

# Digikoppeling Beveiligingstandaarden en voorschriften 3.0.1



Logius Standaard

Vastgestelde versie 21 april 2026

**Deze versie:**

<https://gitdocumentatie.logius.nl/publicatie/dk/beveilig/3.0.1/>

**Laatst gepubliceerde versie:**

<https://gitdocumentatie.logius.nl/publicatie/dk/beveilig/>

**Laatste werkversie:**

<https://logius-standaarden.github.io/Digikoppeling-Beveiligingsstandaarden-en-voorschriften/>

**Vorige versie:**

<https://gitdocumentatie.logius.nl/publicatie/dk/beveilig/2.0.1/>

**Redacteurs:**

[Peter Haasnoot](#) (Logius)

[Nil Barua](#) (Logius)

**Auteur:**

[Pieter Hering](#) (Logius)

**Doe mee:**

[GitHub Logius-standaarden/Digikoppeling-Beveiligingsstandaarden-en-voorschriften](#)

[All issues](#)

[Dien een melding in](#)

[Revisiehistorie](#)

[Pull requests](#)

Dit document is ook beschikbaar in dit niet-normatieve formaat: [PDF](#)



Dit document valt onder de volgende licentie:

[Creative Commons Attribution 4.0 International Public License](#)

## Status van dit document

Dit is de definitieve versie van dit document. Wijzigingen naar aanleiding van consultaties zijn doorgevoerd.

# Inhoudsopgave

## **Status van dit document**

## **Conformiteit**

## **Samenvatting**

## **Documentbeheer**

## **Colofon**

### **1. Inleiding**

- 1.1 Doel en Doelgroep
- 1.2 Digikoppeling
- 1.3 Digikoppeling standaarden

### **2. Identificatie**

- 2.1 Wat is identificatie?
- 2.2 Identificerend nummer

### **3. PKIoverheid certificaten**

- 3.1 Standaarden
- 3.2 Wat is PKIoverheid?
  - 3.2.1 PKIoverheid
  - 3.2.2 PKIoverheid certificaat
- 3.3 Voorschriften
  - 3.3.1 Digikoppeling voorschriften
  - 3.3.2 PKIoverheid Programme of Requirements
  - 3.3.3 Geldigheid
- 3.4 Best practices
- 3.5 Welk certificaat dient gebruikt te worden voor Digikoppeling?

### **4. TLS (Transport Layer Security)**

- 4.1 Standaarden
- 4.2 Digikoppeling voorschriften
- 4.3 Onderbouwing
- 4.4 Overwegingen

### **5. Cipher suites voor TLS, signing en encryptie**

- 5.1 TLS Ciphersuites
- 5.2 XML Signing

- 5.2.1 Digikoppeling voorschriften voor XML signing
- 5.2.2 Reden voor vervanging SHA-1 door SHA-2
- 5.3 XML Encryptie
- 5.3.1 Digikoppeling voorschriften voor payload encryptie

## 6. Lijst met figuren

### A. Referenties

- A.1 Normatieve referenties
- A.2 Informatieve referenties

## § Conformiteit

Naast onderdelen die als niet-normatief gemarkeerd zijn, zijn ook alle diagrammen, voorbeelden, en noten in dit document niet-normatief. Verder is alles in dit document normatief.

## Samenvatting

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.

## § 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              |
| 01/09/2020 | 1.3    | Logius | PKIO Private Root certificaten toegevoegd                      |

| Datum      | Versie | Auteur | Opmerkingen                                                                                                                                                          |
|------------|--------|--------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 01/02/2021 | 1.4    | Logius | Alleen PKIO Private Root toegestaan. Verwijzing naar meest recente versie van [ <a href="#">NCSC 2021</a> ]. Vorige versie was v2.0 uit 2019                         |
| 15/05/2025 | 2.0    | Logius | Uitfasering 3DES                                                                                                                                                     |
| 24/06/2025 | 2.0.1  | Logius | Aanpassing n.a.v. NCSC TLS 2025 Richtlijnen. Verwijzing naar meest recente versie van [ <a href="#">NCSC 2025</a> ]. Vorige versie was [ <a href="#">NCSC 2021</a> ] |

