

**UNIFORME BEVEILIGINGSVOORSCHRIFTEN**  
**TRANSPORT LAYER SECURITY (TLS)**

Datum 11-2-2021  
Versie 1.1 Definitief  
Auteur Edustandaard werkgroep Uniforme Beveiligingsvoorschriften

# INHOUDSOPGAVE

<b>1 Inleiding</b>	<b>4</b>
1.1 Achtergrond	4
1.2 Doel	4
1.3 Doelgroep	4
1.4 Samenhang met andere initiatieven	4
1.5 Taken en verantwoordelijkheden	5
1.6 Beheer en doorontwikkeling	5
<b>2 Algemeen</b>	<b>6</b>
2.1 Bron voor voorschriften	6
2.1.1 TLS-voorschriften NCSC	6
2.2 Onderscheid tussen M2M en H2M	6
2.2.1 Wanneer onderscheid niet mogelijk is	6
2.3 Onderscheid tussen veilige en minder veilige configuraties	6
<b>3 Machine to Machine (M2M)</b>	<b>8</b>
3.1 Volgen van bovenliggende voorschriften	8
3.2 Nadere invulling	8
3.2.1 Versie	8
3.2.2 Algoritmeselecties	8
3.3 Certificaat controle	9
3.3.1 Ingetrokken certificaat	9
3.3.2 Verlopen certificaat	9
3.3.3 Beheer	10
3.3.4 Wijze van certificaat controle	10
3.4 Overige	11
3.4.1 HTTPS	11
3.4.2 SNI voor de cliënt	11
<b>4 Human to Machine (H2M)</b>	<b>12</b>
4.1 Volgen van bovenliggende voorschriften	12
4.2 Nadere invulling	12
4.2.1 Versie	12
4.2.2 Algoritmeselecties	12
4.2.3 OCSP stapling	12
4.3 Overige	12
4.3.1 HTTPS	12
<b>5 PKI</b>	<b>13</b>
5.1 PKIoverheid	13
5.2 Wildcard certificaat	14
5.3 Certificate Authority (CA)	14
5.4 OCSP in het servercertificaat	14
<b>Bijlage I: Afspraken over uitfaseren (H2M)</b>	<b>15</b>
<b>Bijlage II: profielen</b>	<b>16</b>
Basisprofiel M2M v1.1	16
Basisprofiel H2M v1.1	20
UBV Edukoppeling v1.2.1	24

## 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
0.7.1	Jordy van den Elshout	Naar aanleiding van commentaar duiding gegeven aan de scope (zie paragraaf 1.1) en uitzondering bij een Single Page Application (paragraaf 2.2). Daarnaast tekstuele redactie.	5 oktober 2020
0.8	Jordy van den Elshout	Aanpassingen n.a.v. reacties op consultatie en hetgeen besproken tijdens de bijeenkomst oktober 2020. Er is onderscheid gemaakt tussen voorschrift en advies, zowel in tekst als in kleur.	18 november 2020
1.0	Jordy van den Elshout	Profielen zijn bijgewerkt (incl. onderscheid tussen voorschrift en advies) op basis de laatste wijzigingen en controle op consistentie. TLS-ALG-01 is voor de correctheid aangepast naar een eerdere versie. Versie ter goedkeuring.	18 december 2020
1.1	Jordy van den Elshout	Bijgewerkt op basis van TLS-voorschriften v2.1 (NCSC), zoals TLS1.2 naar 'Voldoende' incl. de lijst met 'Algoritmeselecties'. Updaten profielen.	11 februari 2021

# 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, die tussen verschillende partijen plaatsvinden. 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).

In dit document wordt onderscheid gemaakt tussen voorschrift en advies die gelden voor de gegevensuitwisseling tussen partijen (M2M) en met gebruikers (H2M) in het onderwijs. De voorschriften (*donkergroen gemarkeerd*) zijn verplicht en vallen onder een pas-toe-leg-uit principe. Voor het advies (*lichtgroen gemarkeerd*) geldt dat niet. In de voorschriften wordt tevens onderscheid gemaakt tussen 'Veiligheid', 'Beschikbaarheid' en 'Interoperabiliteit'. De voorschriften voor 'Interoperabiliteit' zijn niet verplicht voor de gegevensuitwisseling binnen een eigen organisatie.

