# UNIFORME BEVEILIGINGSVOORSCHRIFTEN
## TRANSPORT LAYER SECURITY (TLS)

| | |
|---|---|
| Datum | 3-9-2020 |
| Versie | 0.7 Concept ter consultatie |
| Auteur | Edustandaard werkgroep Uniforme Beveiligingsvoorschriften |

# INHOUDSOPGAVE

## Historie

| Versie | Auteur | Toelichting | Datum |
|---|---|---|---|
| 0.1 | Jordy van den Elshout | Eerste concept o.b.v. GAP-analyse en input tijdens de eerste werkgroepbijeenkomst. | 21 januari 2020 |
| 0.2 | Jordy van den Elshout | Bijgewerkt concept na input van de tweede bijeenkomst. Daarnaast een bijlage toegevoegd voor profielen, waaronder Edukoppeling. | 23 maart 2020 |
| 0.3 | Jordy van den Elshout | Bijgewerkt concept na input van de derde bijeenkomst. Daarnaast de feedback op het Edukoppeling profiel bijgewerkt. | 24 april 2020 |
| 0.4 | Jordy van den Elshout | Laatste openstaande voorschrift (OCSP stapling) afgerond. Tekstuele aanpassingen voor verduidelijking samenhang incl. hyperlinks naar de juiste bronnen. | 12 mei 2020 |
| 0.5 | Jordy van den Elshout | Bijgewerkt concept na input van de vierde bijeenkomst. Hulptools opgenomen en minimaal eis aan validatie: DV. Tevens voorschrift voor OCSP-stapling aangemerkt als concept. | 25 mei 2020 |
| 0.6 | Jordy van den Elshout | Wijzigingen op basis van advies ROSA-scan en besluit Architectuurraad, waaronder een basisprofiel en de tenzij bij poort 443. Daarnaast de samenhang met WDO en verwijzing naar PvE PKIoverheid toegevoegd. | 11 augustus 2020 |
| 0.7 | Jordy van den Elshout | Voorschriften voor certificaatcontrole toegevoegd. Op basis daarvan de basis profielen bijgewerkt. Tevens basisprofiel voor H2M toegevoegd. Versie ter consultatie. | 3 september 2020 |

# 1 Inleiding

## 1.1 Achtergrond

Ketenpartijen hebben te maken met verschillende gegevensuitwisselingen met de daarbij horende afspraken en standaarden. Hierbij worden ook afspraken gemaakt voor beveiliging. Wanneer deze afspraken per type uitwisseling worden gemaakt kan dit in onderwijsketen leiden tot interoperabiliteitsproblemen en/of inefficiëntie. Daarom is in de bijeenkomst van de Standaardisatieraad van 25 april 2019 besloten om een werkgroep 'Uniforme beveiligingsvoorschriften' (UBV) in het leven te roepen. Deze werkgroep zorgt voor een set uniforme beveiligingsvoorschriften die centraal kunnen worden onderhouden. Verschillende standaarden, zoals Edukoppeling, Uitwisseling Leerlinggegevens en Resultaten (UWLR) en Educatieve Distributie en Toegang (ECK DT), moeten hier dan naar verwijzen in plaats van dat zij deze zelfstandig definiëren. De voorschriften gelden daarmee voor alle gegevensuitwisselingen binnen het onderwijs. Dat geldt bijvoorbeeld voor BRON-uitwisseling via de standaard Edukoppeling. De voorschriften gelden ook voor gegevensuitwisselingen die eigen afspraken hebben, zoals voor Overstap Service Onderwijs (OSO). De afspraken hiervoor zijn gevat onder machine to machine (M2M).

De afspraken zijn ook van toepassing voor alle website en webdiensten die binnen het onderwijs gebruikt worden, aangezien die doorgaans ook een beveiligde verbinding bieden. Daar wordt in dit document apart aandacht aan besteed, onder human to machine (H2M).

## 1.2 Doel

Doel van de afspraak is het onderhouden van een eenduidige set van beveiligingsvoorschriften waarmee de veiligheid, interoperabiliteit en efficiëntie in de onderwijsketen wordt bevorderd.

## 1.3 Doelgroep

Deze voorschriften zijn bedoeld voor organisaties die ict-toepassingen leveren en/of beheren in de onderwijsketen. Dat geldt voor de hele onderwijssector (PO, VO, MBO, HO en WO).

## 1.4 Samenhang met andere initiatieven

De standaarden binnen Edustandaard die (randvoorwaardelijk) gebruikmaken van TLS, zoals Edukoppeling, UWLR en ECK DT, moeten naar de voorschriften in dit document verwijzen en niet (meer) zelf definiëren. Dat geldt ook voor de uitwisselingsdienst OSO.

Sommige voorschriften gelden op basis van een BIV-classificatie. Hiervoor wordt gebruikt gemaakt van het 'Certificeringsschema informatiebeveiliging en privacy ROSA' van Edustandaard. Naast de BIV-classificatie, zijn hier ook maatregelen in gedefinieerd. Bijvoorbeeld voor TLS, waarvoor ook naar deze voorschriften verwezen wordt.

Gebruikte standaarden in dit document, zoals TLS staat op de lijst met Verplichte (pas toe of leg uit) standaarden van Forum Standaardisatie. De Wet Digitale Overheid (WDO) kan deze standaarden verplicht stellen voor (semi-)publieke organisaties. De voorschriften in dit document geven dan tevens een invulling aan de principe pas-toe-leg-uit, als deze voor een organisatie of instelling verplicht gesteld is.

## 1.5 Taken en verantwoordelijkheden

Het eigenaarschap van deze voorschriften is belegd binnen Edustandaard, waar ook andere afspraken binnen het onderwijsdomein worden beheerd. Het beheer en de doorontwikkeling wordt uitgevoerd door de Edustandaard werkgroep Uniforme Beveiligingsvoorschriften.

## 1.6 Beheer en doorontwikkeling

Binnen Edustandaard wordt periodiek (minimaal eenmaal per jaar) de opzet en de werking van de voorschriften besproken met alle relevante stakeholders die vertegenwoordigd zijn in de Standaardisatieraad. Hiertoe wordt input verzameld vanuit de Edustandaard werkgroep Uniforme beveiligingsvoorschriften en vanuit Edu-K.

# 2 Algemeen

### 2.1 Bron voor voorschriften

Voor de Uniforme beveiligingsvoorschriften wordt waar mogelijk gebruik gemaakt van 'hoger gelegen' afspraken. Bij voorkeur internationale afspraken (zoals van INAN), indien nodig nationale afspraken (zoals van Forum Standaardisatie en NCSC) en alleen als die niet voldoen aanvullende afspraken die in deze werkgroep worden gemaakt. Afwijken van bovenliggende afspraken wordt onderbouwd.

#### 2.1.1 TLS-voorschriften NCSC

In geval van afspraken rondom TLS, wordt de 'ICT-beveiligingsrichtlijnen voor Transport Layer Security (TLS)' van NCSC gevolgd. Bij het maken van nadere afspraken wordt gerefereerd aan deze richtlijn. Dat betekent ook dat er voldaan moeten worden aan de TLS-voorschriften van NCSC.

| TLS-ALG-01 |
| --- |
| Het is verplicht te voldoen aan de 'ICT-beveiligingsrichtlijnen voor Transport Layer Security (TLS)' van NCSC. |

### 2.2 Onderscheid tussen M2M en H2M

Bij beveiligde gegevensuitwisselingen wordt onderscheid gemaakt tussen twee typen. De uitwisseling tussen systemen onderling typeren we daarbij als Machine to Machine (M2M). Uitwisseling tussen mens en een systeem typeren we als Human to Machine (H2M). Een voorbeeld hiervan gegevensuitwisseling bij bezoek van een website of gebruik van een webdienst.