## § Colofon

|                 |                                                                        |
|-----------------|------------------------------------------------------------------------|
| Logius          | Postbus 96810 2509 JE Den Haag tel. 0900 555 4555 (10 ct p/m) email    |
| Servicecentrum: | <a href="mailto:servicecentrum@logius.nl">servicecentrum@logius.nl</a> |

## §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 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:

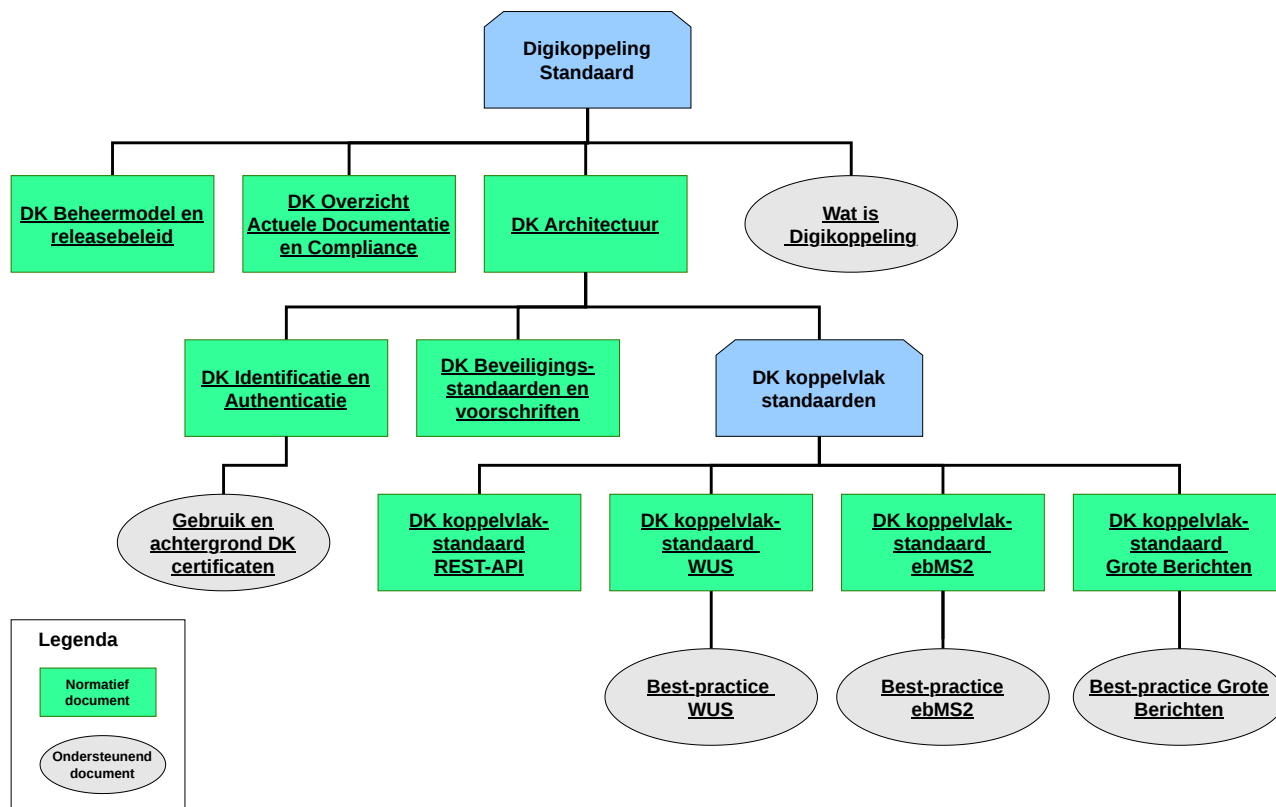
- Inhoud: op deze laag worden de afspraken gemaakt over de inhoud van het uit te wisselen bericht, dus de structuur, semantiek, waardebereiken etc. Digikoppeling houdt zich niet met de inhoud bezig, 'heeft geen boodschap aan de boodschap'.
- Logistiek: op deze laag bevinden zich de afspraken betreffende transportprotocollen (HTTP & TLS), messaging, 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.