## 1.2 Doel

Doel van de afspraak is het onderhouden van een eenduidige set van beveiligingsvoorschriften waarmee de betrouwbaarheid en veiligheid van gegevensuitwisseling in de onderwijsketen wordt bevorderd. En daarmee bijdraagt in enerzijds de interoperabiliteit van de gegevensuitwisseling en anderzijds in de efficiëntie van implementatie en beheer.

## 1.3 Doelgroep

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

## 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) stelt deze standaarden verplicht voor (semi-)publieke organisaties. De voorschriften in dit document geven op deze wijze invulling aan het principe pas-toe-leg-uit, als deze voor een organisatie of instelling verplicht gesteld is.

Bescherming van gegevensuitwisseling is ook een onderdeel van de ISO27001, de standaard voor informatiebeveiliging. Deze voorschriften geven met name invulling aan de beheersmaatregelen 'A.13.2.3 Elektronische berichten' en 'A.14.1.3 Transacties van toepassingen beschermen'.

#### **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.

#### Voorschrift: TLS-ALG-01 (Veiligheid)

De '[ICT-beveiligingsrichtlijnen voor Transport Layer Security \(TLS\)](#)' van NCSC wordt in basis gevolgd en toegepast, tenzij deze TLS-voorschriften specifiek voorschrijft.

Welke voorschriften specifiek zijn dan NCSC en gezamenlijk van toepassing zijn, wordt in een profiel getoond (zie bijlage II: Profielen).

### 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.

#### Advies: TLS-ALG-02 (Veiligheid)

Het is van belang dat de gegevensuitwisseling voor M2M en H2M op separate hostnamen (FQDN) wordt afgehandeld.

#### 2.2.1 Wanneer onderscheid niet mogelijk is

Het kan voorkomen dat er geen onderscheid gemaakt kan worden, zoals bij een *Single Page Application*. Een webpagina die zowel door mensen als machines wordt benaderd. In dat geval gelden zowel de voorschriften van M2M als H2M. Soms kan dat conflicteren, zoals bij TLS-M2M-05 waarbij geen redirect van HTTP naar HTTPS mag plaatsvinden. Op dat moment kan daar door middel van pas-toe-leg-uit principe van afgeweken worden, zodat gebruikers wel naar beveiligde verbinding gestuurd worden.

### 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 TLS1.1 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. Deze scheiding geeft ook inzicht in het gebruik van legacy (configuraties) en kan gebruikt worden bij migratie van een oude/onveilige naar nieuwe/veilig configuratie.

**Voorschrift: TLS-ALG-03 (Veiligheid)**

Gegevensuitwisseling met een minder veilige configuratie dient op een separate hostnaam (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<sup>1</sup>

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.

#### Voorschrift: TLS-M2M-01 (Interoperabiliteit en veiligheid)

TLS 1.0 en TLS 1.1 zijn niet toegestaan.

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.

#### 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: "Alle ondersteunde algoritmeselecties zijn **Goed**, of 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.

---

<sup>1</sup> 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 sslabs.com of hardenize.com ondersteuning bieden. Indien de server niet beschikbaar is voor het internet kunnen tools uitkomst bieden, zoals testssl.



### Voorschrift: 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 achterwege gelaten worden, mits dit niet tot interoperabiliteitsproblemen leidt.

Als deze wel wordt toegevoegd, alleen onder de voorwaarde dat:

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

Als Serviceafnemer mag een selectie hiervan gebruikt worden, 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 PKI-overheid-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. Voor de interoperabiliteit dient een serviceaanbieder alle verplichte cipher suites te ondersteunen. Voor de minder veilige cipher TLS\_DHE geldt een uitzondering, mits dit niet tot interoperabiliteitsproblemen leidt. Dat geldt niet voor een serviceafnemer, die alleen met 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.

### Voorschrift: 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.

### Voorschrift: 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.

### Voorschrift: 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.

### Voorschrift: 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<sup>2</sup> 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).

### Advies: 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.

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 ververs, 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 ververs te worden, om te voorkomen dat een gegevensuitwisseling plaatsvindt met een ingetrokken certificaat.

<sup>2</sup> De webserver die OCSP verzoeken afhandelt voor de Certificate Authority (CA)

#### Advies: 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 verversd als het certificaat ingetrokken is.

#### Tweezijdige certificaat verificatie

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 controleren van het certificaat.

#### Voorschrift: TLS-M2M-13 (Veiligheid)

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.

#### Voorschrift: 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.

#### Voorschrift: 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 een volledige en traceerbare hostnaam, Fully Qualified Domain Names (FQDN). Wanneer alleen een hostnaam (niet FQDN) wordt gebruikt, is de organisatie niet herleidbaar. Ook is daarmee het risico groter op bijvoorbeeld een *man-in-the-middle attack*.