De twee typen gegevensuitwisselingen zijn verschillend van aard en daarom kunnen de beveiligingsafspraken anders zijn. In geval van M2M is het bijvoorbeeld mogelijk om afspraken te maken over beide kanten van de uitwisseling. Iets wat typisch voor H2M niet mogelijk is, omdat op voorhand niet bekend is met welk device of welke browser de (web)server benaderd gaat worden. Om in de praktijk geen last te hebben van deze verschillen tussen geldende afspraken is het van belang om M2M en H2M verkeer op verschillende domeinen af te handelen.

| TLS-ALG-02 |
| --- |
| Gegevensuitwisseling voor M2M en H2M dient op separate domeinen (FQDN) te worden afgehandeld |

### 2.3 Onderscheid tussen veilige en minder veilige configuraties

In legacy-situaties kan het nodig zijn om minder veilige configuraties te gebruiken. Bijvoorbeeld TLS1.0 en TSL1.1 met classificatie 'uitfaseren'. Het gebruik van minder veilige configuraties moet geen risico vormen voor de veilige configuratie. Bijvoorbeeld door een downgrade attack, waarbij de minst veilige TLS-verbinding geforceerd wordt. Daarom is het van belang dat dit gescheiden, dus niet vanuit dezelfde bron (FQDN, serverconfiguratie, virtual host) geconfigureerd is.

| TLS-ALG-03 |
| --- |
| Gegevensuitwisseling met een minder veilige configuratie dient op een separaat domein (FQDN) te worden afgehandeld. |

# 3 Machine to Machine (M2M)

Machine to Machine (M2M) betreft de gegevensuitwisseling tussen systemen onderling. Zoals bij berichtenuitwisseling tussen partijen binnen het onderwijs. Hierbij wordt onderscheid gemaakt tussen serviceaanbieder (de partij die een dienst en/of gegevens beschikbaar stelt) en service-afnemer (de partij die een dienst gebruikt en/of gegevens ophaalt). Soms kan een partij beide zijn, wanneer deze zowel gegevens ophaalt als beschikbaarstelt. Bijvoorbeeld in geval van Overstap Service Onderwijs (OSO).

### 3.1 Volgen van bovenliggende voorschriften[1]

De 'ICT-beveiligingsrichtlijnen voor Transport Layer Security (TLS)' bevat in hoofdstuk 4 een opsomming van TLS versies, algoritmen en opties. Aan de verschillende varianten is daarbij een kwalificatie Onvoldoende, Uit te faseren, Voldoende of Goed aan toegekend. Dat geeft echter geen volledige helderheid over wat toegepast *mag* worden. Om daar volledig helder in te zijn wordt hier daarom de aanvullende afspraak gehanteerd ten aanzien van de te gebruiken TLS versies, algoritmen en opties:

- 'Onvoldoende' **mag niet** gebruikt worden
- 'Uit te faseren' **mag niet** gebruikt worden
- 'Voldoende' **mag** gebruikt worden
- 'Goed' heeft de **voorkeur**

### 3.2 Nadere invulling

Onderstaande voorschriften zijn specifiek en leidend boven de bovenliggende afspraken.

#### 3.2.1 Versie

Voor interoperabiliteit wordt altijd één versie van TLS met een selectie van cipher suites verplicht gesteld. Voor de veiligheid wordt voorkeur gegeven aan een hogere versie.

| **TLS-M2M-01 (Interoperabiliteit en veiligheid)** |
| --- |
| Een Serviceaanbieder is verplicht TLS versie 1.2 te ondersteunen, daarnaast is het aanbevolen voor een Serviceaanbieder om TLS versie 1.3 te ondersteunen.<br><br>Als een Serviceaanbieder TLS versie 1.3 aanbiedt dan is het aanbevolen voor Serviceafnemers om TLS 1.3 te gebruiken.<br><br>TLS 1.0 en TLS 1.1 zijn niet toegestaan |

#### 3.2.2 Algoritmeselecties

Door minimale set van *cipher suites* worden de richtlijnen (B2-1 t/m B2-4) van NCSC voor algoritmeselecties aangescherpt en deels expliciet gemaakt. Dat geldt voor certificaatverificatie, sleuteluitwisseling, bulkversleuteling en hashing. Deze zijn onderdeel van een cipher suite.

De TLS-richtlijn B2-5 van NCSC wordt gevolgd: "De algoritmeselecties worden op basis van de voorgeschreven ordening door de servers gekozen". Wat betreft de volgorde, wordt deze gevolgd uit 'Bijlage C - Lijst met cipher suites'. Lijst met minimale cipher suites, volgt dezelfde volgorde.

[1] De test op internet.nl biedt hierin ondersteuning en geeft inzicht in welke (classificatie aan) configuraties worden gebruikt op de opgegeven URL. Voor andere inzichten en of detail, kan ssllabs.com of hardenize.com ondersteuning bieden. Indien de server niet beschikbaar is voor het internet kunnen tools uitkomst bieden, zoals testssl.

**TLS-M2M-02 (Interoperabiliteit en veiligheid)**

**Een Serviceaanbieder is verplicht om alle onderstaande cipher suites in aangegeven volgorde te ondersteunen.**

*TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384*
*TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256*
*TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384*
*TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256*
*TLS_DHE_RSA_WITH_AES_128_GCM_SHA256*

**De cipher TLS_DHE mag alleen onder voorwaarde gebruikt worden:**

- **RFC 7919 groepen gebruikt worden**
- **Sleutellengte minimaal gelijk is aan de RSA sleutel**
- **Eigen parameters voor DH instelbaar is**

**Een Serviceafnemer mag een selectie hiervan gebruiken uit oogpunt van efficiëntie. Daarbij wordt aanbevolen om de meest veilige cipher te kiezen (hoogste in de lijst).**

In de uitwisselingscontext wordt ook gebruikt gemaakt van PKIoverheid-certificaten, die met RSA zijn ondertekend. Daarom kunnen cipher suites met ECDSA als certificaatverificatie niet verplicht gesteld worden.

De uitwisselingscontext bepaalt of alle verplichte cipher suites benodigd zijn. Een service aanbieder dient alle verplichte cipher suites te ondersteunen. Dat geldt niet voor een serviceafnemer, die alleen serviceaanbieders communiceert. Dat komt de efficiëntie ten goede.

### 3.3 Certificaat controle

Voordat gegevensuitwisseling plaatsvindt, dient het certificaat gecontroleerd te worden op geldigheid. Enerzijds op de verloopdatum en anderzijds of deze ingetrokken is en op de Certificate Revocation List (CRL) staat.

**TLS-M2M-08 (Veiligheid)**

Het certificaat wordt altijd gecontroleerd.

#### 3.3.1 Ingetrokken certificaat

Wanneer een certificaat gecompromitteerd is, wordt deze ingetrokken en op de CRL geplaatst. In dat geval kan het certificaat misbruikt worden en risico's vormen voor de gegevensuitwisseling. Wanneer het controleren niet mogelijk is, kan er niet vastgesteld worden dat een certificaat veilig is.

**TLS-M2M-09 (Veiligheid)**

Een certificaat dat is ingetrokken, of waarvan niet kan worden gecontroleerd of het is ingetrokken, mag niet worden gebruikt.

#### 3.3.2 Verlopen certificaat

Een certificaat heeft een looptijd waarop deze geldig is. Wanneer een certificaat verloopt, verdwijnt deze automatisch van de CRL en kan niet meer gecontroleerd worden of deze is ingetrokken. Omdat de veiligheid van een verlopen certificaat niet meer gegarandeerd kan worden mag het niet meer worden gebruikt.

**TLS-M2M-10 (Veiligheid)**

Een verlopen certificaat mag niet worden gebruikt.

