edustandaard

UNIFORME BEVEILIGINGSVOORSCHRIFTEN
TRANSPORT LAYER SECURITY (TLS)

Datum	8-1-2026
Versie	1.3.1
Auteur	Edustandaard werkgroep Uniforme Beveiligingsvoorschriften

INHOUDSOPGAVE

Historie

Versie	Auteur	Toelichting	Datum
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
1.2	Jordy van den Elshout	Voorschriften voor domeinnaambeveiliging verwerkt onder paragraaf 2.4 'Integriteit van DNS-informatie' en 5.5 'CAA-record'. Op basis hiervan profielen bijgewerkt, incl. de wijziging uit Digikoppeling v1.4 m.b.t. verplicht gebruik van PKIoverheid root certificaat.	23 december 2021
1.3	Jordy van den Elshout	Bijgewerkt op basis van TLS-voorschriften 2025-05 (NCSC), gezien degradatie van ciphers en TLS-opties; van 'Voldoende' naar 'Uit te faseren'. Voor M2M is 1.3 verplicht gesteld incl. een nieuwe selectie van ciphers. Profielen zijn bijgewerkt, mede op basis van Digikoppeling beveiligingsvoorschriften v2.0.1	30 juli 2025
1.3.1	Jordy van den Elshout	Aanscherping na review door kerngroep. TLS-ALG-03 vervalt en TLS-PKI-05 aangescherpt m.b.t. trial-certificaten. Bijlage met uitzondering is verwijderd.	8 januari 2025

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.

Deze set uniforme beveiligingsvoorschriften richt zich in dit document op het gebruik van Transport Layer Security (TLS) en aanverwante beveiligingsaspecten voor het beveiligen van gegevensuitwisseling. Voor de beschrijving van TLS en bijbehorende begrippen, zoals certificaten, cipher suites, protocolversies en gerelateerde beveiligingsmechanismen, wordt aangesloten bij de TLS-beveiligingsrichtlijnen van het Nationaal Cyber Security Centrum (NCSC). Hoofdstuk 1 van deze richtlijnen beschrijft het doel, de werking en de belangrijkste begrippen.

Verschillende standaarden en afspraken, zoals Edukoppeling, het Edu-V afsprakenstelsel en Educatieve Distributie en Toegang (ECK DT), kunnen naar deze uniforme beveiligingsvoorschriften verwijzen in plaats van deze zelfstandig te 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 de Overstap Service Onderwijs (OSO). De afspraken hiervoor zijn gevat onder machine to machine (M2M).

De voorschriften zijn ook van toepassing op alle website en webdiensten die binnen het onderwijs gebruikt worden, aangezien deze doorgaans gebruikmaken van 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 ISO27001:2022, de standaard voor informatiebeveiliging. Deze voorschriften geven met name invulling aan de beheersmaatregelen 'A5.14 Overdragen van informatie' en 'A8.24 Gebruik van cryptografie'.

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 door de Edustandaard werkgroep Uniforme beveiligingsvoorschriften.

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 specifieker voorschrijft.

Welke voorschriften specifieker zijn dan NCSC en gezamenlijk van toepassing zijn, wordt in een profiel getoond (zie bijlage I: 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 Integriteit van DNS-informatie

Voor een veilig en betrouwbare gegevensuitwisseling, is de integriteit van DNS-informatie van belang.

2.3.1 DNSSEC

Domain Name System Security Extensions (DNSSEC) is een beveiliging die een digitale handtekening toevoegt aan DNS-informatie. *"Op deze manier wordt de integriteit van de DNS-informatie beschermd en kan worden gecontroleerd of het DNS-antwoord authentiek is en afkomstig is van de juiste bron."* (IBD, DNSSEC: Voorkom domeinfraude).

DNSSEC is daarmee een belangrijke randvoorwaarden voor een veilige en betrouwbare gegevensuitwisseling. De kans dat DNS-informatie wordt gemanipuleerd en de cliënt met een verkeerde host verbinding maakt wordt daarmee verkleind.

Voorschrift: TLS-ALG-04
Een domeinnaam die wordt gebruikt voor een gegevensuitwisseling dient beveiligd te zijn met DNSSEC

Implementatie: DNSSEC is een standaard dat toegepast wordt op het DNS-systeem: een optie voor het genereren en opnemen van de digitale handtekening bij een domeinnaam. Op internet.nl kan eenvoudig gecontroleerd worden of de domeinnaam beveiligd is met DNSSEC.

2.3.2 Toegangsbeveiliging DNS

Om de integriteit van DNS-informatie te beschermen, is toegangsbeveiliging tot de domeinregistratie (incl. verhuiscode) en het DNS-systeem ook van belang.

Domeinregistratie

Veel aanbieders van domeinregistratie bieden de mogelijkheid tot Multi-Factor Authenticatie (MFA). Hiermee wordt de toegang extra beveiligd voor a) het aanpassen NS record en b) het kunnen verhuizen van een domeinnaam.