## §1.3 Digikoppeling standaarden

De documentatie is als volgt opgebouwd:



*Figuur 1 Opbouw documentatie Digikoppeling*

## Legenda

| Kleur | Soort Document              |
|-------|-----------------------------|
| Groen | Standaard documentatie      |
| Grijs | Ondersteunende documentatie |

## Beheer

- De standaarddocumenten (groen/vierkant aangegeven) vallen onder het beheer zoals geformaliseerd in het document [Digikoppeling Beheermodel](#).
- De ondersteunende documentatie wordt onderhouden door Logius als de beheerder van de standaard (en afgestemd met stakeholders/ gebruikers).
- Alle goedgekeurde documenten zijn te vinden op de website van Logius, [www.logius.nl](http://www.logius.nl).

## §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 via het [\*Digikoppeling Portaal\*](#).

## §3. PKIoverheid certificaten

### §3.1 Standaarden

| Standaarden                            | Status    | Genoemd in                                                                                  |
|----------------------------------------|-----------|---------------------------------------------------------------------------------------------|
| PKIoverheid certificaten & CRL Profile | Verplicht | <a href="#"><i>Certificate Policy/Programme of Requirements PKIoverheid</i></a> , [RFC3447] |

## §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 Programme of Requirements.

Zie ook het document [Digikoppeling Koppelvlakstandaard ebMS2](#) en [PKIoverheid](#)

### § 3.2.2 PKIoverheid certificaat

Het PKIoverheid-certificaat is een computerbestand dat werkt als een digitaal paspoort. Als iemand een website, e-mail of document van uw organisatie wil bekijken, controleert zijn webbrowser of e-mailprogramma het bijbehorende certificaat. Door elkaar te identificeren verkleint de kans dat oplichters zich voor kunnen doen als iemand anders. Digitale certificaten waarborgen dus betrouwbaarheid [[PKIoverheid](#)].

Digikoppeling vereist dat de communicatiepartners PKIoverheid private root 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<br>subject:serialNumber veld is<br>verplicht | Dit is afgesproken met de TSP's in de<br>Digikoppeling Overeenkomsten. Zij<br>verstrekken PKIoverheid certificaten met<br>het OIN in het<br>subject:serialNumber field conform<br>de OIN systematiek als het een |



| Nr                | Voorschrift                                                                                                                                                                                                                          | Toelichting                                                                                                                                  |
|-------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------|
|                   |                                                                                                                                                                                                                                      | certificaat betreft dat voor Digikoppeling wordt gebruikt. [ <i>PKI-CA</i> ]                                                                 |
| PKI002            | PKIoverheid certificaat moet geldig zijn (het mag niet zijn verlopen of ingetrokken).                                                                                                                                                |                                                                                                                                              |
| PKI003<br>(WT004) | De geldigheid van het certificaat wordt getoetst met betrekking tot de geldigheidsdatum en de Certificate Revocation List(CRL) die voldoet aan de eisen van PKIoverheid.                                                             |                                                                                                                                              |
| PKI004<br>(WT005) | De betreffende CRL dient zowel voor de versturende als ontvangende partij te benaderen zijn.                                                                                                                                         |                                                                                                                                              |
| PKI005            | Het certificaat moet zijn van het type PKIoverheid private root (PKI Staat der Nederlanden Private Root) Voor Serviceaanbieders en Servicegebruikers geldt dat zij vanaf 1-1-2021 gebruik moeten maken van private root certificaten | PKIoverheid geeft aan dat voor machine-naar-machine (M2M) verkeer (zoals Digikoppeling) Private root certificaten gebruikt dienen te worden. |

### § 3.3.2 PKIoverheid Programme of Requirements

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) 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 onder een andere 'root' zijn uitgegeven, respectievelijk 'Staat der Nederlanden' (productie) en 'TRIAL PKIoverheid' (test). Deze zijn te vinden op <https://cert.pkioverheid.nl>.