#### Voorschrift: TLS-M2M-06 (Veiligheid)

Maak alleen gebruik van een Fully Qualified Domain Name (FQDN).

#### 3.4.2 SNI voor de cliënt

ServerNameIndication (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.

#### Voorschrift: TLS-M2M-07 (Interoperabiliteit)

Elke cliënt moet ServerNameIndication (SNI) geïmplementeerd hebben.

## 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<sup>3</sup>

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: "Alle ondersteunde algoritmeselecties zijn **Goed**, of 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. Webrowsers 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 gebeurt. 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.

#### Voorschrift: TLS-H2M-02 (Veiligheid)

De server ondersteunt HTTPS, dwingt deze af en past HSTS toe, zodat de communicatie met de gebruiker altijd beveiligd is.

<sup>3</sup> 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 sslabs.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<sup>4</sup>. 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 PKIoverheid TSP's is dit niet geregeld en kent men ook het OIN waarschijnlijk niet en kunnen andere key usages (combi's) toegepast worden.

<sup>4</sup> Zie PKIoverheid Programma van Eisen deel 3b v4.8

#### Voorschrift: TLS-PKI-01 (Veiligheid)

Indien een OIN verplicht en de integriteit daarvan noodzakelijk (niveau 3) is, dient de authenticatie met een certificaat van PKI-overheid plaats te vinden.

#### 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). Een wildcard certificaat wordt meestal ingezet vanuit een oogpunt van kostenbesparing. Kostenbesparing kan meestal beter worden gerealiseerd door gebruik te maken van gratis, open en geautomatiseerde certificaten. Bij het gebruik van een wildcard certificaat is er geen overzicht waar welk certificaat voor gebruikt wordt, wat de kans tot fouten bij vervanging verhoogt. Wanneer een wildcard certificaat op meerdere servers gebruikt wordt, verhoogt dat het risico op compromittatie. De *private key* wordt op dat moment geëxporteerd en gedistribueerd over meerdere servers. Wanneer één van de servers wordt gecompromitteerd, heeft dit ook effect op alle andere servers. Vanuit oogpunt van veiligheid en beschikbaarheid is het dan ook van belang om deze certificaten niet te gebruiken voor cruciale en gevoelige uitwisselingen (Niveau 3 van B, I of V).

#### Voorschrift: TLS-PKI-02 (Veiligheid en beschikbaarheid)

Een wildcard certificaat mag niet gebruikt worden bij gegevensuitwisseling waarvan de classificatie Beschikbaarheid, Integriteit of Vertrouwelijkheid niveau 3 is. Bij een lagere classificatie (B, I of V is geen 3) is een wildcard certificaat wel toegestaan, echter wordt dit gezien de verhoogde kans op compromittatie van de *private key* niet geadviseerd.

#### 5.3 Certificate Authority (CA)

Te allen tijde moet de cliënt de betrouwbaarheid en geldigheid van een servercertificaat kunnen controleren. Hiervoor moet het gebruikte certificaat ondertekend zijn door certificate authority (CA).

#### Voorschrift: 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.

#### Advies: 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 TLS1.1	<ul style="list-style-type: none"><li>- TLS1.2 of hoger ook van toepassing is, zodat bij een (bekende) kwetsbaarheid de kwetsbare versie uitgeschakeld kan worden. EN</li><li>- De optie 'Client-initiated renegotiation' uitgeschakeld is. EN</li><li>- Configuratie nodig is voor het accepteren van verouderde clients.</li></ul>	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 aangegeven 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 v1.1

Het basisprofiel is opgesteld op basis van de UBV TLS v1.1 en NCSC ICT-beveiligingsrichtlijnen voor TLS v2.1.