DNS-systeem

Het DNS-systeem kan in eigen beheer zijn of bij een domeinregistratie gehost worden. In beide gevallen dient deze opgenomen te worden in de maatregel voor toegangsbeheer.

Voorschrift: TLS-ALG-05
Toegangsbeheer is van toepassing op de toegang tot de domeinregistratie en het DNS-systeem. Indien toegang via internet mogelijk is, wordt geadviseerd om Multi-Factor Authenticatie (MFA) toe te passen.

2.4 Beheer en actualiteit

Om de veiligheid en actualiteit van TLS-configuraties te borgen, is het noodzakelijk om toezicht te houden op het gebruik van TLS-versies, cipher suites en certificaten. Structurele monitoring en rapportage ondersteunen de tijdige uitfasering van verouderde instellingen en dragen bij aan continu verbeterbeheer, zoals beoogd in de NCSC TLS-richtlijnen.

Voorschrift: TLS-ALG-06
Het gebruik van TLS-versies, cipher suites en certificaten wordt periodiek gecontroleerd met geautomatiseerde scans. De resultaten worden minimaal jaarlijks geëvalueerd en vastgelegd, zodat het gebruik van verouderde of niet-conforme configuraties tijdig wordt beëindigd.

Automatische controles kunnen worden uitgevoerd met beveiligings- of configuratiescanners die TLS-versies en cipher-suites identificeren (bijv. OpenSSL-scans, Qualys SSL Labs, of interne vulnerability management tools). Deze maatregel ondersteunt de naleving van de NCSC-kwalificaties (“Onvoldoende”, “Uit te faseren”, “Voldoende”, “Goed”) en vormt onderdeel van het proces van continu verbeterbeheer.

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 3 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 minimaal één versie van TLS met een selectie van cipher suites verplicht gesteld. Voor toekomstbestendigheid wordt TLS1.3 voorgeschreven, mede gezien toekomstige dreiging van quantum technologie. Om ServiceAfnemers de tijd te geven om volledig over te stappen op TLS 1.3, wordt TLS 1.2 voorlopig ook verplicht gesteld voor de ServiceAanbieder.

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 en 1.3 te ondersteunen. Vanaf 1-1-2027 is TLS versie 1.2 niet meer verplicht.

3.2.2 Algoritmeselecties

Door Door het vaststellen van een minimale set cipher suites wordt aangesloten bij de algoritmeselecties uit de NCSC TLS-richtlijnen (paragraaf 3.2). Hiermee wordt vastgelegd welke cryptografische mechanismen zijn toegestaan voor het opzetten van een beveiligde verbinding, zoals de manier van authenticatie, sleuteluitwisseling, versleuteling en hashing. Deze mechanismen vormen samen een cipher suite.

De richtlijn van NCSC wordt gevolgd: "*Geef de voorkeur voor het gebruik van **Goede** instellingen, aangevuld met **Voldoende** instellingen ter ondersteuning van oudere software indien noodzakelijk.*". Wat betreft de volgorde, wordt deze gevolgd uit 'Bijlage B - 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.

Voorschrift: TLS-M2M-02 (Interoperabiliteit en veiligheid)

Een Serviceaanbieder is verplicht om alle onderstaande cipher suites te ondersteunen.

TLS 1.3
TLS_AES_256_GCM_SHA384
TLS_AES_128_GCM_SHA256

TLS 1.2
TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256

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 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. Voor de interoperabiliteit dient een serviceaanbieder alle verplichte cipher suites te ondersteunen.

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, voordat de gegevensuitwisseling plaatsvindt.

3.3.1 ongeldig 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.

Wanneer een certificaat is verlopen, 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-09 (Veiligheid)

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

3.3.2 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.

3.3.3 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).

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 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.

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 ververst als het certificaat ingetrokken is.

3.3.4 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.

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

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

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.

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[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.
- '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 van NCSC wordt gevolgd: "Geef de voorkeur voor het gebruik van **Goede** instellingen, aangevuld met **Voldoende** instellingen ter ondersteuning van oudere software indien noodzakelijk. ". Wat betreft de volgorde, wordt deze gevolgd uit 'Bijlage B - Lijst met cipher suites' van de TLS-richtlijnen van NCSC. Cipher suites met classificatie 'Voldoende' **mag** gebruikt worden, echter heeft 'Goed' de **voorkeur.**

Het gebruik van **Goede algoritmes** biedt niet alleen een hogere mate van veiligheid en forward secrecy, maar draagt ook bij aan bescherming tegen de opkomende **quantumdreiging**. De TLS-richtlijnen 2025-05 van het NCSC adviseren het gebruik van hybride sleuteluitwisselingen, zoals **X25519MLKEM768**, die extra weerstand bieden tegen aanvallen met toekomstige quantumcomputers.