### § 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 PKIoverheid. Zie eis PKI002 en PKI003.

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

Wanneer er tijdens de looptijd van een certificaat een bepaalde gebeurtenis plaatsvindt, dan moet het certificaat worden ingetrokken. Bijvoorbeeld wanneer de bijbehorende private sleutel is gecompromitteerd of wanneer de organisatie waarvoor het certificaat is uitgegeven wordt opgeheven of van (handels)naam wijzigt.

Het [Certificate Policy/Programme of Requirements PKIoverheid](#) beschrijft in de secties 4.1.2, 4.5.2 en 4.9.1 de gebeurtenissen wanneer certificaten ingetrokken moeten worden. Om de geldigheid van certificaten correct te controleren is een juiste systeemtijd essentieel. Afwijkingen kunnen leiden tot onterechte acceptatie of afwijzing. Het is daarom verstandig systemen automatisch te synchroniseren met een betrouwbare tijdsbron, bijvoorbeeld via [NTP](#).

### §3.4 Best practices

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

### §3.5 Welk certificaat dient gebruikt te worden voor Digikoppeling?

| Certificaat                                                  | OID                             |
|--------------------------------------------------------------|---------------------------------|
| G1 Private Services Server (met domeinnamen)                 | 2.16.528.1.1003.1.2.8.6         |
| G4 Private TLS Generic Devices Organization Validated Server | 2.16.528.1.1003.1.2.44.15.35.11 |

#### NOOT

Let op: De PKIo G1/G3 certificaten vervallen vanaf november 2028. Zorg ervoor dat u op tijd migreert naar de G4 certificaten. Voor meer informatie, zie [artikel](#).

## §4. TLS (Transport Layer Security)

Transport Layer Security (TLS) is een protocol dat een veilige versleutelde verbinding legt tussen systemen waardoor gegevens vertrouwelijk en compleet wordt uitgewisseld. Binnen de context van Digikoppeling verplicht TLS het gebruik van wederzijdse authenticatie van de betrokken partijen, zodat alleen geautoriseerde systemen kunnen communiceren met elkaar.

### §4.1 Standaarden

| Standaarden                                                                                                                    | Status             | Bron                                |
|--------------------------------------------------------------------------------------------------------------------------------|--------------------|-------------------------------------|
| TLS 1.2 [ <a href="#">RFC5246</a> ]                                                                                            | Verplicht          | [ <a href="#">NCSC 2025</a> ]       |
| TLS 1.3 [ <a href="#">RFC8446</a> ]                                                                                            | Zeer<br>aanbevolen | [ <a href="#">NCSC 2025</a> ]       |
| HTTP over TLS Transport Layer Security ([ <a href="#">RFC2818</a> ], [ <a href="#">RFC5785</a> ], [ <a href="#">RFC7230</a> ]) | Informational      | IETF<br>[ <a href="#">RFC5322</a> ] |

### §4.2 Digikoppeling voorschriften

| Nr     | Voorschrift                                                                                                                                                                                                 | Toelichting                                                                                                                                                     |
|--------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------|
| TLS001 | Authenticatie is verplicht met TLS en PKI-overheid 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 | NCSC geeft aan: “Configureer het gebruik van TLS 1.2 ter ondersteuning van oudere clients, maar geef de voorkeur aan TLS 1.3 waar mogelijk. Andere versies zijn |

| Nr     | Voorschrift                                                                  | Toelichting                                                            |
|--------|------------------------------------------------------------------------------|------------------------------------------------------------------------|
|        | dan is het aanbevolen voor Serviceafnemers om TLS 1.3 te gebruiken           | niet veilig in het gebruik.” Zie [NCSC 2025]                           |
|        | 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 [NCSC 2025]                                                        |