Cat.	Onderwerp	Status	Ref.	Voorschrift
0. TLS Versie	TLS Versie	UBV hanteren; basisprofiel	UBV - Voorschrift: TLS-M2M-01	TLS 1.0 en TLS 1.1 zijn niet toegestaan.  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.
1. TLS	TLS-richtlijn NCSC	UBV hanteren; basisprofiel	UBV - Voorschrift: TLS-ALG-01	De 'ICT-beveiligingsrichtlijnen voor Transport Layer Security (TLS)' van NCSC wordt in basis gevolgd en toegepast, tenzij deze TLS-voorschriften specifiekere voorschrijft.
1. TLS	Onderscheid tussen M2M en H2M	UBV hanteren; basisprofiel	UBV - Advies: TLS-ALG-02	Het is van belang dat de gegevensuitwisseling voor M2M en H2M op separate hostnamen (FQDN) wordt afgehandeld.
1. TLS	Onderscheid tussen veilige en legacy-configurati e	UBV hanteren; basisprofiel	UBV - Voorschrift: TLS-ALG-03	Gegevensuitwisseling met een minder veilige configuratie dient op een separate hostnaam (FQDN) te worden afgehandeld.
1. TLS	Hashfuncties voor sleuteluitwisselin g	NCSC hanteren o.b.v. UBV (Volgen van bovenliggende voorschriften)	NCSC - Hashfuncties voor sleuteluitwisselin g (Tabel 5)	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 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, curve 448, curve 25519 Mag: secp224r1
1. TLS	Cipher Suites	UBV hanteren; basisprofiel	UBV - Voorschrift: TLS-M2M-02	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 achterwege gelaten worden, mits dit niet tot interoperabiliteitsproblemen leidt. Als deze wel wordt toegevoegd, alleen onder de voorwaarde dat: - RFC 7919 groepen gebruikt worden - Sleutellengte minimaal gelijk is aan de RSA sleutel - Eigen parameters voor DH instelbaar is  Als Serviceafnemer mag een selectie hiervan gebruikt worden, uit oogpunt van efficiëntie. Daarbij wordt aanbevolen om de meest veilige cipher te kiezen (hoogste in de lijst).
1. TLS	Sleuteluitwisseling	NCSC hanteren o.b.v. UBV (Volgen van bovenliggende voorschriften)	NCSC - Richtlijn B4-1	Wanneer er voor de sleuteluitwisseling gebruik wordt gemaakt van DHE, dan is de geheime parameter tijdelijk van aard, willekeurig gekozen uit een uniforme verdeling en van een adequate omvang voor het gekozen finite field.
1. TLS	Sleuteluitwisseling	NCSC hanteren o.b.v. UBV (Volgen van bovenliggende voorschriften)	NCSC - Richtlijn B4-2	Wanneer er voor de sleuteluitwisseling gebruik wordt gemaakt van ECDHE, dan is de geheime parameter tijdelijk van aard, willekeurig gekozen uit een uniforme verdeling en van een adequate omvang voor de gekozen elliptische kromme.
1.1 TLS Opties	Poortnummer	UBV hanteren; basisprofiel	UBV - Voorschrift: 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	NCSC hanteren o.b.v. UBV (Volgen van bovenliggende voorschriften)	NCSC - 0-RTT	Uit (of n.v.t. voor TLS 1.3)
1.1 TLS Opties	Client-initiated renegotiation	NCSC hanteren o.b.v. UBV (Volgen van bovenliggende voorschriften)	NCSC - Client-initiated renegotiation	Voorkeur: Uit (of n.v.t. in TLS1.2 en ouder) Mag: Aan
1.1 TLS Opties	Compressie	NCSC hanteren o.b.v. UBV (Volgen van bovenliggende voorschriften)	NCSC - Compressie	Voorkeur: Geen compressie Mag: Compressie op applicatieniveau

1.1 TLS Opties	Insecure renegotiation	NCSC hanteren o.b.v. UBV (Volgen van bovenliggende voorschriften)	NCSC - Insecure renegotiation	Uit (of n.v.t. voor TLS 1.3)
1.1 TLS Opties	OCSP stapling	UBV hanteren; basisprofiel	UBV - Advies: TLS-M2M-03	Bij voorkeur wordt OCSP-stapling op de server toegepast, zodat de cliënt niet afhankelijk is van een derde partij.  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; basisprofiel	UBV - Advies: 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 ververs als het certificaat ingetrokken is.
1.1 TLS Opties	Redirect	UBV hanteren; basisprofiel	UBV - Voorschrift: TLS-M2M-05	Er mag geen gebruik gemaakt worden van redirects die vanaf HTTP redirecten naar HTTPS.
1.1 TLS Opties	SNI	UBV hanteren; basisprofiel	UBV - Voorschrift: TLS-M2M-07	Elke cliënt moet ServerNameIndication (SNI) geïmplementeerd hebben.
PKI	Certificaat	NCSC hanteren o.b.v. UBV (Volgen van bovenliggende voorschriften)	NCSC - Richtlijn B3-1	De server biedt een certificaat aan ter authenticatie.
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.
PKI	Certificaat controle	UBV hanteren; basisprofiel	UBV - Voorschrift: TLS-M2M-08	Het certificaat wordt altijd gecontroleerd.
PKI	Certificaat controle	UBV hanteren; basisprofiel	UBV - Voorschrift: 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	UBV hanteren; basisprofiel	UBV - Voorschrift: TLS-M2M-10	Een verlopen certificaat mag niet worden gebruikt.
PKI	Certificaat controle	UBV hanteren; basisprofiel	UBV - Voorschrift: 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	UBV hanteren; basisprofiel	UBV - Voorschrift: TLS-M2M-13	Voorschriften voor de server gelden ook voor de cliënt als een clientcertificaat gebruikt wordt voor een tweezijdige TLS-verbinding.