Advies: TLS-H2M-01 (Veiligheid)
Overweeg het configureren van hybride sleuteluitwisselingen om de weerbaarheid tegen de dreiging quantumcomputers te vergroten.

4.2.3 OCSP stapling

OCSP-stapling 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 gebeurt. Dat betekent dat dit door middel van HTTPS moet verlopen. Daarnaast is het tegenwoordig gewoon

[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.

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.

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.

Voor ontwikkel-, test- en acceptatieomgevingen bestaan ook certificaten die uitsluitend bedoeld zijn voor testdoeleinden, zoals certificaten uit een Trial-CA. Deze certificaten bieden geen gecontroleerde organisatie-identiteit en kunnen in sommige gevallen zelfs een OIN bevatten zonder dat hier een geldige validatie tegenover staat. Wanneer dergelijke certificaten in een productieomgeving worden gebruikt, bestaat het risico dat een organisatie onterecht als een betrouwbare partij wordt herkend. Dit kan leiden tot fouten of verstoringen in ketens waar het OIN wordt gebruikt voor identificatie. Daarom mag in productie uitsluitend worden gewerkt met certificaten uit de reguliere PKIoverheid-keten.

[4] 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 PKIoverheid plaats te vinden. In productieomgevingen mogen uitsluitend certificaten uit de reguliere PKIoverheid-keten worden gebruikt. Certificaten uit test- of Trial-CA's, of andere certificaten die geen gevalideerde PKIoverheid-identiteit borgen zijn in productie niet toegestaan. Ook de bijbehorende CA-keten mag niet op productieomgevingen aanwezig zijn.

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[5]. 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.

[5] Zie whitepaper van National Security Agency/Central Security Service: Avoid Dangers of Wildcard TLS Certificates and the ALPACA Technique

5.5 CAA-record

"CAA is een DNS-record dat domeineigenaren extra controle geeft over SSL-certificaten die worden uitgegeven voor diens domeinen. Met het CAA record geeft een domeineigenaar aan welke certificate authority (CA) certificaten uit mag geven voor diens domeinen. Een domein eigenaar kan dit zelf regelen zonder dat hier medewerking vanuit de CA voor nodig is. Zo kan de eigenaar van een domein zelf bepalen welke CA's certificaten mogen uitgeven voor zijn of haar domeinen. CA's moeten bij uitgifte van een certificaat verplicht het CAA record van het betreffende domein controleren" (bron: Forum Standaardisatie, CAA)

CAA is alleen effectief als het DNS waarin het CAA-record geadministreerd wordt, is beschermd met DNSSEC. Zonder DNSSEC-bescherming kan een aanvaller het DNS-verkeer omleiden, waardoor het CAA-record niet meer effectief is. De CAA-specificatie (RFC 6844) adviseert dan ook uitdrukkelijk het gebruik van CAA in combinatie met DNSSEC.

Het toevoegen van een CAA record verkleint daarmee de kans dat een certificaat onbedoeld en ongewenst door een onbevoegde CA wordt uitgegeven en bv. misbruikt wordt voor een *man-in-the-middle* aanval.

Met een CAA-record kan niet alleen aangegeven worden welke CA het certificaat mag uitgeven, maar ook welk soort certificaat. Een gewoon of wildcard-certificaat. Daarmee kan tevens het beleid - welke certificaten gebruikt mogen worden - technisch afgedwongen worden, waarmee voorkomen wordt dat een wildcard-certificaat voor een domeinnaam uitgegeven kan worden.

Advies: TLS-PKI-05 (Veiligheid)
Voeg CAA-records toe aan de gebruikte domeinnamen om aan te geven welke CA, welk certificaat (wildcard of gewoon) mag uitgeven. Zorg dat de CAA-records alleen bestaan uit CA's en type certificaten die ook daadwerkelijk gebruikt (mogen) worden voor dat desbetreffende domeinnaam. Voeg tevens per domeinnaam een CAA-record met een e-mailadres voor melding op misbruik toe. (Bv. CAA-record: iodef abuse@domeinnaam.nl)

BIJLAGE I: 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 v1.3

Het basisprofiel op basis van de UBV TLS v1.3 en NCSC ICT-beveiligingsrichtlijnen voor TLS 2025-05.

