

**Edukoppeling**

Overzicht Edukoppeling voorschriften

(concept)

Edustandaard

Datum: December 2016

**Inhoudsopgave**

[1. Inleiding 3](#_Toc466974566)

[1.1. Doel en doelgroep van dit document 3](#_Toc466974567)

[2. Edukoppeling 1.2 4](#_Toc466974568)

[2.1. Toepassing van het openbare internet 4](#_Toc466974569)

[2.2. Toepassing van enkel het Digikoppeling WUS profiel 4](#_Toc466974570)

[2.3. Toepassing van PKI-Overheid en DUO certificaten (ODOC) 4](#_Toc466974571)

[2.4. Toepassing van specifieke eisen aan WS-addressing 4](#_Toc466974572)

[2.5. Toepassing specifieke eisen aan de foutafhandeling 5](#_Toc466974573)

[3. Digikoppeling WUS 3.0 5](#_Toc466974574)

[3.1. WUS WSDL 5](#_Toc466974575)

[3.2. WUS WS-Addressing 6](#_Toc466974576)

[3.3. WUS Binaire data 7](#_Toc466974577)

[3.4. WUS Beveiliging bij point to point communicatie (2W-be) 7](#_Toc466974578)

[3.5. Bij End to End communicatie (2W-be-S en 2W-be-SE) 8](#_Toc466974579)

[3.6. Betrouwbare gegevensoverdracht o.b.v. WUS WS-RM (Geen) 9](#_Toc466974586)

[3.7. Namespaces (Geen) 9](#_Toc466974587)

[3.8. WUS Foutafhandeling (Geen) 9](#_Toc466974588)

[4. Digikoppeling beveiligingsstandaarden en voorschriften 9](#_Toc466974589)

[4.1. PKI 9](#_Toc466974590)

[4.1.1. PKIOverheid PvE 9](#_Toc466974591)

[4.1.2. Algemene beveiliging voorschriften rond PKI. 10](#_Toc466974592)

[4.2. Digikoppeling TLS 10](#_Toc466974593)

[4.3. Cipher suites voor TLS, signing en encryptie 10](#_Toc466974594)

[4.3.1. TLS 10](#_Toc466974595)

[4.3.2. Ondertekenen 11](#_Toc466974596)

[4.3.3. Versleuteling 11](#_Toc466974597)

[5. Referenties 13](#_Toc466974598)

[5.1. Digikoppeling 13](#_Toc466974599)

[5.1.1. Normatieve referenties 13](#_Toc466974600)

[5.1.2. Niet-normatieve referenties 13](#_Toc466974601)

[5.2. Onderwijs 14](#_Toc466974602)

[5.2.1. Samenwerking Informatiebeveiliging Onderwijsketen platform 14](#_Toc466974603)

[5.2.2. Dienst Uitvoering Onderwijs (DUO) 15](#_Toc466974604)

# Inleiding

Dit document heeft als doel om inzichtelijk te maken welke voorschriften er relevant zijn bij een Edukoppeling implementiatie. Hiertoe zijn de voorschriften uit de verschillende standaarden verzameld. Het kopiëren en dus dubbel beheer van voorschriften is niet handig, maar leden van de Edukoppeling werkgroep hebben aangegeven dat er behoefte is aan een dergelijk overzicht. Het document bevat vele links naar sites met aanvullende informatie. Deze kunnen wijzigen en we willen de lezer van dit document vragen om niet werkende links te melden bij de beheerder van Edukoppeling.

De voorschriften zijn overgenomen uit de volgende documenten:

1. Edukoppeling versie 1.2
2. Digikoppeling WUS 3.0 versie 3.4\*
3. Digikoppeling beveiligingsstandaarden + voorschriften (v1.0)\*
4. Digikoppeling Identificatie en authenticatie 1.3\*

\* Dit is de huidige definitieve versie. Momenteel is echter bekend dat men WS-RM uit Digikoppeling wil verwijderen. Wanneer en hoe dit gebeurt is nu nog niet duidelijk. Het is in ieder geval de bedoeling dat dit document wel meebeweegt met wijzigingen in de Digikoppeling standaard. Hierop zal dus wel actief beheer op worden gevoerd.