PKI	CN	UBV hanteren; ontbreekt in DK	UBV - Voorschrift: TLS-M2M-06	Maak alleen gebruik van een Fully Qualified Domain Name (FQDN).
PKI	OIN	UBV hanteren; basisprofiel	UBV - Voorschrift: 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	UBV hanteren; basisprofiel	UBV - Voorschrift: TLS-PKI-02	Een wildcard certificaat mag niet gebruikt worden bij gegevensuitwisseling waarvan de classificatie Beschikbaarheid, Integriteit of Vertrouwelijkheid niveau 3 is. Bij een lagere classificatie (B, I of V is geen 3) is een wildcard certificaat wel toegestaan, echter wordt dit gezien de verhoogde kans op compromittatie van de private key niet geadviseerd.
PKI	Certificaat	UBV hanteren; basisprofiel	UBV - Voorschrift: TLS-PKI-03	Het certificaat moet ondertekend zijn door een CA en de cliënt moet deze kunnen controleren op geldigheid.
PKI	Certificaat	UBV hanteren; ontbreekt in DK	UBV - Advies: 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	Certificaat	NCSC hanteren o.b.v. UBV (Volgen van bovenliggende voorschriften)	NCSC - Hashfuncties voor certificaatverificatie (Tabel 3)	Voorkeur: SHA-512, SHA-384, SHA-256 Mag niet: SHA-1 , MD5

## Basisprofiel H2M v1.1

Het basisprofiel is opgesteld op basis van de UBV TLS v1.1 en NCSC ICT-beveiligingsrichtlijnen voor TLS v2.1.

Cat.	Onderwerp	Status	Ref.	Voorschrift
0. TLS Versie	TLS Versie	NCSC hanteren o.b.v. UBV (Volgen van bovenliggende voorschriften)	NCSC - Versies	Voorkeur: TLS1.3 Mag: TLS1.2 TLS1.1 of TLS 1.0 mag niet, tenzij aan voorwaarden wordt voldaan (zie bijlage I)
1. TLS	TLS-richtlijn NCSC	UBV hanteren; basisprofiel	UBV - Voorschrift: TLS-ALG-01	De 'ICT-beveiligingsrichtlijnen voor Transport Layer Security (TLS)' van NCSC wordt in basis gevolgd en toegepast, tenzij deze TLS-voorschriften specifiekere voorschrijft.
1. TLS	Onderscheid tussen M2M en H2M	UBV hanteren; basisprofiel	UBV - Advies: TLS-ALG-02	Het is van belang dat de gegevensuitwisseling voor M2M en H2M op separate hostnamen (FQDN) wordt afgehandeld.
1. TLS	Onderscheid tussen veilige en legacy-configuratie	UBV hanteren; basisprofiel	UBV - Voorschrift: TLS-ALG-03	Gegevensuitwisseling met een minder veilige configuratie dient op een separate hostnaam (FQDN) te worden afgehandeld.
1. TLS	Cipher Suites	NCSC hanteren o.b.v. UBV (Volgen van bovenliggende voorschriften)	NCSC - Bijlage C – Lijst met cipher suites	<p>Voorkeur:</p> <p>TLS_AES_256_GCM_SHA384            TLS_CHACHA20_POLY1305_SHA256            TLS_AES_128_GCM_SHA256</p> <p>Mag:</p> <p>TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384            TLS_ECDHE_ECDSA_WITH_CHACHA20_POLY1305_SHA256            TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256            TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384            TLS_ECDHE_RSA_WITH_CHACHA20_POLY1305_SHA256            TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256</p> <p>TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384            TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA            TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256            TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA            TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384            TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA            TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256            TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA            TLS_DHE_RSA_WITH_AES_256_GCM_SHA384            TLS_DHE_RSA_WITH_CHACHA20_POLY1305_SHA256            TLS_DHE_RSA_WITH_AES_128_GCM_SHA256            TLS_DHE_RSA_WITH_AES_256_CBC_SHA256            TLS_DHE_RSA_WITH_AES_256_CBC_SHA            TLS_DHE_RSA_WITH_AES_128_CBC_SHA256            TLS_DHE_RSA_WITH_AES_128_CBC_SHA</p> <p>Mag niet: overige (zie NCSC - Bijlage C - Lijst met cipher suites)</p>