### §4.3 Onderbouwing

Zowel de Digikoppeling-koppelvlakstandaard ebMS2 als de Digikoppeling-koppelvlakstandaard WUS en Digikoppeling-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 PKI-overheid 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 [NCSC 2025] 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 die de NCSC-classificatie ‘uit te faseren’ hebben, zijn sinds 1 januari 2021 niet meer toegestaan. | Zie [ <i>NCSC 2025</i> ] |

### §5.2 XML Signing

#### § 5.2.1 Digikoppeling voorschriften voor XML signing

| Nr      | Voorschrift                                                                                                                                                                           | Toelichting                                                                                                                                                   |
|---------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------|
| SIGN001 | Signing met SHA-2 is verplicht.                                                                                                                                                       | Minimaal 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-256, SHA-384, SHA-512 [ <i>xmlenc-core</i> ], <i>FIPS PUB 180-4: Secure Hash Standard (SHS)</i> | Zie ook <a href="https://www.w3.org/TR/xmlldsig-core1/#sec-DigestMethod">https://www.w3.org/TR/xmlldsig-core1/#sec-DigestMethod</a> [ <i>xmlldsig-core1</i> ] |
| SIGN004 | Het SignatureMethod Algorithm kan gebruik maken van een van de volgende algoritmen: [SHA-256] [SHA-384] [SHA-512]                                                                     | Zie ook <a href="https://www.w3.org/TR/xmlldsig-core1/#sec-DigestMethod">https://www.w3.org/TR/xmlldsig-core1/#sec-DigestMethod</a> voor voorbeelden          |

## § 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 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. | [AES]                                                                                                                             |
| ENC002 | Encryptie conform XML versleuteling [xmlesc-core] is verplicht                                                             | [xmlesc-core]                                                                                                                     |
| ENC003 | De ondersteunde data encryption (data versleuteling) algoritmen zijn: 3DES(*) AES128 AES256                                | [xmlesc-core] (Gebruik GCM mode) (*) 3DES-encryptie verouderd: Niet gebruiken. 3DES-decryptie toegestaan voor legacy applicaties; |
| ENC004 | Het Key transport algorithm maakt gebruik van de RSA-OAEP algoritmen.                                                      | [RFC5756], [xmlesc-core], [RFC5756]                                                                                               |

## §6. Lijst met figuren

Figuur 1 Opbouw documentatie Digikoppeling

## §A. Referenties

### §A.1 Normatieve referenties

#### [AES]

NIST FIPS 197: Advanced Encryption Standard (AES). November 2001. URL:  
<https://csrc.nist.gov/publications/fips/fips197/fips-197.pdf>

#### [DK-Portaal]

Digikoppeling Portaal. Logius. URL: <https://oinregister.logius.nl/>

#### [FIPS-180-4]

FIPS PUB 180-4: Secure Hash Standard (SHS). U.S. Department of Commerce/National Institute of Standards and Technology. August 2015. National Standard. URL:  
<https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.180-4.pdf>

#### [HTTPS-factsheet NCSC]

Factsheet HTTPS kan een stuk veiliger. NCSC. November 2014. URL:  
<https://www.ncsc.nl/documenten/factsheets/2019/juni/01/factsheet-https-kan-een-stuk-veiliger>

#### [NCSC 2025]

Transport Layer Security (TLS) richtlijnen 2025-05. NCSC. June 2025. URL:  
<https://www.ncsc.nl/wat-kun-je-zelf-doen/documenten/publicaties/2025/juni/01/ict-beveiligingsrichtlijnen-voor-transport-layer-security-2025-05>

#### [PKI-CA]

Aansluiten als Trust Service Provider. Logius. URL:  
<https://www.logius.nl/domeinen/toegang/aansluiten-als-trust-service-provider>

