Logius - Standaard

Digikoppeling Beveiligingstandaarden en voorschriften 1.4

Logius Standaard

Deze versie:
https://publicatie.centrumvoorstandaarden.nl/dk/beveilig/1.4

Laatst gepubliceerde versie:
https://publicatie.centrumvoorstandaarden.nl/dk/beveilig/

Laatste werkversie:
https://logius-standaarden.github.io/Digikoppeling-Beveiligingsstandaarden-en-voorschriften/

Vorige versie
https://publicatie.centrumvoorstandaarden.nl/dk/beveilig/1.3/

Redacteurs:
Peter Haasnoot
Pieter Hering (Logius)

Auteur:
Pieter Hering

Doe mee:
GitHub Logius-standaarden/Digikoppeling-Beveiligingsstandaarden-en-voorschriften
Dien een melding in
Revisiehistorie
Pull requests

This document is also available in this non-normative format: pdf

---

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.

Status van dit document

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

Het OBDO heeft op advies van het Forum Standaardisatie deze versie vastgesteld.

Inhoudsopgave

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
01/02/2020	1.4	Logius	Alleen PKIO Private Root toegestaan. Verwijzing naar meest recente versie van [NCSC 2021]. Vorige versie was [NCSC 2019]

Colofon

Logius Servicecentrum:	Postbus 96810 2509 JE Den Haag t. 0900 555 4555 (10 ct p/m) e.servicecentrum@logius.nl

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 Digikoppeling standaarden bestaan uit de volgende documenten (groene blokken zijn onderdeel 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. De hele set informatie die tezamen nodig is voor een complete generieke Digikoppeling koppelvlakdefinitie bestaat uit:

- Interfacedefinitie.
- 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-Authenticatie]] voor meer informatie.

Het OIN register is bereikbaar op *https://portaal.digikoppeling.nl/registers/*.

3. PKIoverheid certificaten §

3.1 Standaarden §

Standaarden	Status	Genoemd in
PKIoverheid certificaten & CRL Profile	Verplicht	PKIoverheid Programma van Eisen [PKI Policy], [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 Programma van Eisen.

Zie ook het document [Digikoppeling-Cert] 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 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 wordt gebruikt. [PKI CA]
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 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.	
PKI005	Het certificaat moet zijn van het type PKIoverheid private root (PKI Staat der Nederlanden Private Root) [1]. [1] Uitzondering is wanneer er in het kader van certificaatbeheer op 1 server reden is om PKIO public root certificaten te gebruiken voor zowel koppeling als voor webserver. Hier dienen dan bilateraal afspraken over te worden gemaakt tussen de partijen. (Bij gebruik van PKIO public root certificaten is een specifieke eis en aandachtspunt dat deze vanwege externe regelgeving altijd binnen drie tot vijf dagen vervangen moeten kunnen worden.) Deze uitzondering is toegestaan tot 01-12-2022 Voor Serviceaanbieders en Servicegebruikers geldt dat zij uiterlijk per 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 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) 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-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 'Staat der Nederlanden Root Private Root’ en ‘PKI TRIAL root’.

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]	Verplicht	[NCSC 2021]
TLS 1.3 [rfc8446]	Optioneel	[NCSC 2021]
HTTP over TLS Transport Layer Security ([rfc2818], [rfc5785], [rfc7230])	Informational	IETF [rfc5322]

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.

Nr	Voorschrift	Toelichting
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 2021]
	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 2021]

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 [NCSC 2021] 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 [NCSC 2021]

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 [xmlenc-core], *FIPS PUB 180-4 Secure Hash Standard*	Zie ook https://www.w3.org/TR/xmldsig-core1/#sec-DigestMethod [xmldsig-core1]
SIGN004	Het SignatureMethod Algorithm kan gebruik maken van een van de volgende algoritmen: [SHA-224] [SHA-256] [SHA-384] [SHA-512]	Zie ook https://www.w3.org/TR/xmldsig-core1/#sec-DigestMethod 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 [NCSC 2021] 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.	[AES]
ENC002	Encryptie conform XML versleuteling [xmlenc-core] is verplicht	[xmlenc-core]
ENC003	De ondersteunde data encryption (data versleuteling) algoritmen zijn: 3DES AES128 AES256	[xmlenc-core] (Gebruik GCM mode indien beschikbaar anders CBC mode in combinatie met een signature)
ENC004	Het Key transport algorithm maakt gebruik van de RSA-OAEP algoritmen.	[rfc5756], [xmlenc-core], [rfc5756]

6. 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.

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

[FIPS-180-4]
FIPS PUB 180-4 Secure Hash Standard. U.S. Department of Commerce/National Institute of Standards and Technology. URL: https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.180-4.pdf

[HTTPS-factsheet NCSC]
Factsheet HTTPS kan een stuk veiliger. NCSC. Nov 2014. URL: https://www.ncsc.nl/documenten/factsheets/2019/juni/01/factsheet-https-kan-een-stuk-veiliger

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

[PKI CA]
Toegetreden vertrouwensdienstverleners. Logius. URL: https://www.logius.nl/diensten/pkioverheid/aansluiten-als-tsp/toegetreden-vertrouwensdienstverleners

[PKI Policy]
Programma van Eisen (PKIoverheid). Logius. URL: https://www.logius.nl/diensten/pkioverheid/aansluiten-als-tsp/pogramma-van-eisen

[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://tools.ietf.org/html/rfc3447

[rfc5246]
The Transport Layer Security (TLS) Protocol Version 1.2 T. Dierks; E. Rescorla. IETF. August 2008. Proposed Standard. URL: https://tools.ietf.org/html/rfc5246

[rfc5322]
Internet Message Format. P. Resnick, Ed.. IETF. October 2008. Draft Standard. URL: https://tools.ietf.org/html/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://tools.ietf.org/html/rfc5756

[rfc5785]
Defining Well-Known Uniform Resource Identifiers (URIs). M. Nottingham; E. Hammer-Lahav. IETF. April 2010. Proposed Standard. URL: https://tools.ietf.org/html/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://tools.ietf.org/html/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 §

[Digikoppeling Architectuur]
Digikoppeling Architectuur. Logius Centrum voor standaarden. Logius. december 2020. URL: https://centrumvoorstandaarden.github.io/Architectuur2.0-metRestfulAPI/static.html

[Digikoppeling Identificatie-Authenticatie]
Digikoppeling Identificatie en Authenticatie. Logius. URL: http://www.logius.nl/digikoppeling

[Digikoppeling-Cert]
Gebruik en achtergrond van Digikoppeling certificaten. Logius. URL: http://www.logius.nl/digikoppeling

[NCSC 2019]
ICT-beveiligingsrichtlijnen voor Transport Layer Security (TLS) v2.0 NCSC. April 2019. URL: https://www.ncsc.nl/documenten/publicaties/2019/mei/01/ict-beveiligingsrichtlijnen-voor-transport-layer-security-tls

[PKIoverheid]
PKIoverheid. Logius. URL: https://www.logius.nl/diensten/pkioverheid

↥