## Doel en doelgroep van dit document

Dit document heeft als doel ondersteuning te bieden bij Edukoppeling implementiaties en is bedoeld voor medewerkers die bij de (technische) implementatie van Edukoppeling betrokken zijn. Het gaat hierom werknemers (ontwikkelaars, architecten, projectmanagers, informatiemanagers etc.) werkzaam bij softwareleveranciers, bij uitgevers, bij distributeurs, bij uitvoeringsorganisaties als DUO, Kennisnet, Studielink, SBB en de Inspectie van het Onderwijs en, indien van toepassing, ook bij onderwijsinstellingen. De lezer van dit document willen wij vragen om zaken die ontbreken of onduidelijk zijn te melden bij de beheerder van Edukoppeling (<https://www.edustandaard.nl/standaarden/afspraken/afspraak/edukoppeling/1.2/>).

|  |  |  |  |
| --- | --- | --- | --- |
| **Afkorting** | **Rol** | **Taak**  | **Doelgroep** |
| MT | Management | Bevoegdheid om namens organisatie (strategische) besluiten te nemen. | Nee |
| PL | Projectleiding | Verzorgen van de aansturing van projecten. | Nee |
| A&D | Analyseren & ontwerpen  | Analyseren en ontwerpen van oplossingsrichtingen. Het verbinden van Business aan de IT. | Ja |
| OT&B | Ontwikkelen, testen en beheer | Ontwikkelt, bouwt en configureert de techniek conform specificaties. Zorgen voor beheer na ingebruikname.  | Ja |

# Edukoppeling 1.2

Het doel dat Edukoppeling nastreeft is het op een generieke manier kunnen uitwisselen van gegevens binnen de onderwijssector. Het bouwt hierbij voort op een standaard van de Nederlandse overheid, Digikoppeling. Edukoppeling is een vernauwing van de Digikoppeling standaard en is meer toegespitst op het onderkennen van het gebruik van SaaS leveranciers.

De 1.2 versie van Edukoppeling kent een aantal beperkende en aanvullende voorschriften op de Digikoppeling standaard, dit zijn:

1. Toepassing van het openbare internet
2. Toepassing van enkel het Digikoppeling WUS profiel
3. Toepassing van PKI-Overheid en DUO certificaten
4. Toepassing van specifieke eisen aan WS-addressing
5. Toepassing specifieke eisen aan de foutafhandeling

## Toepassing van het openbare internet

De Edukoppeling Transactiestandaard gebruikt het openbare internet, geen Diginetwerk of ander privaat netwerk.

## Toepassing van enkel het Digikoppeling WUS profiel

De Edukoppeling Transactiestandaard past alleen Digikoppeling WUS profielen toe voor zowel bevragingen als meldingen. Daarnaast kan het profiel Grote Berichten toegepast worden wanneer dit meer bruikbaar is. De profielen WS-RM en ebMS worden niet toegepast.

## Toepassing van PKI-Overheid en DUO certificaten (ODOC)

De Edukoppeling Transactiestandaard schrijft het gebruik van PKI-ODOC en/of PKI-Overheid certificaten voor daar waar binnen het WUS profiel het gebruik van een PKI-certificaat wordt voorgeschreven (zoals bij TLS, ondertekening en versleuteling van het bericht).

## Toepassing van specifieke eisen aan WS-addressing

De Edukoppeling Transactiestandaard stelt specifieke eisen aan het gebruik van WS-addressing headers om formele (bv onderwijsinstellingen) en administratieve partijen (bv SaaS-leveranciers) te kunnen onderscheiden. In de Edukoppeling Architectuur worden hiervoor een aantal rollen onderscheiden, dit zijn:

1. De eindorganisatie is de organisatie die in het kader van zijn doelstellingen samenwerkt met een andere organisatie (wordt via de WS-Addressing headers WSA:To en WSA:From gecommuniceerd).
2. De gegevensbewerker is een organisatie die in opdracht van de eindorganisatie gegevens verzamelt, opslaat, berekeningen uitvoert, verstrekt en dergelijke.
3. Een logistieke dienstverlener is een organisatie die faciliteert bij de verzending en ontvangst van berichten.

## Toepassing specifieke eisen aan de foutafhandeling

In de Edukoppeling Architectuur worden 5 soorten foutafhandeling en verwerking daarvan beschreven. Technische fouten zijn in lijn met de Digikoppeling (DK) afspraken, maar de lijst is voor Edukoppeling (EK) aangevuld. Deze aanvullingen hebben te maken met voorschrift 4.