Onderwerp	Status	Ref.	Voorschrift
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 en 1.3 te ondersteunen. Vanaf 1-1-2027 is TLS versie 1.2 niet meer verplicht.
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 specifieker voorschrijft.
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.
DNSSEC	UBV hanteren; basisprofiel	UBV - Voorschrift: TLS-ALG-04	Een domeinnaam dat wordt gebruikt voor een gegevensuitwisseling dient beveiligd te zijn met DNSSEC
Toegangsbeveiliging DNS	UBV hanteren; basisprofiel	UBV - Voorschrift: TLS-ALG-05	Toegangsbeheer is van toepassing op de toegang tot de domeinregistratie en het DNS-systeem. Indien toegang via internet mogelijk is, wordt geadviseerd om Multi-Factor Authenticatie (MFA) toe te passen.
Beheer en actualiteit	UBV hanteren; basisprofiel	UBV - Voorschrift: TLS-ALG-06	Het gebruik van TLS-versies, cipher suites en certificaten wordt periodiek gecontroleerd met geautomatiseerde scans. De resultaten worden minimaal jaarlijks geëvalueerd en vastgelegd, zodat het gebruik van verouderde of niet-conforme configuraties tijdig wordt beëindigd.
Cipher Suites	UBV hanteren; basisprofiel	UBV - Voorschrift: TLS-M2M-02	Een Serviceaanbieder is verplicht om alle onderstaande cipher suites in aangegeven volgorde te ondersteunen. TLS1.3 TLS_AES_256_GCM_SHA384 TLS_AES_128_GCM_SHA256 TLS 1.2 TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 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).

Hashfuncties voor sleuteluitwisseling	NCSC hanteren o.b.v. UBV (Volgen van bovenliggende voorschriften)	NCSC - 3.3.5 Hashfuncties voor TLS	Voorkeur: SHA-256, -384 en -512 Mag: geen; overige mogen niet gebruikt worden
Lengte van RSA-sleutels	NCSC hanteren o.b.v. UBV (Volgen van bovenliggende voorschriften)	NCSC - 3.3.2.1 Lengte van RSA-sleutels	Voorkeur: minimaal 3072 bit Mag: geen; overige mogen niet gebruikt worden
Padding schema	NCSC hanteren o.b.v. UBV (Volgen van bovenliggende voorschriften)	NCSC - 3.3.2.1 Padding schema	Mag: PSA-PSS Mag niet: PSA-PKCS#1 v1.5
Ondersteunde elliptische krommen	NCSC hanteren o.b.v. UBV (Volgen van bovenliggende voorschriften)	NCSC - 3.3.2.1 Elliptic curce	Voorkeur: n.v.t. Mag: secp512r1, secp384r1, secp256r1, curve448*, curve25519*, brainpoolP512r1, brainpoolP384r1 en brainpoolP256r1 *Enkel te gebruiken voor ECDHE
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.
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.
Redirect	UBV hanteren; basisprofiel	UBV - Voorschrift: TLS-M2M-05	Er mag geen gebruik gemaakt worden van redirects die vanaf HTTP redirecten naar HTTPS.
SNI	UBV hanteren; basisprofiel	UBV - Voorschrift: TLS-M2M-07	Elke cliënt moet ServerNameIndication (SNI) geïmplementeerd hebben.
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 ververst als het certificaat ingetrokken is.
0-RTT	NCSC hanteren o.b.v. UBV (Volgen van bovenliggende voorschriften)	NCSC - 3.4.4 Sessie hervatten (0-RTT)	Geen 0-RTT (of n.v.t. voor TLS 1.2)
Client-initiated renegotiation	NCSC hanteren o.b.v. UBV (Volgen van bovenliggende voorschriften)	NCSC - 3.4.2 Renegotiation	Bij gebruik van TLS1.2: Voorkeur: Uit Mag: Gelimiteerd, secure renegotiation N.v.t. bij TLS1.3
Compressie	NCSC hanteren o.b.v. UBV (Volgen van bovenliggende voorschriften)	NCSC - 3.4.1 Compressie	Voorkeur: Geen compressie; n.v.t. met TLS1.3 Mag: Compressie op applicatieniveau

Sleuteluitwisseling	NCSC hanteren o.b.v. UBV (Volgen van bovenliggende voorschriften)	NCSC - 3.3.3 Sleuteluitwisseling	Voorkeur: X25519MLKEM768, SecP256r1MLKEM768, SecP384r1MLKEM1024 Verplicht: ECDHE Mag niet: DHE, RSA, DH, ECDH, KRB59, NULL, PSK9, SR
Sessie hervatten (Sessie-ID's, sessietickets)	NCSC hanteren o.b.v. UBV (Volgen van bovenliggende voorschriften)	NCSC - 3.4.2 Sessie hervatten (Sessie-ID's, sessietickets)	Voorkeur: Geen optie tot hervatting, of Sessietickets)TLS1.3) Mag: Sessietickets of Sessie-ID's + aanvullende beschermingsmaatregelen* * Ter bescherming van de opslagen sessie-parameter en.of encryptiesleiutel voor sessietickets. Uit bruikbaarheidsoogpunt genieten sessietickets de voorkeur, gegeven de extra overhead die het gebruik van Sessie-ID's met zich meebrengt.
Certificaat	NCSC hanteren o.b.v. UBV (Volgen van bovenliggende voorschriften)	NCSC - 3.3.2 Authenticatie	Maak gebruik van authenticatie op basis van X509 certificaten. Verplicht: RSA
CN	UBV hanteren; ontbreekt in DK	UBV - Voorschrift: TLS-M2M-06	Maak alleen gebruik van een Fully Qualified Domain Name (FQDN).
Certificaat controle	UBV hanteren; basisprofiel	UBV - Voorschrift: TLS-M2M-08	Het certificaat wordt altijd gecontroleerd, voordat de gegevensuitwisseling plaatsvindt.
Certificaat controle	UBV hanteren; basisprofiel	UBV - Voorschrift: TLS-M2M-09	Een certificaat dat is verlopen, ingetrokken, of waarvan niet kan worden gecontroleerd of het is ingetrokken, mag niet worden gebruikt.
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.
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.
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. In productieomgevingen mogen uitsluitend certificaten uit de reguliere PKIoverheid-keten worden gebruikt. Certificaten uit test- of Trial-CA's, of andere certificaten die geen gevalideerde PKIoverheid-identiteit borgen zijn in productie niet toegestaan. Ook de bijbehorende CA-keten mag niet op productieomgevingen aanwezig zijn.
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.
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.
Certificaat	UBV hanteren; basisprofiel	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.