#### 3.3.3 Beheer

Aangezien door het verlopen van een certificaat de gegevensuitwisseling niet meer plaats kan vinden, is het zaak het certificaat tijdig te verlengen. Het beheer van certificaten dient dan ook goed georganiseerd te zijn. Het wordt aanbevolen om het proces van verlengen zoveel mogelijk geautomatiseerd plaats te laten vinden. Hierbij kan gebruik worden gemaakt van Automatic Certificate Management Environment (ACME), een protocol dat certificaten automatische en tijdig kan vervangen.

| **TLS-M2M-11 (Beschikbaarheid)** |
| --- |
| Beheer van certificaten dient goed georganiseerd te zijn, zodat dit niet leidt tot beschikbaarheidsproblemen. Geadviseerd wordt om het proces van verlengen zoveel mogelijk geautomatiseerd plaats te laten vinden. |

#### 3.3.4 Wijze van certificaat controle

Of een certificaat geldig of verlopen is kan de cliënt zelfstandig controleren op basis van de in het certificaat opgenomen meta data. Het controleren op ingetrokken certificaten kan met CRL of het Online Certificate Status Protocol (OCSP). In geval van CRL controleert de cliënt of het certificaat op deze lijst staat. Met OCSP stuurt de cliënt een controle verzoek naar de OCSP-responder[2] die aangeeft of deze ingetrokken is. In beide gevallen is de cliënt afhankelijk van een derde partij. Wat betekent dat een outbound verbinding mogelijk moet zijn naar alle mogelijke CRL providers en OCSP-responders. Als deze niet beschikbaar is of een foutmelding geeft, kan het certificaat niet gecontroleerd worden en leidt dit tot beschikbaarheidsproblemen. Eerdere voorschrift (TLS-M2M-09) schrijft namelijk voor dat de gegevensuitwisseling niet mag plaatsvinden als het certificaat niet gecontroleerd kan worden (failsafe).

**OCSP-stapling**

Het OCSP verzoek kan ook door de server zelf meegestuurd worden met OCSP-stapling. Op dat moment is de cliënt niet afhankelijk van een derde partij, wat kan leiden tot beschikbaarheidsproblemen. Ook heeft de cliënt geen internet toegang nodig tot alle mogelijke OCSP-responders, wat bijdraagt aan een veilige configuratie en efficiëntie in beheer (van de firewall).

| **TLS-M2M-03 (Beschikbaarheid en veiligheid)** |
| --- |
| Bij voorkeur wordt OCSP-stapling op de server toegepast, zodat de cliënt niet afhankelijk is van een derde partij.<br><br>Geadviseerd wordt om daarbij gebruik te maken van een OCSP-proxy, zodat de server zelf ook geen directe toegang tot het internet, de OCSP-responder nodig heeft. |

**OCSP-caching**

Door OCSP-stapling heeft de cliënt geen afhankelijkheid van de OCSP-responder meer, maar de server wel. Daarom is een cache met periodiek verversing van de OCSP-response noodzakelijk. Gemiddeld is een OCSP-response 7 dagen geldig. Hoe eerder deze wordt ververst, hoe langer het duurt voordat dit tot problemen leidt. Wanneer een certificaat ingetrokken is, mag de gegevensuitwisseling niet meer plaatsvinden. In dat geval dient de cache ververst te worden, om te voorkomen dat een gegevensuitwisseling plaatsvindt met een ingetrokken certificaat.

| **TLS-M2M-12 (Beschikbaarheid)** |
| --- |
| Bij voorkeur wordt de OCSP-response periodiek gecached voor OCSP-stapling, zodat er geen directe afhankelijkheid is van de OCSP-responder. De cache wordt ververst als het certificaat ingetrokken is. |

**Tweezijdige certificaat verificatie**

[2] De webserver die OCSP verzoeken afhandelt voor de Certificate Authority (CA)

In geval van tweezijdige certificaat verificatie, ofwel clientcertificaten, biedt de cliënt een eigen clientcertificaat aan. Op dat moment gelden de voorschriften voor de server ook voor cliënt, zoals het toepassen van OCSP-stapling.

| TLS-M2M-13 |
| --- |
| Voorschriften voor de server gelden ook voor de cliënt als een clientcertificaat gebruikt wordt voor een tweezijdige TLS-verbinding. |

### 3.4 Overige

#### 3.4.1 HTTPS

HTTPS is door het IANA gestandaardiseerd op poort 443. Wanneer van een standaard afgeweken wordt, zijn door verschillende partijen en op verschillende niveaus (van applicatie tot netwerk) afspraken en aanpassingen nodig. Dat leidt tot inefficiënt en kans op fouten. Wat tevens leidt tot onveilige situaties, mede door de verruiming van verkeer op andere poorten dan 443.

Aangezien deze verplichting een grote impact kan hebben op bestaande configuraties, mag bij bilaterale uitwisselingen anders worden afgesproken.

| TLS-M2M-04 (Interoperabiliteit) |
| --- |
| Het is verplicht voor communicatie over HTTPS poort 443 te gebruiken, tenzij bij bilaterale uitwisselingen anders wordt afgesproken. |

Er mag geen redirect beschikbaar zijn welke de webservice calls redirect vanaf HTTP naar HTTPS. De reden hiervoor is dat een call over HTTP direct een payload bevat waar datalekken risicovol kunnen zijn.

| TLS-M2M-05 (Veiligheid) |
| --- |
| Er **mag geen** gebruik gemaakt worden van redirects die vanaf HTTP redirecten naar HTTPS |

De betrouwbaarheid wordt vergroot door alleen gebruik te maken van volledige en traceerbare domeinnamen, Fully Qualified Domain Names (FQDN).

| TLS-M2M-06 (Veiligheid) |
| --- |
| Maak alleen gebruik van volledige en traceerbare domeinnamen, Fully Qualified Domain Names (FQDN) |

#### 3.4.2 SNI

ServerNameIndiciation (SNI) is een toevoeging op TLS die het mogelijk maakt om aan één IP-adres en poort verschillende diensten met SSL certificaten te verbinden. Dat levert verschillende voordelen op, zoals efficiëntie in beheer en onderhoud. Wanneer SNI niet op de cliënt wordt geïmplementeerd, levert dit interoperabiliteit problemen op.

| TLS-M2M-07 (Interoperabiliteit) |
| --- |
| ServerNameIndication (SNI) **moet** door elk systeem dat acteert als cliënt geïmplementeerd zijn |

# 4 Human to Machine (H2M)

Human to Machine (H2M) betreft de gegevensuitwisseling tussen mens en systeem. Voorbeelden hiervan zijn: bezoek van een website, gebruik van een webapplicatie en gebruik van een app met gegevensuitwisseling.

## 4.1 Volgen van bovenliggende voorschriften[3]

De 'ICT-beveiligingsrichtlijnen voor Transport Layer Security (TLS)' bevat in hoofdstuk 4 een opsomming van TLS versies, algoritmen en opties. Aan de verschillende varianten is daarbij een kwalificatie Onvoldoende, Uit te faseren, Voldoende of Goed aan toegekend. Dat geeft echter geen volledige helderheid over wat toegepast *mag* worden. Om daar volledig helder in te zijn wordt hier daarom de aanvullende afspraak gehanteerd ten aanzien van de te gebruiken TLS versies, algoritmen en opties:

- 'Onvoldoende' **mag niet** gebruikt worden
- 'Uit te faseren' **mag niet** gebruikt worden, tenzij afspraken over uitfaseren binnen de sector gemaakt zijn (zie bijlage I).
- 'Voldoende' **mag** gebruikt worden,
- 'Goed' heeft de **voorkeur**

## 4.2 Nadere invulling

### 4.2.1 Versie

Geen aanvullende afspraak. Versie met classificatie 'Voldoende' **mag** gebruikt worden, echter heeft 'Goed' de **voorkeur.**

### 4.2.2 Algoritmeselecties

De TLS-richtlijn B2-5 van NCSC wordt gevolgd: "De algoritmeselecties worden op basis van de voorgeschreven ordening door de servers gekozen". Wat betreft de volgorde, wordt deze gevolgd uit 'Bijlage C - Lijst met cipher suites' van de TLS-richtlijnen van NCSC.
Cipher suites met classificatie 'Voldoende' **mag** gebruikt worden, echter heeft 'Goed' de **voorkeur.**