#### [PKIO-PvE]

Certificate Policy/Programme of Requirements PKIoverheid. Logius. URL:  
<https://cp.pkioverheid.nl/>

#### [RFC2818]

HTTP Over TLS. E. Rescorla. IETF. May 2000. Informational. URL:  
<https://httpwg.org/specs/rfc2818.html>

#### [RFC3447]

Public-Key Cryptography Standards (PKCS) #1: RSA Cryptography Specifications Version 2.1. J. Jonsson; B. Kaliski. IETF. February 2003. Informational. URL: <https://www.rfc->

[editor.org/rfc/rfc3447](http://editor.org/rfc/rfc3447)

**[RFC5246]**

*The Transport Layer Security (TLS) Protocol Version 1.2*. T. Dierks; E. Rescorla. IETF. August 2008. Proposed Standard. URL: <https://www.rfc-editor.org/rfc/rfc5246>

**[RFC5322]**

*Internet Message Format*. P. Resnick, Ed. IETF. October 2008. Draft Standard. URL: <https://www.rfc-editor.org/rfc/rfc5322>

**[RFC5756]**

*Updates for RSAES-OAEP and RSASSA-PSS Algorithm Parameters*. S. Turner; D. Brown; K. Yiu; R. Housley; T. Polk. IETF. January 2010. Proposed Standard. URL: <https://www.rfc-editor.org/rfc/rfc5756>

**[RFC5785]**

*Defining Well-Known Uniform Resource Identifiers (URIs)*. M. Nottingham; E. Hammer-Lahav. IETF. April 2010. Proposed Standard. URL: <https://www.rfc-editor.org/rfc/rfc5785>

**[RFC7230]**

*Hypertext Transfer Protocol (HTTP/1.1): Message Syntax and Routing*. R. Fielding, Ed.; J. Reschke, Ed. IETF. June 2014. Proposed Standard. URL: <https://httpwg.org/specs/rfc7230.html>

**[RFC8446]**

*The Transport Layer Security (TLS) Protocol Version 1.3*. E. Rescorla. IETF. August 2018. Proposed Standard. URL: <https://www.rfc-editor.org/rfc/rfc8446>

**[xmldsig-core1]**

*XML Signature Syntax and Processing Version 1.1*. Donald Eastlake; Joseph Reagle; David Solo; Frederick Hirsch; Magnus Nyström; Thomas Roessler; Kelvin Yiu. W3C. 11 April 2013. W3C Recommendation. URL: <https://www.w3.org/TR/xmldsig-core1/>

**[xmlenc-core]**

*XML Encryption Syntax and Processing*. Donald Eastlake; Joseph Reagle. W3C. 10 December 2002. W3C Recommendation. URL: <https://www.w3.org/TR/xmlenc-core/>

## § A.2 Informatieve referenties

**[DK-Architectuur]**

*Digikoppeling Architectuur*. Logius. URL: <https://gitdocumentatie.logius.nl/publicatie/dk/architectuur/>

**[DK-Beheermodel]**

*Digikoppeling Beheermodel*. Logius. URL: <https://gitdocumentatie.logius.nl/publicatie/dk/beheer/>



**[DK-gbachtcert]**

*Digikoppeling Koppelvlakstandaard ebMS2*. Logius. URL:  
<https://gitdocumentatie.logius.nl/publicatie/dk/ebms/>

**[DK-IDAuth]**

*Digikoppeling Identificatie en Authenticatie*. Logius. URL:  
<https://gitdocumentatie.logius.nl/publicatie/dk/idauth/>

**[NCSC 2021]**

*ICT-beveiligingsrichtlijnen voor Transport Layer Security (TLS) v2.1*. NCSC. January 2021.  
URL: <https://www.ncsc.nl/documenten/publicaties/2021/januari/19/ict-beveiligingsrichtlijnen-voor-transport-layer-security-2.1>

**[PKIoverheid]**

*PKIoverheid*. Logius. URL: <https://www.logius.nl/domeinen/toegang/pkioverheid>