Certificaat	UBV hanteren; basisprofiel	UBV - Advies: TLS-PKI-05	Voeg CAA-records toe aan de gebruikte domeinnamen om aan te geven welke CA, welk certificaat (wildcard of gewoon) mag uitgeven. Zorg dat de CAA-records alleen bestaan uit CA's en type certificaten die ook daadwerkelijk gebruikt (mogen) worden voor dat desbetreffende domeinnaam. Voeg tevens per domeinnaam een CAA-record met een e-mailadres voor melding op misbruik toe. (Bv. CAA-record: iodef abuse@domeinnaam.nl)
TLS-bibliotheek	NCSC hanteren o.b.v. UBV (Volgen van bovenliggende voorschriften)	NCSC - Randvoorwaarden: TLS-bibliotheken	Kies voor een betrouwbare TLS-bibliotheek die past bij jouw toepassing.* Zie TLS-Beveiligingsrichtlijnen Hoofdstuk 4. Randvoorwaarden
Toevalsgetallen	NCSC hanteren o.b.v. UBV (Volgen van bovenliggende voorschriften)	NCSC - Randvoorwaarden: Toevalsgetallen	De meeste besturingssystemen en TLS-bibliotheken bevatten een goede, cryptografisch veilige PRNG. Identificeer welke PRNG er gebruikt wordt in jouw TLS-bibliotheek en onderzoek of deze hoge kwaliteits-toevalsgetallen genereert (d.w.z. onvoorspelbare toevalsgetallen). Consulteer hiervoor de (leverancier van) de TLS-bibliotheek die je gebruikt voor jouw toepassing. Van de volgende RNG is bekend dat hij onveilig is: Dual EC DRBG [22.* Zie TLS-Beveiligingsrichtlijnen Hoofdstuk 4. Randvoorwaarden

Basisprofiel H2M v1.3

Het basisprofiel op basis van de UBV TLS v1.3 en NCSC ICT-beveiligingsrichtlijnen voor TLS 2025-05.

Onderwerp	Status	Ref.	Voorschrift
TLS Versie	NCSC hanteren o.b.v. UBV (Volgen van bovenliggende voorschriften)	NCSC - 3.3.1 Versies	Voorkeur: TLS1.3 Mag: TLS1.2 Mag niet: TLS1.1, TLS 1.0 en SSL
Certificaat	NCSC hanteren o.b.v. UBV (Volgen van bovenliggende voorschriften)	NCSC - 3.3.2 Authenticatie	Maak gebruik van authenticatie op basis van X509 certificaten. Voorkeur: n.v.t. Mag: ECDSA, RSA (RSA-PSS) en EdDSA* * Maak gebruik van Elliptic curve Ed448 of Ed25519
Cipher Suites	NCSC hanteren o.b.v. UBV (Volgen van bovenliggende voorschriften)	NCSC - Bijlage B – Lijst met cipher suites	Voorkeur TLS_AES_256_GCM_SHA384 TLS_CHACHA20_POLY1305_SHA256 Mag TLS_AES_128_GCM_SHA256 TLS_AES_128_CCM_SHA256 TLS_ECDHE_ECDSA_WITH_CHACHA20_POLY1305_SHA256 TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384 TLS_ECDHE_ECDSA_WITH_AES_256_CCM TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 TLS_ECDHE_ECDSA_WITH_AES_128_CCM TLS_ECDHE_RSA_WITH_CHACHA20_POLY1305_SHA256 TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA25 Mag niet: overige met de status Uit te faseren. Zie NCSC - Bijlage B - Lijst met cipher suites.
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 specifieker voorschrijft.
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.
Beheer en actualiteit	UBV hanteren; basisprofiel	UBV - Voorschrift: TLS-ALG-06	Het gebruik van TLS-versies, cipher suites en certificaten wordt periodiek gecontroleerd met geautomatiseerde scans. De resultaten worden minimaal jaarlijks geëvalueerd en vastgelegd, zodat het gebruik van verouderde of niet-conforme configuraties tijdig wordt beëindigd.
Ondersteun de finite field-groepen	NCSC hanteren o.b.v. UBV (Volgen van bovenliggende voorschriften)	NCSC - Ondersteunde finite field-groepen	N.v.t. Wordt gebruikt met DHE; deze mag niet gebruikt worden.
DNSSEC	UBV hanteren; basisprofiel	UBV - Voorschrift: TLS-ALG-04	Een domeinnaam dat wordt gebruikt voor een gegevensuitwisseling dient beveiligd te zijn met DNSSEC
Toegangsbeveiliging DNS	UBV hanteren; basisprofiel	UBV - Voorschrift: TLS-ALG-05	Toegangsbeheer is van toepassing op de toegang tot de domeinregistratie en het DNS-systeem. Indien toegang via internet mogelijk is, wordt geadviseerd om Multi-Factor Authenticatie (MFA) toe te passen.
Sleuteluitwisseling	UBV hanteren; basisprofiel	UBV - Advies: TLS-H2M-01	Overweeg het configureren van hybride sleuteluitwisselingen om de weerbaarheid tegen de dreiging quantumcomputers te vergroten.

