA] NIST Special Publication 800-67 Revision 1 *Recommendation for the Triple Data Encryption Algorithm (TDEA) Block Cipher*

[BLOCK] NIST Cryptographic Toolkit: Block Ciphers, http://csrc.nist.gov/groups/ST/toolkit/block_ciphers.html

6.2.2 Secure Hash Standard (FIPS 180-4)

FIPS 180-4 on the CSRC FIPS publications page: http://csrc.nist.gov/publications/PubsFIPS.html#180-4

6.2.3 Gebruik en achtergronden Digikoppeling certificaten

Beschrijft het correcte gebruik en installatie van certificaten t.b.v. Digikoppeling.

6.2.4 Uitschakelen SSLen upgrade open SSL

https://www.ncsc.nl/actueel/nieuwsberichten/ncsc-publiceert-nieuw-factsheet-schakel-ssl-2.0-uit-en-upgrade-openssl.html

6.2.5 [HTTPS- factsheet NCSC] HTTPS factsheet

https://www.ncsc.nl/actueel/factsheets/factsheet-https-kan-een-stuk-veiliger.html

6.2.6 Digikoppeling Identificatie en Authenticatie

Dit document is onderdeel van de Digikoppeling standaard. https://www.logius.nl/standaarden/digikoppeling/architectuur-en-koppelvlakstandaarden/

6.2.7 Digikoppeling Architectuur

Dit document is onderdeel van de Digikoppeling standaard. https://www.logius.nl/standaarden/digikoppeling/architectuur-en-koppelvlakstandaarden/