### 4.2.3 OCSP stapling

Deze functionaliteit zorgt ervoor dat de OCSP-informatie (voor het controleren van de geldigheid van een certificaat) door de server zelf wordt verstrekt. Hierdoor hoeft de cliënt geen verzoek te doen bij de OCSP-server wat tot een privacy-risico kan leiden. De certificaatleverancier ontvangt hiermee het surfgedrag van de gebruiker. De effectiviteit is echter onduidelijk, omdat de cliënt zelf bepaalt hoe de controle plaatsvindt. Webbrowsers hebben daar alternatieve wijze voor, zoals CRLite. Het betreft dan ook een advies om dit toe te passen (zie 4.1 Volgen van bovenliggende voorschriften)

## 4.3 Overige

### 4.3.1 HTTPS

Bij het uitwisselen van gegevens moet de gebruiker ervan uit kunnen gaan dat dit veilig en betrouwbaar gebeurd. Dat betekent dat dit door middel van HTTPS moet verlopen. Daarnaast is het tegenwoordig gewoon goed dat websites HTTPS ondersteunen en gebruikers hier automatisch naar worden doorverwezen. Daarnaast dient HSTS toegepast worden voor de bescherming tegen een *downgrade attack* naar HTTP.

| **TLS-H2M-02 (Veiligheid)** |
| --- |
| De server ondersteunt HTTPS, dwingt deze af en past HSTS toe, zodat de communicatie met de gebruiker altijd beveiligd is. |

[3] De test op internet.nl biedt hierin ondersteuning en geeft inzicht in welke (classificatie aan) configuraties worden gebruikt op de opgegeven URL. Voor andere inzichten en of detail, kan ssllabs.com of hardenize.com ondersteuning bieden.

# 5 PKI

De betrouwbaarheid van de gegevensuitwisseling is tevens afhankelijk van de Public Key Infrastructure (PKI) waaronder het gebruikte certificaat is uitgegeven. Waaronder het proces voor uitgifte waarbij verschillende niveaus van validatie plaatsvindt.

In hoofdlijnen wordt bij:

- Domein Validatie (DV) gecontroleerd of de aanvrager ook het domein beheert.
- Organisatie validatie (OV) wordt tevens gecontroleerd of de gegevens in het aangevraagde certificaat overeenkomen met handelsregister. Op basis van het telefoonnummer uit het handelsregister, wordt telefonische validatie uitgevoerd met de opgegeven contactpersoon.
- Uitgebreide validatie (EV) wordt tevens gecontroleerd of de aanvraag door een bevoegd persoon wordt gedaan, zoals opgenomen in het handelsregister. Daarnaast vindt voor elk verzoek een telefonische validatie plaats.

| Validatie | Domein (DV) | Organisatie (OV) | Uitgebreid (EV) |
|---|---|---|---|
| Verificatie domeinbeheerder | v | v | v |
| Verificatie van de organisatiegegevens | x | v | v |
| Verificatie via telefonisch contact | x | Initieel | Elk verzoek, zoals verlenging of aanpassing |

De keuze van het soort certificaat dient zelf gemaakt te worden, waarbij DV minimaal verplicht is.

Wanneer gekozen wordt voor een DV is de betrouwbaarheid afhankelijk van de toegangsbeveiliging tot het domein-, dns- en websitebeheer. De validatie van een DV verloopt namelijk via een DNS-record of website, zoals het geval bij Let's Encrypt. Wanneer een domein of website wordt gehackt, kan daarmee ook een certificaat bemachtigd en misbruikt worden. Bijvoorbeeld met een *man-in-the-middle attack*.

Indien een gebruiker de identiteit van een dienst moet kunnen controleren, dan is minimaal een OV nodig. Op dat moment is de naam van de organisatie opgenomen in het certificaat, die zichtbaar is voor de gebruiker.

### 5.1 PKIoverheid

PKIoverheid biedt zowel een OV als een EV server certificaat. Een belangrijk verschil is de invulling van het 'serieel nummer'. Bij een EV variant dient het KvK nummer opgenomen te worden. Bij een OV is dit vrij en kan het OIN opgenomen worden[4]. Aangezien bij M2M communicatie een OIN verplicht kan zijn, is daarvoor alleen de OV variant geschikt. Een EV variant kan wel voor bijvoorbeeld een website gebruikt worden.

Bij een PKIoverheid certificaat is er bij de Trusted Service Provider (TSP) een proces ingericht dat de identiteit van private partij controleert in het handelsregister. Hiermee is de identiteit en indirect de authenticatie via het certificaat geregeld. Bij niet PKIo TSP's is dit niet geregeld en kent men ook het OIN waarschijnlijk niet en kunnen andere key usages (combi's) toegepast worden.

| **TLS-PKI-01 (Veiligheid)** |
|---|
| Indien een OIN verplicht en de integriteit daarvan noodzakelijk (niveau 3) is, dient de authenticatie met een certificaat van PKIoverheid plaats te vinden. |

[4] Zie PKIoverheid Programma van Eisen deel 3b v4.8

### 5.2 Wildcard certificaat

Een wildcard certificaat maakt het mogelijk om via één certificaat alle subdomeinen van een domein te voorzien van een beveiligde verbinding (bijvoorbeeld *.domeinnaam.nl). Hierdoor is er geen overzicht waar welke certificaat gebruikt wordt, wat kan leiden tot fouten bij vervanging. Wanneer een wildcard certificaat op meerdere servers gebruikt moet worden, dient de *privatekey* gedistribiteurt worden. Dat verhoogd het risico op compromitteren. Vanuit security oogpunt is dan ook het advies om deze certificaten niet te gebruiken voor cruciale en gevoelige uitwisselingen (Niveau 3 van B, I of V).

| **TLS-PKI-02 (Veiligheid)** |
| --- |
| Een wildcard certificaat mag niet gebruikt worden bij gegevensuitwisseling waarvan de classificatie Beschikbaarheid, Integriteit of Vertrouwelijkheid niveau 3 is. |

### 5.3 Certificate Authority (CA)

Te allen tijde moet de cliënt de betrouwbaarheid en geldigheid van een certificaat kunnen controleren. Hiervoor moet het gebruikte certificaat ondertekend zijn door certificate authority (CA). De CA kan zowel commercieel, gratis, van de overheid of van een (eigen) organisatie zijn.

| **TLS-PKI-03 (Veiligheid)** |
| --- |
| Het certificaat moet ondertekend zijn door een CA en de cliënt moet deze kunnen controleren op geldigheid. |

### 5.4 OCSP in het servercertificaat

Wanneer OCSP-stapling wordt toegepast, kan dit ook in het certificaat kenbaar gemaakt worden. Op deze wijze weet de cliënt of OCSP-stapling wordt toegepast en kan de verbinding verbreken als er geen OCSP-stapling wordt aangeboden.

| **TLS-PKI-04 (Veiligheid)** |
| --- |
| Indien OCSP-stapling wordt toegepast, wordt geadviseerd om het attribuut *must staple* op te nemen in het certificaat zodat de cliënt hier ook op kan acteren. |

# Bijlage I: Afspraken over uitfaseren (H2M)

Configuratie met classificatie 'Uit te faseren' **mag niet** gebruikt worden, tenzij afspraken over uitfaseren binnen de sector gemaakt zijn. Dat zijn de voorschriften die gelden voor H2M voor de toepassing van bovenliggende afspraken o.b.v. de NCSC ICT-beveiligingsrichtlijnen voor TLS. In onderstaande tabel zijn deze afspraken opgenomen.