Ondersteun de elliptische krommen	NCSC hanteren o.b.v. UBV (Volgen van bovenliggende voorschriften)	NCSC - 3.3.2.1 Elliptic curce	Voorkeur: n.v.t. Mag: secp512r1, secp384r1, secp256r1, curve448*, curve25519*, brainpoolP512r1, brainpoolP384r1 en brainpoolP256r1 *Enkel te gebruiken voor ECDHE
Lengte van RSA-sleutels	NCSC hanteren o.b.v. UBV (Volgen van bovenliggende voorschriften)	NCSC - 3.3.2.1 Lengte van RSA-sleutels	Voorkeur: minimaal 3072 bit Mag: geen; overige mogen niet gebruikt worden
Padding schema	NCSC hanteren o.b.v. UBV (Volgen van bovenliggende voorschriften)	NCSC - 3.3.2.1 Padding schema	Mag: PSA-PSS Mag niet: PSA-PKCS#1 v1.5
Sleuteluitwisseling	NCSC hanteren o.b.v. UBV (Volgen van bovenliggende voorschriften)	NCSC - 3.3.3 Sleuteluitwisseling	Voorkeur: X25519MLKEM768, SecP256r1MLKEM768, SecP384r1MLKEM1024 Mag: ECDHE Mag niet: DHE, RSA, DH, ECDH, KRB59, NULL, PSK9, SR
Hashfuncties voor bulkversleuteling en het genereren van random numbers	NCSC hanteren o.b.v. UBV (Volgen van bovenliggende voorschriften)	NCSC - 3.3.5 Hashfuncties voor TLS	Voorkeur: SHA-256, -384 en -512 Mag: geen; overige mogen niet gebruikt worden
Compressie	NCSC hanteren o.b.v. UBV (Volgen van bovenliggende voorschriften)	NCSC - 3.4.1 Compressie	Voorkeur: Geen compressie; n.v.t. met TLS1.3 Mag: Compressie op applicatieniveau
Client-initiated renegotiation	NCSC hanteren o.b.v. UBV (Volgen van bovenliggende voorschriften)	NCSC - 3.4.2 Renegotiation	Bij gebruik van TLS1.2: Voorkeur: Uit Mag: Gelimiteerd, secure renegotiation N.v.t. bij TLS1.3
Sessie hervatten (Sessie-ID's, sessietickets)	NCSC hanteren o.b.v. UBV (Volgen van bovenliggende voorschriften)	NCSC - 3.4.3 Sessie hervatten (Sessie-ID's, sessietickets)	Voorkeur: Geen optie tot hervatting, of Sessietickets)TLS1.3) Mag: Sessietickets of Sessie-ID's + aanvullende beschermingsmaatregelen* * Ter bescherming van de opslagen sessie-parameter en.of encryptiesleiutel voor sessietickets. Uit bruikbaarheidsoogpunt genieten sessietickets de voorkeur, gegeven de extra overhead die het gebruik van Sessie-ID's met zich meebrengt.
0-RTT	NCSC hanteren o.b.v. UBV (Volgen van bovenliggende voorschriften)	NCSC - 3.4.4 Sessie hervatten (0-RTT)	Geen 0-RTT (of n.v.t. voor TLS 1.2)
OCSP stapling	NCSC hanteren o.b.v. UBV (Volgen van bovenliggende voorschriften)	NCSC - 3.4.5 Certificaatstatuscontrole (OCSP-stapling)	Configureer het gebruik van OCSP-stapling op jouw server als dit mogelijk is. Hiermee bied je jouw clients een privacyvriendelijke manier om de herroepingsstatus van jouw certificaat te controleren. Let op dat sommige CA's geen ondersteuning bieden voor OCSP vanuit privacyoverwegingen. In de praktijk is het daardoor niet altijd mogelijk om OCSP-stapling te configureren
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.
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.