# Digikoppeling WUS 3.0

Dit is een overzicht van de Digikoppeling voorschriften. De beschrijvingen zijn beknopt gehouden en voor de volledige beschrijving wordt naar de standaard verwezen. Edukoppeling bouwt voort op de Digikoppeling standaard en heeft dus impact op de onderstaande Digikoppeling voorschriften. De voorschriften van Edukoppeling zijn leidend. Dit is met name het geval rond WS-Addressing en PKI voorschriften.

Digikoppeling WUS onderkent de volgende groepen van voorschriften:

1. WSDL
2. WS-Addressing
3. Binaire data
4. Beveiliging
5. Betrouwbaarheid
6. Namespace

## WUS WSDL

Voorschriften ten gevolge van de keuze voor BP 1.2.

|  |  |
| --- | --- |
| **Nr** | **Omschrijving** |
| WW001 | Voor de SOAP berichten wordt SOAP 1.1 en “document-literal binding” gehanteerd. Hierbij wordt als transport binding HTTP voorgeschreven. |
| WW002 | Datatypen moeten voldoen aan de XML Schema Part 2: Datatypes |
| WW003 | Toepassing van document –literal style resulteert dat het SOAP “body” element slechts 1 XML element bevatten |
| WW004 | Basic Profile stelt eisen aan het “PortType” van een WSDL. Hierbij mogen de “parts” van de “messages” alleen een “element” bevatten (geen “parts” die een “type” attribuut gebruiken). |

Aanvullende voorschriften vanuit Digikoppeling op WSDL

|  |  |
| --- | --- |
| **Nr** | **Omschrijving** |
| WS001 | Er kunnen meerdere operaties per web service gedefinieerd worden. |
| WS002 | De SOAPAction aanduiding in de WSDL wordt gevuld met een lege string (“”), wordt weggelaten, of heeft dezelfde vulling als de {http://www.w3.org/2007/05/addressing/metadata}Action in de WSDL. In de HTTP Header van het bericht moet de SOAPAction een lege string met quotes zijn (“”), of een waarde hebben gelijk aan de WS-Addressing Action (wsa:Action). |
| WS003 | De Digikoppeling WUS ondersteunt alleen de zogenaamde “request/response” berichtenuitwisseling |
| WS005 | De WSDL bevat slechts één “portType” per WSDL bestand. |
| WS006 | Digikoppeling ondersteunt alleen UTF-8. |
| WS007 | In de header zijn geen eigen velden (header blocks) toegestaan. De header bevat alleen de in het betreffende profiel vastgestelde velden, die dus uitsluitend gedefinieerd zijn in het betreffende WS-I profiel (respectievelijk de onderliggende OASIS/W3C standaarden). |
| WS008 | Het is verplicht een WS-Addressing Action referentie op te nemen in de WSDL. Het definiëren van een WS-Addressing action in WSDL kan met behulp van de Web Services Addressing 1.0 – Metadata standaard. |

## WUS WS-Addressing

LET OP: Edukoppeling heeft afwijkende voorschriften op dit punt. Raadpleeg de Edukoppeling documentatie om de juiste WS-Adressing headers in berichten op te nemen met de juiste vulling.

|  |  |
| --- | --- |
| **Nr** | **Omschrijving** |
| WA001 | Digikoppeling WUS gebruikt de volgende velden uit WS-Addressing:* wsa:To
* wsa:Action
* wsa:MessageID
* wsa:RelatesTo
* wsa:ReplyTo
* wsa:From
 |

Het request bevat de volgende WSA velden:



Het response bevat de volgende WSA velden:



## WUS Binaire data

|  |  |
| --- | --- |
| **Nr** | **Omschrijving** |
| WM001 | Toepassen MTOM wordt door web service requester bepaald. |