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 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 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, curve 448, curve 25519 Mag: secp224r1
1. TLS	Ondersteunde finite field-groepen	NCSC hanteren o.b.v. UBV (Volgen van bovenliggende voorschriften)	NCSC - Ondersteunde finite field-groepen	Mag: ffdhe4096, ffdhe3072 (RFC 7919) Mag niet: ffdhe2048 (RFC 7919) en overige groepen
1. TLS	Cipher Suites	NCSC hanteren o.b.v. UBV (Volgen van bovenliggende voorschriften)	NCSC - Richtlijn B2-5	Alle ondersteunde algoritmeselecties zijn <b>Goed</b> , of de algoritmeselecties worden op basis van de voorgeschreven ordening door de servers gekozen.
1. TLS	Sleuteluitwisseling	NCSC hanteren o.b.v. UBV (Volgen van bovenliggende voorschriften)	NCSC - Richtlijn B4-1	Wanneer er voor de sleuteluitwisseling gebruik wordt gemaakt van DHE, dan is de geheime parameter tijdelijk van aard, willekeurig gekozen uit een uniforme verdeling en van een adequate omvang voor het gekozen finite field.
1. TLS	Sleuteluitwisseling	NCSC hanteren o.b.v. UBV (Volgen van bovenliggende voorschriften)	NCSC - Richtlijn B4-2	Wanneer er voor de sleuteluitwisseling gebruik wordt gemaakt van ECDHE, dan is de geheime parameter tijdelijk van aard, willekeurig gekozen uit een uniforme verdeling en van een adequate omvang voor de gekozen elliptische kromme.
1. TLS	Hashfuncties voor sleuteluitwisseling	NCSC hanteren o.b.v. UBV (Volgen van bovenliggende voorschriften)	NCSC - Hashfuncties voor sleuteluitwisseling (Tabel 5)	SHA2-ondersteuning voor handtekeningen: Ja (ondersteuning van SHA-256, SHA-384 of SHA-512)

1.1 TLS Opties	OCSP stapling	NCSC hanteren o.b.v. UBV (Volgen van bovenliggende voorschriften)	NCSC - OCSP stapling	Voorkeur: aan Mag: uit
1.1 TLS Opties	0-RTT	NCSC hanteren o.b.v. UBV (Volgen van bovenliggende voorschriften)	NCSC - 0-RTT	Uit (of n.v.t. voor TLS 1.3)
1.1 TLS Opties	Client-initiated renegotiation	NCSC hanteren o.b.v. UBV (Volgen van bovenliggende voorschriften)	NCSC - Client-initiated renegotiation	Voorkeur: Uit (of n.v.t. in TLS1.2 en ouder) Mag: Aan
1.1 TLS Opties	Compressie	NCSC hanteren o.b.v. UBV (Volgen van bovenliggende voorschriften)	NCSC - Compressie	Voorkeur: Geen compressie Mag: Compressie op applicatieniveau
1.1 TLS Opties	Insecure renegotiation	NCSC hanteren o.b.v. UBV (Volgen van bovenliggende voorschriften)	NCSC - Insecure renegotiation	Uit (of n.v.t. voor TLS 1.3)
Overig	HTTPS	UBV hanteren; basisprofiel	UBV - Voorschrift: 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	NCSC hanteren o.b.v. UBV (Volgen van bovenliggende voorschriften)	NCSC - Richtlijn B3-1	De server biedt een certificaat aan ter authenticatie.
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.
PKI	OIN	UBV hanteren; basisprofiel	UBV - Voorschrift: 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	UBV hanteren; basisprofiel	UBV - Voorschrift: TLS-PKI-02	Een wildcard certificaat mag niet gebruikt worden bij gegevensuitwisseling waarvan de classificatie Beschikbaarheid, Integriteit of Vertrouwelijkheid niveau 3 is. Bij een lagere classificatie (B, I of V is geen 3) is een wildcard certificaat wel toegestaan, echter wordt dit gezien de verhoogde kans op compromittatie van de private key niet geadviseerd.
PKI	Certificaat	UBV hanteren; basisprofiel	UBV - Voorschrift:	Het certificaat moet ondertekend zijn door een CA en de cliënt moet deze kunnen controleren op geldigheid.