Het gebruik van ‘uit te faseren’ configuraties neemt risico's met zich mee. Dat betekent dat deze alleen onder bepaalde voorwaarden veilig gebruikt kunnen worden. Dat geldt ook voor de duur. Wanneer de vervaldatum verstreken is, geldt de uitzondering niet meer. Op dat moment mag het desbetreffende configuratie niet meer gebruikt worden en dient deze uitgefaseerd te zijn.

| Cat. | Onderwerp | Configuratie | Voorwaarden | Vervalt op |
|---|---|---|---|---|
| 0. TLS Versie | TLS Versie | TLS1.0<br>TLS1.1 | - TLS1.2 of hoger ook van toepassing is, zodat bij een (bekende) kwetsbaarheid de kwetsbare versie uitgeschakeld kan worden. EN<br>- Configuratie nodig is voor het accepteren van verouderde clients. | 1-1-2021 |

# BIJLAGE II: PROFIELEN

Standaarden moeten voldoen aan eisen uit verschillende voorschriften. Waaronder die van NCSC, maar soms ook andere zoals Digikoppeling. Om het overzicht te bieden voor de implementatie verantwoordelijke, zijn profielen opgesteld. Daarin is te zien welke eis gehanteerd moet worden, en welke dat is. Bij elke eis is aangeven waarom deze gevolgd moet worden. Daarnaast wat de bron en referentie is.

De profielen worden beheerd door de werkgroep UBV. Wijzigingen kunnen door de desbetreffende werkgroep van het profiel aangemeld worden. Bijvoorbeeld wanneer gerelateerde voorschriften veranderen. Een nieuw profiel wordt door beide werkgroepen vastgesteld.

**Basisprofiel M2M v1.0**

Het basisprofiel is opgesteld op basis van de UBV TLS v0.7 en NCSC ICT-beveiligingsrichtlijnen voor TLS v2.0.

| Cat. | Onderwerp | UBV Hfst/§ | Status | Ref. | Voorschrift |
|---|---|---|---|---|---|
| 1. TLS | TLS-richtlijn NCSC | 2 Alg. | UBV hanteren; basisprofiel | UBV - TLS-ALG-01 | Het is verplicht te voldoen aan de 'ICT-beveiligingsrichtlijnen voor Transport Layer Security (TLS)' van NCSC. |
| 1. TLS | Onderscheid tussen M2M en H2M | 2 Alg. | UBV hanteren; basisprofiel | UBV - TLS-ALG-02 | Gegevensuitwisseling voor M2M en H2M dient op separate domeinen (FQDN) te worden afgehandeld |
| 1. TLS | Onderscheid tussen veilige en legacy-configuratie | 2 Alg. | UBV hanteren; basisprofiel | UBV - TLS-ALG-03 | Gegevensuitwisseling met een minder veilige configuratie dient op een separaat domein (FQDN) te worden afgehandeld. |
| 1. TLS | Hashfuncties voor bulkversleuteling en het genereren van random numbers | 3.1 | NCSC hanteren o.b.v. UBV (Volgen van bovenliggende voorschriften) | NCSC - Hashfuncties voor bulkversleuteling en het genereren van random numbers | Voorkeur: HMAC-SHA-256, -384 en -512<br>Mag: HMAC-SHA-1 |
| 1. TLS | Hashfuncties voor sleuteluitwisseling | 3.1 | NCSC hanteren o.b.v. UBV (Volgen van bovenliggende voorschriften) | NCSC - Hashfuncties voor sleuteluitwisseling | SHA2-ondersteuning voor handtekeningen: Ja (ondersteuning van SHA-256, SHA-384 of SHA-512) |
| 1. TLS | Lengte van RSA-sleutels | 3.1 | NCSC hanteren o.b.v. UBV (Volgen van bovenliggende | NCSC - Lengte van RSA-sleutels | Voorkeur: minimaal 3072 bit<br>Mag: 2048 - 3071 bit |

| | | | | | |
|---|---|---|---|---|---|
| | | | voorschriften ) | | |
| 1. TLS | Ondersteunde elliptische krommen | 3.1 | NCSC hanteren o.b.v. UBV (Volgen van bovenliggende voorschriften ) | NCSC - Ondersteunde elliptische krommen | Voorkeur: secp384r1, secp256r1, x448, x25519<br>Mag: secp224r1 |
| 1. TLS | TLS Versie | 3.2.1 | UBV hanteren; basisprofiel | UBV - TLS-M2M-01 | Een Serviceaanbieder is verplicht TLS versie 1.2 te ondersteunen, daarnaast is het aanbevolen voor een Serviceaanbieder om TLS versie 1.3 te ondersteunen.<br><br>Als een Serviceaanbieder TLS versie 1.3 aanbiedt dan is het aanbevolen voor Serviceafnemers om TLS 1.3 te gebruiken.<br><br>TLS 1.0 en TLS 1.1 zijn niet toegestaan |
| 1. TLS | Cipher Suites | 3.2.2 | UBV hanteren; basisprofiel | UBV - TLS-M2M-02 | Een Serviceaanbieder is verplicht om alle onderstaande cipher suites in aangegeven volgorde te ondersteunen.<br>TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384<br>TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256<br>TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384<br>TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256<br>TLS_DHE_RSA_WITH_AES_128_GCM_SHA256<br><br>De cipher TLS_DHE mag alleen onder voorwaarde gebruikt worden:<br>RFC 7919 groepen gebruikt worden<br>Sleutellengte minimaal gelijk is aan de RSA sleutel<br>Eigen parameters voor DH instelbaar is<br><br>Een Serviceafnemer mag een selectie hiervan gebruiken uit oogpunt van efficiëntie. Daarbij wordt aanbevolen om de meest veilige cipher te kiezen (hoogste in de lijst). |
| 1. TLS | Poortnummer | 3.4.1 | UBV hanteren; basisprofiel | UBV - TLS-M2M-04 | Het is verplicht voor communicatie over HTTPS poort 443 te gebruiken, tenzij bij bilaterale uitwisselingen anders wordt afgesproken. |
| 1.1 TLS Opties | 0-RTT | 3.1 | NCSC hanteren o.b.v. UBV (Volgen van bovenliggende voorschriften ) | NCSC - 0-RTT | Uit |

| | | | | | |
|---|---|---|---|---|---|
| 1.1 TLS Opties | Client-initiated renegotiation | 3.1 | NCSC hanteren o.b.v. UBV (Volgen van bovenliggende voorschriften) | NCSC - Client-initiated renegotiation | Uit |
| 1.1 TLS Opties | Compressie | 3.1 | NCSC hanteren o.b.v. UBV (Volgen van bovenliggende voorschriften) | NCSC - Compressie | Voorkeur: Geen compressie<br>Mag: Compressie op applicatieniveau |
| 1.1 TLS Opties | Insecure renegotiation | 3.1 | NCSC hanteren o.b.v. UBV (Volgen van bovenliggende voorschriften) | NCSC - Insecure renegotiation | Uit |
| 1.1 TLS Opties | OCSP stapling | 3.1 | UBV hanteren; basisprofiel | UBV - TLS-M2M-03 | Bij voorkeur wordt OCSP-stapling op de server toegepast, zodat de cliënt niet afhankelijk is van een derde partij.<br><br>Geadviseerd wordt om daarbij gebruik te maken van een OCSP-proxy, zodat de server zelf ook geen directe toegang tot het internet, de OCSP-responder nodig heeft. |
| 1.1 TLS Opties | OCSP stapling | 3.3.4 | UBV hanteren; basisprofiel | UBV - TLS-M2M-12 | Bij voorkeur wordt de OCSP-response periodiek gecached voor OCSP-stapling, zodat er geen directe afhankelijkheid is van de OCSP-responder. De cache wordt ververst als het certificaat ingetrokken is. |
| 1.1 TLS Opties | Redirect | 3.4.1 | UBV hanteren; basisprofiel | UBV - TLS-M2M-05 | Er mag geen gebruik gemaakt worden van redirects die vanaf HTTP redirecten naar HTTPS |
| 1.1 TLS Opties | SNI | 3.4.2 | UBV hanteren; basisprofiel | UBV - TLS-M2M-07 | ServerNameIndication (SNI) moet door elk systeem dat acteert als cliënt geïmplementeerd zijn |
| PKI | Certificaat | 3.1 | NCSC hanteren o.b.v. UBV (Volgen van bovenliggende voorschriften) | NCSC - Richtlijn B3-4 | Als het aangeboden certificaat niet direct door de root CA is ondertekend, biedt de server tussenliggende CA's aan die het pad authenticeren tussen de root CA en het aangeboden certificaat. |