## WUS Beveiliging bij point to point communicatie (2W-be)

|  |  |
| --- | --- |
| **Nr** | **Omschrijving** |
| WT001 | Authenticatie op transportniveau gebeurt op basis TLS met tweezijdige authenticatie. Client and Server authenticatie is vereist gebruikmakend van HTTPS en alle genoemde TLS versies.De TLS implementatie mag niet op SSL v3 terug kunnen vallen. |
| WT002 | 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 als gesteld in de functionele eisen Authenticatie Digikoppeling. Met het toepassen van PKIoverheid-certificaten die Digikoppeling compliant zijn, wordt hieraan voldaan. |
| WT003 | De minimaal ondersteunde TLS encryptie algoritmen en sleutellengtes worden beschreven in het document Digikoppeling beveiligingsstandaarden en voorschriften |
| 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. |
| WT005 | De betreffende CRL dient zowel voor de versturende als ontvangende partij te benaderen zijn. |
| WT006 | Voor communicatie over HTTPS wordt port 443 gebruikt. |
| WT007 | Binnen een TLS-sessie kunnen meerdere berichten verstuurd worden |
| WT008 | Voor de TLS-sessie moet een maximale duur gelden, na het verloop hiervan wordt de verbinding verbroken. Partijen zijn vrij om de maximale duur zelf te bepalen. |

## Bij End to End communicatie (2W-be-S en 2W-be-SE)

|  |  |
| --- | --- |
| **Nr** | **Omschrijving** |
| WB001 | Toepassen WS-Security 1.0 en WS-Security 1.1 |
| WB002 | Toepassen van Timestamp in security header met Timestamp Created is verplicht. Timestamp Expires is optioneel.Timestamp CreatedVerplicht onderdeel van een Timestamp.Timestamp ExpiresOptioneel onderdeel van een Timestamp.Timestamp tijdDe tijdstamp moet een Universal Time Coordinated (UTC) tijdzone aanduiding hebben. Bij het toepassen van een timestamp gaat tijdsynchronisatie van de verschillende communicerende systemen een rol spelen. Indien dit niet mogelijk is moet hiermee met de vulling van de Created en Expires rekening worden gehouden door middel van een “timestampSkew“. |
| WB003 | Indien WS-Security wordt toegepast, is ondertekenen verplicht en versleutelen optioneel |
| WB004 | Ondertekenen van bericht onderdelen SOAP:body, SOAP:headers (WS-Addressing headers en Timestamp) is verplicht bij toepassing van End-to-End beveiliging |
| WB005 | Bij toepassen van versleutelen geldt dit voor de volgende bericht onderdelen: SOAP:body |
| WB006 | Berichten worden eerst ondertekend en vervolgens versleuteld. |
| WB007 | Technische gegevens ten behoeve van ondertekenen:* Onderteken optie Algoritme: Exclusive XML Canonicalization
* DigestMethod Algorithm: Zie SIGN001-4
* SignatureMethod Algorithm: Zie SIGN001-4
 |
| WB008 | Technische gegevens ten behoeve van versleutelen:* Data Encryption Algorithms: NVT
* Key Transport Algorithms: NVT
 |
| WB009 | Security token X.509 Certificate Token (PKI Overheid Digikoppeling certificaat). |
| WB010 | Publieke sleutel dat gebruikt is voor het signing proces dient meegeleverd te worden met het bericht via een ‘Direct security token’ reference.Het certificaat wordt in het bericht meegestuurd. Hiermee kan de ontvanger door middel van het meegeleverd certificaat de handtekening controleren. Het certificaat dient uiteraard wel vertrouwd te zijn via een truststore configuratie. |
| WB011 | Het toepassen van End-to-End beveiliging wordt op serviceniveau aangeduid. Alle operaties en dus berichten (request en response) worden ontsloten volgens één bepaald Digikoppeling profiel. |
| WB012 | Voor het versleutelen van het responsebericht wordt het certificaat in het requestbericht gebruikt. |

1. 1.
	2.
	3.
	4.
	5.

## Betrouwbare gegevensoverdracht o.b.v. WUS WS-RM (Geen)

NVT

##  Namespaces (Geen)

Geen voorschriften

## WUS Foutafhandeling (Geen)

Geen voorschriften

# Digikoppeling beveiligingsstandaarden en voorschriften

Bij de Digikoppeling beveiligingsstandaarden worden de volgende groepen van voorschriften onderkend:

1. PKI
2. TLS
3. Cipher suites

## PKI

### PKIOverheid PvE

LET OP: Edukoppeling heeft afwijkende voorschriften op dit punt. Raadpleeg de Edukoppeling documentatie om te bepalen welke certificaten toegepast kunnen worden.