TLS-PKI-03				
PKI	Certificaat	UBV hanteren; ontbreekt in DK	UBV - Advies: 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	Certificaat	NCSC hanteren o.b.v. UBV (Volgen van bovenliggende voorschriften)	NCSC - Hashfuncties voor certificaatverificatie (Tabel 3)	Voorkeur: SHA-512, SHA-384, SHA-256 Mag niet: SHA-1, MD5

## UBV Edukoppeling v1.2.1

Het Edukoppeling profiel is opgesteld op basis van de UBV TLS v1.1, NCSC ICT-beveiligingsrichtlijnen voor TLS v2.1 en Digikoppeling (DK) beveiligingsstandaarden en voorschriften v1.3.

Cat.	Onderwerp	Status	Ref.	Voorschrift
0. TLS Versie	TLS Versie	UBV hanteren; overgenomen van DK (TLS004)	UBV - Voorschrift: TLS-M2M-01	<p>TLS 1.0 en TLS 1.1 zijn niet toegestaan.</p> <p>Een Serviceaanbieder is verplicht TLS versie 1.2 te ondersteunen.</p> <p>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.</p>
1. TLS	TLS-richtlijn NCSC	UBV hanteren; in lijn met DK (TLS006)	UBV - Voorschrift: TLS-ALG-01	De 'ICT-beveiligingsrichtlijnen voor Transport Layer Security (TLS)' van NCSC wordt in basis gevolgd en toegepast, tenzij deze TLS-voorschriften specifiek voorschrijft.
1. TLS	Onderscheid tussen M2M en H2M	UBV hanteren; ontbreekt in DK	UBV - Advies: TLS-ALG-02	Het is van belang dat de gegevensuitwisseling voor M2M en H2M op separate hostnamen (FQDN) wordt afgehandeld.
1. TLS	Onderscheid tussen veilige en legacy-configuratie	UBV hanteren; ontbreekt in DK	UBV - Voorschrift: TLS-ALG-03	Gegevensuitwisseling met een minder veilige configuratie dient op een separate hostnaam (FQDN) te worden afgehandeld.
1. TLS	Cipher Suites	UBV hanteren; specifiek dan DK (TLSCIP001)	UBV - Voorschrift: TLS-M2M-02	<p>Een Serviceaanbieder is verplicht om alle onderstaande cipher suites in aangegeven volgorde te ondersteunen.</p> <p>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</p> <p>De cipher TLS_DHE mag achterwege gelaten worden, mits dit niet tot interoperabiliteitsproblemen leidt. Als deze wel wordt toegevoegd, alleen onder de voorwaarde dat:</p> <ul style="list-style-type: none"> <li>- RFC 7919 groepen gebruikt worden</li> <li>- Sleutellengte minimaal gelijk is aan de RSA sleutel</li> <li>- Eigen parameters voor DH instelbaar is</li> </ul> <p>Als Serviceafnemer mag een selectie hiervan gebruikt worden, uit oogpunt van efficiëntie. Daarbij wordt aanbevolen om de meest veilige cipher te kiezen (hoogste in de lijst).</p>