| | | | | | |
|---|---|---|---|---|---|
| PKI | Certificaat controle | 3.3 | UBV hanteren; basisprofiel | UBV - TLS-M2M-08 | Het certificaat wordt altijd gecontroleerd. |
| PKI | Certificaat controle | 3.3 | UBV hanteren; basisprofiel | UBV - TLS-M2M-09 | Een certificaat dat is ingetrokken, of waarvan niet kan worden gecontroleerd of het is ingetrokken, mag niet worden gebruikt. |
| PKI | Certificaat controle | 3.3 | UBV hanteren; basisprofiel | UBV - TLS-M2M-10 | Een verlopen certificaat mag niet worden gebruikt. |
| PKI | Certificaat controle | 3.3 | UBV hanteren; basisprofiel | UBV - TLS-M2M-11 | Beheer van certificaten dient goed georganiseerd te zijn, zodat dit niet leidt tot beschikbaarheidsproblemen. Geadviseerd wordt om het proces van verlengen zoveel mogelijk geautomatiseerd plaats te laten vinden. |
| PKI | Certificaat controle | 3.3 | UBV hanteren; basisprofiel | UBV - TLS-M2M-13 | Voorschriften voor de server gelden ook voor de cliënt als een clientcertificaat gebruikt wordt voor een tweezijdige TLS-verbinding. |
| PKI | CN | 3.4.1 | UBV hanteren; ontbreekt in DK | UBV - TLS-M2M-06 | Maak alleen gebruik van volledige en traceerbare domeinnamen, Fully Qualified Domain Names (FQDN) |
| PKI | OIN | 5 PKI | UBV hanteren; basisprofiel | UBV - TLS-PKI-01 | Indien een OIN verplicht en de integriteit daarvan noodzakelijk (niveau 3) is, dient de authenticatie met een certificaat van PKIoverheid plaats te vinden. |
| PKI | Certificaat | 5 PKI | UBV hanteren; basisprofiel | UBV - TLS-PKI-02 | Een wildcard certificaat mag niet gebruikt worden bij gegevensuitwisseling waarvan de classificatie Beschikbaarheid, Integriteit of Vertrouwelijkheid niveau 3 is. |
| PKI | Certificaat | 5 PKI | UBV hanteren; basisprofiel | UBV - TLS-PKI-03 | Het certificaat moet ondertekend zijn door een CA en de cliënt moet deze kunnen controleren op geldigheid. |
| PKI | Certificaat | 5 PKI | UBV hanteren; ontbreekt in DK | UBV - TLS-PKI-04 | Indien OCSP-stapling wordt toegepast, wordt geadviseerd om het attribuut must staple op te nemen in het certificaat zodat de cliënt hier ook op kan acteren. |

**Basisprofiel H2M v1.0**

Het basisprofiel is opgesteld op basis van de UBV TLS v0.7 en NCSC ICT-beveiligingsrichtlijnen voor TLS v2.0.

| Cat. | Onderwerp | UBV Hfst/§ | Status | Ref. | Voorschrift |
|---|---|---|---|---|---|
| 1. TLS | TLS-richtlijn NCSC | 2 Alg. | UBV hanteren; basisprofiel | UBV - TLS-ALG-01 | Het is verplicht te voldoen aan de 'ICT-beveiligingsrichtlijnen voor Transport Layer Security (TLS)' van NCSC. |
| 1. TLS | Onderscheid tussen M2M en H2M | 2 Alg. | UBV hanteren; basisprofiel | UBV - TLS-ALG-02 | Gegevensuitwisseling voor M2M en H2M dient op separate domeinen (FQDN) te worden afgehandeld |
| 1. TLS | Onderscheid tussen veilige en legacy-configuratie | 2 Alg. | UBV hanteren; basisprofiel | UBV - TLS-ALG-03 | Gegevensuitwisseling met een minder veilige configuratie dient op een separaat domein (FQDN) te worden afgehandeld. |
| 1. TLS | TLS Versie | 4.2.1 Versies | NCSC hanteren o.b.v. UBV (Volgen van bovenliggende voorschriften) | NCSC - Versies | Voorkeur: TLS1.3 of TLS1.2<br>TLS1.1 of TLS 1.0 mag niet, tenzij aan voorwaarden wordt voldaan (zie bijlage I) |
| 1. TLS | Cipher Suites | 4.2.2 Algoritmeselecties | NCSC hanteren o.b.v. UBV (Volgen van bovenliggende voorschriften) | NCSC - Bijlage C – Lijst met cipher suites | Voorkeur:<br>TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384<br>TLS_ECDHE_ECDSA_WITH_CHACHA20_POLY1305_SHA256<br>TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256<br>TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384<br>TLS_ECDHE_RSA_WITH_CHACHA20_POLY1305_SHA256<br>TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256<br><br>Mag:<br>TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384<br>TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA<br>TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256<br>TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA<br>TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384<br>TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA<br>TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256<br>TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA<br>TLS_DHE_RSA_WITH_AES_256_GCM_SHA384<br>TLS_DHE_RSA_WITH_CHACHA20_POLY1305_SHA256<br>TLS_DHE_RSA_WITH_AES_128_GCM_SHA256<br>TLS_DHE_RSA_WITH_AES_256_CBC_SHA256<br>TLS_DHE_RSA_WITH_AES_256_CBC_SHA<br>TLS_DHE_RSA_WITH_AES_128_CBC_SHA256<br>TLS_DHE_RSA_WITH_AES_128_CBC_SHA |

| | | | | | |
|---|---|---|---|---|---|
| 1. TLS | Hashfuncties voor bulkversleuteling en het genereren van random numbers | 4.1 | NCSC hanteren o.b.v. UBV (Volgen van bovenliggende voorschriften) | NCSC - Hashfuncties voor bulkversleuteling en het genereren van random numbers | Voorkeur: HMAC-SHA-256, -384 en -512<br>Mag: HMAC-SHA-1 |
| 1. TLS | Hashfuncties voor sleuteluitwisseling | 4.1 | NCSC hanteren o.b.v. UBV (Volgen van bovenliggende voorschriften) | NCSC - Hashfuncties voor sleuteluitwisseling | SHA2-ondersteuning voor handtekeningen: Ja (ondersteuning van SHA-256, SHA-384 of SHA-512) |
| 1. TLS | Lengte van RSA-sleutels | 4.1 | NCSC hanteren o.b.v. UBV (Volgen van bovenliggende voorschriften) | NCSC - Lengte van RSA-sleutels | Voorkeur: minimaal 3072 bit<br>Mag: 2048 - 3071 bit |
| 1. TLS | Ondersteunde elliptische krommen | 4.1 | NCSC hanteren o.b.v. UBV (Volgen van bovenliggende voorschriften) | NCSC - Ondersteunde elliptische krommen | Voorkeur: secp384r1, secp256r1, x448, x25519<br>Mag: secp224r1 |
| 1.1 TLS Opties | OCSP stapling | 4.2.3 | NCSC hanteren o.b.v. UBV (Volgen van bovenliggende voorschriften) | NCSC - OCSP stapling | Voorkeur: aan<br>Mag: uit |
| 1.1 TLS Opties | 0-RTT | 4.1 | NCSC hanteren o.b.v. UBV (Volgen van bovenliggende voorschriften) | NCSC - 0-RTT | Uit |
| 1.1 TLS Opties | Client-initiated renegotiation | 4.1 | NCSC hanteren o.b.v. UBV (Volgen van bovenliggende voorschriften) | NCSC - Client-initiated renegotiation | Uit |
| 1.1 TLS Opties | Compressie | 4.1 | NCSC hanteren o.b.v. UBV (Volgen van bovenliggende voorschriften) | NCSC - Compressie | Voorkeur: Geen compressie<br>Mag: Compressie op applicatieniveau |
| 1.1 TLS Opties | Insecure renegotiation | 4.1 | NCSC hanteren o.b.v. UBV (Volgen van bovenliggende voorschriften) | NCSC - Insecure renegotiation | Uit |