|  |  |
| --- | --- |
| **Nr** | **Omschrijving** |
| - | Een PKIoverheid certificaat dient conform de eisen van het PKIoverheid PvE te worden uitgegeven door de CSP. |
| - | 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. |
| - | 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’. |
| RFC 3647 | 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. |
| RFC 3647 | De volgende partijen mogen in een verzoek tot intrekking van een eindgebruikercertificaat doen:* de certificaatbeheerder;
* de certificaathouder;
* de abonnee;
* de CSP;
* ieder andere, naar het oordeel van de CSP, belanghebbende partij/persoon.
 |
| RFC 3647 | 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 | Ter verbijzondering van het in {16} IETF RFC 2560 gestelde is het gebruikt van vooraf berekende OCSP responses (precomputed responses) niet toegestaan |

### Algemene beveiliging voorschriften rond PKI.

|  |  |
| --- | --- |
| **Nr** | **Omschrijving** |
| PKI001 | Gebruik OIN in subject serial number veld is verplicht |
| PKI002 | PKIoverheid certificaat moet geldig zijn (dus mag niet zijn verlopen of ingetrokken) |
| PKI003 | 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 ook WT004. |
| PKI004 | De betreffende CRL dient zowel voor de versturende als ontvangende partij te benaderen zijn. Zie ook WT005. |

## Digikoppeling TLS

Algemene beveiliging voorschriften rond TLS.

|  |  |
| --- | --- |
| **Nr** | **Omschrijving** |
| - | TLS 1.2 (RFC5246) verplicht |
| - | HTTP over TLS Transport Layer Security (RFC2818, RFC5785, RFC7230) informational |
| 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 terug kunnen vallen. |
| TLS004 | TLS 1.0 en TLS 1.1 zijn niet meer toegestaan |
| TLS005 | Voor communicatie over HTTPS wordt port 443 gebruikt. |

## Cipher suites voor TLS, signing en encryptie

Beveiliging voorschriften rond cipher suites.

### TLS

|  |  |
| --- | --- |
| **Nr** | **Omschrijving** |
| TLSCIPH001 | Minimaal verplichtDe onderstaande TLS encryptie algoritmen en sleutellengtes MOETEN minimaal worden ondersteund:• TLS\_RSA\_WITH\_AES\_256\_CBC\_SHA• TLS\_RSA\_WITH\_AES\_128\_CBC\_SHA |
| TLSCIPH002 | Sterk aanbevolenOndersteuning 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 |

### Ondertekenen

PKIoverheid stelt SHA-2 als eis. Alle certificaten die onder de root Staat der Nederlanden worden uitgegeven moeten voldoen aan SHA-2.

|  |  |
| --- | --- |
| **Nr** | **Omschrijving** |
| SIGN001 | Signing met SHA-2 is verplicht. Minimaal SHA-224 of SHA-256. |
| SIGN002 | Signing conform XMLDSIG is verplicht |
| SIGN003 | Het DigestMethod Algorithm moet gebruik maken van een van de volgende algorithmen:[SHA-224][SHA-256][SHA-384][SHA-512] |
| SIGN004 | Het SignatureMethod Algorithm kan gebruik maken van een van de volgende algorithmen:[SHA-224][SHA-256][SHA-384][SHA-512] |

### Versleuteling

|  |  |
| --- | --- |
| **Nr** | **Omschrijving** |
| ENC001 | Indien er gebruik wordt gemaakt van XML encryption op payload niveau dient de FIPS 197 standaard (AES) te worden gebruikt. |
| ENC002 | Encryptie conform XML versleuteling [XML Encryption] is verplicht |
| ENC003 | 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 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 |
| ENC004 | De ondersteunde data encryption (data versleuteling) algoritmen zijn: [3DES] of [AES128] of [AES256]  |
| ENC005 | Het Key transport algorithm maakt gebruik van de RSA1\_5 of RSA-OAEP algorithmen. |

# Referenties

## Digikoppeling

### 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>

.

[ICT beveiligingsrichtlijnen voor TLS]

URL <https://www.ncsc.nl/actueel/whitepapers/ict-beveiligingsrichtlijnen-voortransport-layer-security-tls.html>

[PKI-CA] PKI Overheid toegetreden certificatiehouders.

URL <https://www.logius.nl/ondersteuning/pkioverheid/aansluiten-als-csp/toegetreden-csps/>

[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.

URL <http://www.ietf.org/rfc/rfc5322.txt>

[XMLDSIG] Joint W3C/IETF XML-Signature Syntax and Processing specification.