1. TLS	Poortnummer	UBV hanteren; tegenstrijdig met DK (TLS005)	UBV - Voorschrift: 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 PKI-overheid certificaten
1. TLS	Tweezijdige TLS	DK hanteren; ontbreekt in UBV	DK - TLS002	Tweezijdig TLS is verplicht
1. TLS	Hashfuncties voor sleuteluitwisseling	NCSC hanteren o.b.v. UBV (Volgen van bovenliggende voorschriften)	NCSC - Hashfuncties voor sleuteluitwisseling (Tabel 5)	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 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, curve 448, curve 25519 Mag: secp224r1
1. TLS	Sleuteluitwisseling	NCSC hanteren o.b.v. UBV (Volgen van bovenliggende voorschriften)	NCSC - Richtlijn B4-1	Wanneer er voor de sleuteluitwisseling gebruik wordt gemaakt van DHE, dan is de geheime parameter tijdelijk van aard, willekeurig gekozen uit een uniforme verdeling en van een adequate omvang voor het gekozen finite field.
1. TLS	Sleuteluitwisseling	NCSC hanteren o.b.v. UBV (Volgen van bovenliggende voorschriften)	NCSC - Richtlijn B4-2	Wanneer er voor de sleuteluitwisseling gebruik wordt gemaakt van ECDHE, dan is de geheime parameter tijdelijk van aard, willekeurig gekozen uit een uniforme verdeling en van een adequate omvang voor de gekozen elliptische kromme.
1.1 TLS Opties	Redirect	UBV hanteren; ontbreekt in DK	UBV - Voorschrift: 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 - Voorschrift: TLS-M2M-07	Elke cliënt moet ServerNameIndication (SNI) geïmplementeerd hebben.
1.1 TLS Opties	OCSP stapling	UBV hanteren; ontbreekt in DK	UBV - Advies: TLS-M2M-03	Bij voorkeur wordt OCSP-stapling op de server toegepast, zodat de cliënt niet afhankelijk is van een derde partij.  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 - Advies: 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 (of n.v.t. voor TLS 1.3)
1.1 TLS Opties	Client-initiated renegotiation	NCSC hanteren o.b.v. UBV (Volgen van bovenliggende voorschriften)	NCSC - Client-initiated renegotiation	Voorkeur: Uit (of n.v.t. in TLS1.2 en ouder) Mag: Aan
1.1 TLS Opties	Compressie	NCSC hanteren o.b.v. UBV (Volgen van bovenliggende voorschriften)	NCSC - Compressie	Voorkeur: Geen compressie Mag: Compressie op applicatieniveau
1.1 TLS Opties	Insecure renegotiation	NCSC hanteren o.b.v. UBV (Volgen van bovenliggende voorschriften)	NCSC - Insecure renegotiation	Uit (of n.v.t. voor TLS 1.3)
Berichtondertekening		DK hanteren; ontbreekt in UBV	DK - SIGN001	Signing met SHA-2 is verplicht (bij toepassing van 2W-be-S of 2W-be-SE profiel)
Berichtondertekening		DK hanteren; ontbreekt in UBV	DK - SIGN002	Signing conform XMLDSIG is verplicht (bij toepassing van 2W-be-S of 2W-be-SE profiel)
Berichtondertekening		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]
Berichtondertekening		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] (bij toepassing van 2W-be-S of 2W-be-SE profiel)
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 (bij toepassing van 2W-be-SE profiel)
Berichtversleuteling		DK hanteren; ontbreekt in UBV	DK - ENC002	Encryptie conform XML versleuteling [XML Encryption] is verplicht ( <a href="http://www.w3.org/TR/xmlenc-core/">http://www.w3.org/TR/xmlenc-core/</a> ) (bij toepassing van 2W-be-SE profiel)
Berichtversleuteling		DK hanteren; ontbreekt in UBV	DK - ENC003	De ondersteunde data encryption (data versleuteling) algoritmen zijn: 3DES AES128 AES256 (bij toepassing van 2W-be-SE profiel)
Berichtversleuteling		DK hanteren; ontbreekt in UBV	DK - ENC004	Het Key transport algorithm maakt gebruik van de RSA-OAEP algoritmen (bij toepassing van 2W-be-SE profiel)
PKI	CN	UBV hanteren; ontbreekt in DK	UBV - Voorschrift:	Maak alleen gebruik van een Fully Qualified Domain Name (FQDN).

TLS-M2M-06				
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	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).  Voor Serviceaanbieders geldt dat zij uiterlijk per 1-1-2021 gebruik van private root certificaten moeten ondersteunen.
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 - Advies: 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 - Voorschrift: TLS-M2M-08	Het certificaat wordt altijd gecontroleerd.
PKI	PKIoverheid	UBV hanteren; strenger dan DK (PKI002)	UBV - Voorschrift: 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 - Voorschrift: TLS-M2M-10	Een verlopen certificaat mag niet worden gebruikt.
PKI	PKIoverheid	UBV hanteren; ontbreekt in DK	UBV - Voorschrift: 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 - Voorschrift: 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	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.
PKI	Certificaat	NCSC hanteren o.b.v. UBV (Volgen van bovenliggende voorschriften)	NCSC - Richtlijn B3-1	De server biedt een certificaat aan ter authenticatie.

PKI	Certificaat	NCSC hanteren o.b.v. UBV (Volgen van bovenliggende voorschriften)	NCSC - Hashfuncties voor certificaatverifica tie (Tabel 3)	Voorkeur: SHA-512, SHA-384, SHA-256 Mag niet: SHA-1 , MD5
-----	-------------	--	--	--