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. In productieomgevingen mogen uitsluitend certificaten uit de reguliere PKIoverheid-keten worden gebruikt. Certificaten uit test- of Trial-CA's, of andere certificaten die geen gevalideerde PKIoverheid-identiteit borgen zijn in productie niet toegestaan. Ook de bijbehorende CA-keten mag niet op productieomgevingen aanwezig zijn.
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.
Certificaat	UBV hanteren; basisprofiel	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.
Certificaat	UBV hanteren; basisprofiel	UBV - Advies: TLS-PKI-05	Voeg CAA-records toe aan de gebruikte domeinnamen om aan te geven welke CA, welk certificaat (wildcard of gewoon) mag uitgeven. Zorg dat de CAA-records alleen bestaan uit CA's en type certificaten die ook daadwerkelijk gebruikt (mogen) worden voor dat desbetreffende domeinnaam. Voeg tevens per domeinnaam een CAA-record met een e-mailadres voor melding op misbruik toe. (Bv. CAA-record: iodef abuse@domeinnaam.nl)
TLS-bibliotheek	NCSC hanteren o.b.v. UBV (Volgen van bovenliggende voorschriften)	NCSC - Randvoorwaarden: TLS-bibliotheken	Kies voor een betrouwbare TLS-bibliotheek die past bij jouw toepassing.* Zie TLS-Beveiligingsrichtlijnen Hoofdstuk 4. Randvoorwaarden
Toevalsgetallen	NCSC hanteren o.b.v. UBV (Volgen van bovenliggende voorschriften)	NCSC - Randvoorwaarden: Toevalsgetallen	De meeste besturingssystemen en TLS-bibliotheken bevatten een goede, cryptografisch veilige PRNG. Identificeer welke PRNG er gebruikt wordt in jouw TLS-bibliotheek en onderzoek of deze hoge kwaliteits-toevalsgetallen genereert (d.w.z. onvoorspelbare toevalsgetallen). Consulteer hiervoor de (leverancier van) de TLS-bibliotheek die je gebruikt voor jouw toepassing. Van de volgende RNG is bekend dat hij onveilig is: Dual EC DRBG Zie TLS-Beveiligingsrichtlijnen Hoofdstuk 4. Randvoorwaarden

UBV Edukoppeling v1.3

Het Edukoppeling profiel is opgesteld op basis van de UBV TLS v1.3, NCSC ICT-beveiligingsrichtlijnen voor TLS 2025-05 en Digikoppeling (DK) beveiligingsstandaarden en voorschriften v2.0.1.

Onderwerp	Status	Ref.	Voorschrift
TLS Versie	UBV hanteren; overgenomen van DK (TLS004)	UBV - Voorschrift: TLS-M2M-01	TLS 1.0 en TLS 1.1 zijn niet toegestaan. Een Serviceaanbieder is verplicht TLS versie 1.2 en 1.3 te ondersteunen. Vanaf 1-1-2027 is TLS versie 1.2 niet meer verplicht.
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
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 specifieker voorschrijft.
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.
DNSSEC	UBV hanteren; ontbreekt in DK	UBV - Voorschrift: TLS-ALG-04	Een domeinnaam dat wordt gebruikt voor een gegevensuitwisseling dient beveiligd te zijn met DNSSEC
Toegangsbeveiliging DNS	UBV hanteren; ontbreekt in DK	UBV - Voorschrift: TLS-ALG-05	Toegangsbeheer is van toepassing op de toegang tot de domeinregistratie en het DNS-systeem. Indien toegang via internet mogelijk is, wordt geadviseerd om Multi-Factor Authenticatie (MFA) toe te passen.
Beheer en actualiteit	UBV hanteren; ontbreekt in DK	UBV - Voorschrift: TLS-ALG-06	Het gebruik van TLS-versies, cipher suites en certificaten wordt periodiek gecontroleerd met geautomatiseerde scans. De resultaten worden minimaal jaarlijks geëvalueerd en vastgelegd, zodat het gebruik van verouderde of niet-conforme configuraties tijdig wordt beëindigd.
Cipher Suites	UBV hanteren; specifieker dan DK (TLSCIP001)	UBV - Voorschrift: TLS-M2M-02	Een Serviceaanbieder is verplicht om alle onderstaande cipher suites in aangegeven volgorde te ondersteunen. TLS1.3 TLS_AES_256_GCM_SHA384 TLS_AES_128_GCM_SHA256 TLS 1.2 TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 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).
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.
Authenticatie	DK hanteren; in lijn met UBV (TLS-PKI-01)	DK - TLS001	Authenticatie is verplicht met TLS en PKIoverheid certificaten
Tweezijdige TLS	DK hanteren; ontbreekt in UBV	DK - TLS002	Tweezijdig TLS is verplicht