| | | | | | |
|---|---|---|---|---|---|
| 1.1 TLS Opties | OCSP stapling | 4.1 | UBV hanteren; basisprofiel | UBV - TLS-M2M-03 | Bij voorkeur wordt OCSP-stapling op de server toegepast, zodat de cliënt niet afhankelijk is van een derde partij.<br><br>Geadviseerd wordt om daarbij gebruik te maken van een OCSP-proxy, zodat de server zelf ook geen directe toegang tot het internet, de OCSP-responder nodig heeft. |
| Overig | HTTPS | 4.3 Overige | UBV hanteren; basisprofiel | UBV - TLS-H2M-02 | De server ondersteunt HTTPS, dwingt deze af en past HSTS toe, zodat de communicatie met de gebruiker altijd beveiligd is. |
| PKI | Certificaat | 4.1 | NCSC hanteren o.b.v. UBV (Volgen van bovenliggende voorschriften) | NCSC - Richtlijn B3-4 | Als het aangeboden certificaat niet direct door de root CA is ondertekend, biedt de server tussenliggende CA's aan die het pad authenticeren tussen de root CA en het aangeboden certificaat. |
| PKI | OIN | 5 PKI | UBV hanteren; basisprofiel | UBV - TLS-PKI-01 | Indien een OIN verplicht en de integriteit daarvan noodzakelijk (niveau 3) is, dient de authenticatie met een certificaat van PKIoverheid plaats te vinden. |
| PKI | Certificaat | 5 PKI | UBV hanteren; basisprofiel | UBV - TLS-PKI-02 | Een wildcard certificaat mag niet gebruikt worden bij gegevensuitwisseling waarvan de classificatie Beschikbaarheid, Integriteit of Vertrouwelijkheid niveau 3 is. |
| PKI | Certificaat | 5 PKI | UBV hanteren; basisprofiel | UBV - TLS-PKI-03 | Het certificaat moet ondertekend zijn door een CA en de cliënt moet deze kunnen controleren op geldigheid. |
| PKI | Certificaat | 5 PKI | UBV hanteren; ontbreekt in DK | UBV - TLS-PKI-04 | Indien OCSP-stapling wordt toegepast, wordt geadviseerd om het attribuut must staple op te nemen in het certificaat zodat de cliënt hier ook op kan acteren. |

**UBV Edukoppeling v1.1**

Het Edukoppeling profiel is opgesteld op basis van de UBV TLS v0.7, NCSC ICT-beveiligingsrichtlijnen voor TLS v2.0 en Digikoppeling (DK) beveiligingsstandaarden en voorschriften v1.2 (incl. PKI005 uit conceptversie 1.3)

N.B. Voorschriften voor berichtondertekening en berichtversleuteling zijn alleen van toepassing bij WUS/SaaS-profiel met ondertekenen (2W-be-S)

| Cat. | Onderwerp | Status | Ref. | Voorschrift |
|---|---|---|---|---|
| 0. TLS Versie | TLS Versie | UBV hanteren; overgenomen van DK (TLS004) | UBV - TLS-M2M-01 | Een Serviceaanbieder is verplicht TLS versie 1.2 te ondersteunen, daarnaast is het aanbevolen voor een Serviceaanbieder om TLS versie 1.3 te ondersteunen.<br><br>Als een Serviceaanbieder TLS versie 1.3 aanbiedt dan is het aanbevolen voor Serviceafnemers om TLS 1.3 te gebruiken.<br><br>TLS 1.0 en TLS 1.1 zijn niet toegestaan |
| 1. TLS | TLS-richtlijn NCSC | UBV hanteren; in lijn met DK (TLS006) | UBV - TLS-ALG-01 | Het is verplicht te voldoen aan de 'ICT-beveiligingsrichtlijnen voor Transport Layer Security (TLS)' van NCSC. |
| 1. TLS | Onderscheid tussen M2M en H2M | UBV hanteren; ontbreekt in DK | UBV - TLS-ALG-02 | Gegevensuitwisseling voor M2M en H2M dient op separate domeinen (FQDN) te worden afgehandeld |
| 1. TLS | Onderscheid tussen veilige en legacy-configuratie | UBV hanteren; ontbreekt in DK | UBV - TLS-ALG-03 | Gegevensuitwisseling met een minder veilige configuratie dient op een separaat domein (FQDN) te worden afgehandeld. |
| 1. TLS | Cipher Suites | UBV hanteren; specifieker dan DK (TLSCIP001) | UBV - TLS-M2M-02 | Een Serviceaanbieder is verplicht om alle onderstaande cipher suites in aangegeven volgorde te ondersteunen.<br>TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384<br>TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256<br>TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384<br>TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256<br>TLS_DHE_RSA_WITH_AES_128_GCM_SHA256<br><br>De cipher TLS_DHE mag alleen onder voorwaarde gebruikt worden:<br>RFC 7919 groepen gebruikt worden<br>Sleutellengte minimaal gelijk is aan de RSA sleutel<br>Eigen parameters voor DH instelbaar is<br><br>Een Serviceafnemer mag een selectie hiervan gebruiken uit oogpunt van efficiëntie. Daarbij wordt aanbevolen om de meest veilige cipher te kiezen (hoogste in de lijst). |
| 1. TLS | Poortnummer | UBV hanteren; tegenstrijdig met DK (TLS005) | UBV - TLS-M2M-04 | Het is verplicht voor communicatie over HTTPS poort 443 te gebruiken, tenzij bij bilaterale uitwisselingen anders wordt afgesproken. |

| | | | | |
|---|---|---|---|---|
| 1. TLS | Terugvallen op eerdere versies | DK hanteren; in lijn met UBV (3.1) | DK - TLS003 | De TLS implementatie mag niet op SSL v3 en eerdere versies terugvallen |
| 1. TLS | Authenticatie | DK hanteren; in lijn met UBV (TLS-PKI-01) | DK - TLS001 | Authenticatie is verplicht met TLS en PKIoverheid certificaten |
| 1. TLS | Tweezijdige TLS | DK hanteren; ontbreekt in UBV | DK - TLS002 | Tweezijdig TLS is verplicht |
| 1. TLS | Hashfuncties voor bulkversleuteling en het genereren van random numbers | NCSC hanteren o.b.v. UBV (Volgen van bovenliggende voorschriften) | NCSC - Hashfuncties voor bulkversleuteling en het genereren van random numbers | Voorkeur: HMAC-SHA-256, -384 en -512<br>Mag: HMAC-SHA-1 |
| 1. TLS | Hashfuncties voor sleuteluitwisseling | NCSC hanteren o.b.v. UBV (Volgen van bovenliggende voorschriften) | NCSC - Hashfuncties voor sleuteluitwisseling | SHA2-ondersteuning voor handtekeningen: Ja (ondersteuning van SHA-256, SHA-384 of SHA-512) |
| 1. TLS | Lengte van RSA-sleutels | NCSC hanteren o.b.v. UBV (Volgen van bovenliggende voorschriften) | NCSC - Lengte van RSA-sleutels | Voorkeur: minimaal 3072 bit<br>Mag: 2048 - 3071 bit |
| 1. TLS | Ondersteunde elliptische krommen | NCSC hanteren o.b.v. UBV (Volgen van bovenliggende voorschriften) | NCSC - Ondersteunde elliptische krommen | Voorkeur: secp384r1, secp256r1, x448, x25519<br>Mag: secp224r1 |
| 1.1 TLS Opties | Redirect | UBV hanteren; ontbreekt in DK | UBV - TLS-M2M-05 | Er mag geen gebruik gemaakt worden van redirects die vanaf HTTP redirecten naar HTTPS |
| 1.1 TLS Opties | SNI | UBV hanteren; ontbreekt in DK | UBV - TLS-M2M-07 | ServerNameIndication (SNI) moet door elk systeem dat acteert als cliënt geïmplementeerd zijn |
| 1.1 TLS Opties | OCSP stapling | UBV hanteren; ontbreekt in DK | UBV - TLS-M2M-03 | Bij voorkeur wordt OCSP-stapling op de server toegepast, zodat de cliënt niet afhankelijk is van een derde partij.<br><br>Geadviseerd wordt om daarbij gebruik te maken van een OCSP-proxy, zodat de server zelf ook geen directe toegang tot het internet, de OCSP-responder nodig heeft. |