URL <http://www.w3.org/TR/2002/REC-xmldsig-core-20020212/>

NB: FIPS-1803 is vervangen door FIPS 180-4. XMLDSIG verwijst nog naar FIPS 180-3.

[XML Encryption] XML Encryption Syntax and Processing. W3C Recommendation.

URL <http://www.w3.org/TR/xmlenc-core/> beschrijft de volgende algorithmen:

* RSA1\_5] <http://www.w3.org/2001/04/xmlenc#rsa-1_5>
* [RSA-OAEP] <http://www.w3.org/2001/04/xmlenc#rsa-oaepmgf1p>
* [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] <http://www.w3.org/2001/04/xmlenc#aes128-cbc>
* [AES256] <http://www.w3.org/2001/04/xmlenc#aes256-cbc>

### Niet-normatieve referenties

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

**Block ciphers**

NCSC onderkent zowel AES als triple DES (block ciphers) als encryptie algorithmen. 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>

**Secure Hash Standard (FIPS 180-4)**

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

**Gebruik en achtergronden Digikoppeling certificaten**

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

**ICT beveiligingsrichtlijnen voor TLS**

URL <https://www.ncsc.nl/actueel/whitepapers/ict-beveiligingsrichtlijnen-voortransport-layer-security-tls.html>

**Uitschakelen SSLen upgrade open SSL**

URL <https://www.ncsc.nl/actueel/nieuwsberichten/ncsc-publiceert-nieuwfactsheet-schakel-ssl-2.0-uit-en-upgrade-openssl.html>

**HTTPS factsheet**

URL <https://www.ncsc.nl/actueel/nieuwsberichten/nieuw-factsheet-https-kan-een-stuk-veiliger.html>

**Digikoppeling Identificatie en Authenticatie**

**Dit document is onderdeel van de Digikoppeling documentatie.**

<https://www.logius.nl/fileadmin/logius/ns/diensten/digikoppeling/koppelvlakstandaarden/Digikoppeling_Identificatie_en_Authenticatie_v1_3.pdf>

**Digikoppeling 3.0 Architectuur**

**Dit document is onderdeel van de Digikoppeling documentatie.**

URL <https://www.logius.nl/standaarden/digikoppeling/architectuur-en-koppelvlakstandaarden/?L=1>

**Nationaal Cyber Security Center**

Actuele beveiligingsinformatie van NCSC

URL https://www.ncsc.nl/actueel/beveiligingsadviezen

## Onderwijs

### Samenwerking Informatiebeveiliging Onderwijsketen platform

**Certificeringsschema**

Het Certificeringsschema is gerelateerd aan de Edukoppeling Transactiestandaard. Waar Edukoppeling gaat over de verbinding tussen organisaties, gaat het Certificeringsschema over informatiebeveiliging en privacy bínnen die organisaties.

Binnen het Samenwerkingsplatform wordt gewerkt aan een ROSA katern privacy en beveiliging, waarin kaders (principes) opgenomen worden waar ketenpartijen, dus ook scholen, (op termijn) aan dienen te voldoen. Voor het hoger onderwijs zijn door SURF juridische normenkaders ontwikkeld voor zowel leveranciers van clouddiensten. Vanuit de ROSA wordt gewerkt aan afstemming en samenhang tussen het schema en andere initiatieven binnen en buiten het onderwijs. De 1.1 versie is de huidige vastgestelde standaard en bestaat voornamelijk uit een set maatregelen gebaseerd op de Cloud control matrix van de Cloud Security Alliance. Deze is te vinden op: <https://www.edustandaard.nl/standaarden/afspraken/afspraak/certificeringsschema/1.1/>

De 2.0 versie is gebaseerd op ISO 27001 en ISO 27002 en uitgebreid met beschrijvingen over het proces, toezicht, et cetera. Deze nieuwe conceptversie is te vinden op: <https://www.edustandaard.nl/standaarden/afspraken/afspraak/certificeringsschema/2.0/>

### Dienst Uitvoering Onderwijs (DUO)

**ODOC Certificaten**

De CSP dienstverlening van Dienst Uitvoering Onderwijs / Ministerie van Onderwijs, Cultuur en Wetenschap is beschreven in de Certificate Practice Statement.

<https://zakelijk.duo.nl/cps/>

<https://zakelijk.duo.nl/cps/CP_OCW_Digitaal_Onderwijs_Certificaat.pdf>