| | | | | |
|---|---|---|---|---|
| 1.1 TLS Opties | OCSP stapling | UBV hanteren; ontbreekt in DK | UBV - TLS-M2M-12 | Bij voorkeur wordt de OCSP-response periodiek gecached voor OCSP-stapling, zodat er geen directe afhankelijkheid is van de OCSP-responder. De cache wordt ververst als het certificaat ingetrokken is. |
| 1.1 TLS Opties | 0-RTT | NCSC hanteren o.b.v. UBV (Volgen van bovenliggende voorschriften) | NCSC - 0-RTT | Uit |
| 1.1 TLS Opties | Client-initiated renegotiation | NCSC hanteren o.b.v. UBV (Volgen van bovenliggende voorschriften) | NCSC - Client-initiated renegotiation | Uit |
| 1.1 TLS Opties | Compressie | NCSC hanteren o.b.v. UBV (Volgen van bovenliggende voorschriften) | NCSC - Compressie | Voorkeur: Geen compressie<br>Mag: Compressie op applicatieniveau |
| 1.1 TLS Opties | Insecure renegotiation | NCSC hanteren o.b.v. UBV (Volgen van bovenliggende voorschriften) | NCSC - Insecure renegotiation | Uit |
| Berichtonder tekening | | DK hanteren; ontbreekt in UBV | DK - SIGN001 | Signing met SHA-2 is verplicht. |
| Berichtonder tekening | | DK hanteren; ontbreekt in UBV | DK - SIGN002 | Signing conform XMLDSIG is verplicht |
| Berichtonder tekening | | DK hanteren; ontbreekt in UBV | DK - SIGN003 | Het DigestMethod Algorithm moet gebruik maken van een van de volgende algoritmen: [SHA-224] [SHA-256] [SHA-384] 5.3.1.15.2.1.1 [SHA-512] |
| Berichtonder tekening | | DK hanteren; ontbreekt in UBV | DK - SIGN004 | Het SignatureMethod Algorithm kan gebruik maken van een van de volgende algoritmen: [SHA-224] [SHA-256] [SHA-384] [SHA-512] |
| Berichtversleuteling | | DK hanteren; ontbreekt in UBV | DK - ENC001 | Indien er gebruik wordt gemaakt van XML encryption op payload niveau dient de FIPS 197 standaard (AES) te worden gebruikt. |
| Berichtversleuteling | | DK hanteren; ontbreekt in UBV | DK - ENC002 | Encryptie conform XML versleuteling [XML Encryption] is verplicht (http://www.w3.org/TR/xmlenc-core/) |

| | | | | |
|---|---|---|---|---|
| Berichtversleuteling | | DK hanteren; ontbreekt in UBV | DK - ENC003 | De ondersteunde data encryption (data versleuteling) algoritmen zijn: 3DES AES128 AES256 |
| Berichtversleuteling | | DK hanteren; ontbreekt in UBV | DK - ENC004 | Het Key transport algorithm maakt gebruik van de RSA-OAEP algoritmen. |
| PKI | CN | UBV hanteren; ontbreekt in DK | UBV - TLS-M2M-06 | Maak alleen gebruik van volledige en traceerbare domeinnamen, Fully Qualified Domain Names (FQDN) |
| PKI | OIN | DK hanteren; in lijn met UBV (TLS-PKI-01) | DK - Paragraaf 3.1 | Verplicht: PKIoverheid certificaten & CRL Profile |
| PKI | PKIoverheid | DK hanteren; in lijn met UBV (TLS-PKI-02) | DK - PKI005 (Concept v1.3) | Het certificaat moet zijn van het type PKIoverheid public root (PKI Staat der Nederlanden Root) of PKIoverheid private root (PKI Staat der Nederlanden Private Root) |
| PKI | PKIoverheid | DK hanteren; in lijn met UBV (TLS-PKI-03) | DK - 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. |
| PKI | PKIoverheid | UBV hanteren; ontbreekt in DK | UBV - TLS-PKI-04 | Indien OCSP-stapling wordt toegepast, wordt geadviseerd om het attribuut must staple op te nemen in het certificaat zodat de cliënt hier ook op kan acteren. |
| PKI | PKIoverheid | UBV hanteren; ontbreekt in DK | UBV - TLS-M2M-08 | Het certificaat wordt altijd gecontroleerd. |
| PKI | PKIoverheid | UBV hanteren; strenger dan DK (PKI002) | UBV - TLS-M2M-09 | Een certificaat dat is ingetrokken, of waarvan niet kan worden gecontroleerd of het is ingetrokken, mag niet worden gebruikt. |
| PKI | PKIoverheid | UBV hanteren; in lijn met DK (PKI002) | UBV - TLS-M2M-10 | Een verlopen certificaat mag niet worden gebruikt. |
| PKI | PKIoverheid | UBV hanteren; ontbreekt in DK | UBV - TLS-M2M-11 | Beheer van certificaten dient goed georganiseerd te zijn, zodat dit niet leidt tot beschikbaarheidsproblemen. Geadviseerd wordt om het proces van verlengen zoveel mogelijk geautomatiseerd plaats te laten vinden. |
| PKI | PKIoverheid | UBV hanteren; in lijn met DK | UBV - TLS-M2M-13 | Voorschriften voor de server gelden ook voor de cliënt als een clientcertificaat gebruikt wordt voor een tweezijdige TLS-verbinding. |
| PKI | PKIoverheid | DK hanteren; ontbreekt in UBV | DK - PKI001 | Gebruik OIN in subject serial number veld is verplicht |
| PKI | PKIoverheid | DK hanteren; ontbreekt in UBV | DK - PKI004 (WT005 | De betreffende CRL dient zowel voor de versturende als ontvangende partij te benaderen zijn |

| | | | | |
|---|---|---|---|---|
| PKI | Gebruik van publieke sleutel en certificaat door vertrouwende partij | DK hanteren; ontbreekt in UBV | DK - RFC 3647 - PvE 4.5.2 | 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.<br><br>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. 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. |
| PKI | Wie mag een verzoek tot intrekking doen | DK hanteren; ontbreekt in UBV | DK - RFC 3647 - PvE 4.9.2 | De volgende partijen mogen in een verzoek tot intrekking van een eindgebruikercertificaat doen:<br>- de certificaatbeheerder;<br>- de certificaathouder;<br>- de abonnee;<br>- de TSP;<br>ieder andere, naar het oordeel van de TSP, belanghebbende partij/persoon. |
| PKI | Controlevoorwaarden bij raadplegen certificaat statusinformatie | DK hanteren; ontbreekt in UBV | DK - RFC 3647 - PvE 4.9.6 | 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. |
| PKI | Online intrekking/statuscontrole | DK hanteren; ontbreekt in UBV | DK - RFC 3647 - PvE 4.9.9 | Ter verbijzondering van het in {16} IETF RFC 2560 gestelde is het gebruikt van vooraf berekende OCSP responses (precomputed responses) niet toegestaan. |
| PKI | Certificaat | NCSC hanteren o.b.v. UBV (Volgen van bovenliggende voorschriften) | NCSC - Richtlijn B3-4 | Als het aangeboden certificaat niet direct door de root CA is ondertekend, biedt de server tussenliggende CA's aan die het pad authenticeren tussen de root CA en het aangeboden certificaat. |