Hashfuncties voor sleuteluitwisseling	NCSC hanteren o.b.v. UBV (Volgen van bovenliggende voorschriften)	NCSC - 3.3.5 Hashfuncties voor TLS	Voorkeur: SHA-256, -384 en -512 Mag: geen; overige mogen niet gebruikt worden
Lengte van RSA-sleutels	NCSC hanteren o.b.v. UBV (Volgen van bovenliggende voorschriften)	NCSC - 3.3.2.1 Lengte van RSA-sleutels	Voorkeur: minimaal 3072 bit Mag: geen; overige mogen niet gebruikt worden
Padding schema	NCSC hanteren o.b.v. UBV (Volgen van bovenliggende voorschriften)	NCSC - 3.3.2.1 Padding schema	Mag: PSA-PSS Mag niet: PSA-PKCS#1 v1.5
Ondersteunde elliptische krommen	NCSC hanteren o.b.v. UBV (Volgen van bovenliggende voorschriften)	NCSC - 3.3.2.1 Elliptic curce	Voorkeur: n.v.t. Mag: secp512r1, secp384r1, secp256r1, curve448*, curve25519*, brainpoolP512r1, brainpoolP384r1 en brainpoolP256r1 *Enkel te gebruiken voor ECDHE
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.
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.
SNI	UBV hanteren; ontbreekt in DK	UBV - Voorschrift: TLS-M2M-07	Elke cliënt moet ServerNameIndication (SNI) geïmplementeerd hebben.
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.
Client-initiated renegotiation	NCSC hanteren o.b.v. UBV (Volgen van bovenliggende voorschriften)	NCSC - Client-initiated renegotiation	Voorkeur: Uit bij TLS1.2; n.v.t. met TLS1.3 Mag: Gelimiteerd, secure renegotiation
Compressie	NCSC hanteren o.b.v. UBV (Volgen van bovenliggende voorschriften)	NCSC - 3.4.1 Compressie	Voorkeur: Geen compressie; n.v.t. met TLS1.3 Mag: Compressie op applicatieniveau
Sessie hervatten (0-RTT)	NCSC hanteren o.b.v. UBV (Volgen van bovenliggende voorschriften)	NCSC - 3.4.4 Sessie hervatten (0-RTT)	Geen 0-RTT (of n.v.t. voor TLS 1.2)
Sessie hervatten (Sessie-ID's, sessietickets)	NCSC hanteren o.b.v. UBV (Volgen van bovenliggende voorschriften)	NCSC - 3.4.3 Sessie hervatten (Sessie-ID's, sessietickets)	Voorkeur: Geen optie tot hervatting, of Sessietickets)TLS1.3) Mag: Sessietickets of Sessie-ID's + aanvullende beschermingsmaatregelen* * Ter bescherming van de opslagen sessie-parameter en.of encryptiesleiutel voor sessietickets. Uit bruikbaarheidsoogpunt genieten sessietickets de voorkeur, gegeven de extra overhead die het gebruik van Sessie-ID's met zich meebrengt.
Sleuteluitwisseling	NCSC hanteren o.b.v. UBV (Volgen van bovenliggende voorschriften)	NCSC - 3.3.3 Sleuteluitwisseling	Voorkeur: X25519MLKEM768, SecP256r1MLKEM768, SecP384r1MLKEM1024 Verplicht: ECDHE Mag niet: DHE, RSA, DH, ECDH, KRB59, NULL, PSK9, SR
	DK hanteren; ontbreekt in UBV	DK - SIGN001	Signing met SHA-2 is verplicht: [minimaal SHA-256] (bij toepassing van 2W-be-S of 2W-be-SE profiel)

	DK hanteren; ontbreekt in UBV	DK - SIGN002	Signing conform XMLDSIG is verplicht (bij toepassing van 2W-be-S of 2W-be-SE profiel)
	DK hanteren; ontbreekt in UBV	DK - SIGN003	Het DigestMethod Algorithm moet gebruik maken van een van de volgende algoritmen: [SHA-256] [SHA-384] 5.3.1.15.2.1.1 [SHA-512]
	DK hanteren; ontbreekt in UBV	DK - SIGN004	Het SignatureMethod Algorithm kan gebruik maken van een van de volgende algoritmen: [SHA-256] [SHA-384] [SHA-512] (bij toepassing van 2W-be-S of 2W-be-SE profiel)
	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)
	DK hanteren; ontbreekt in UBV	DK - ENC002	Encryptie conform XML versleuteling [XML Encryption] is verplicht (http://www.w3.org/TR/xmlenc-core/) (bij toepassing van 2W-be-SE profiel)
	DK hanteren; ontbreekt in UBV	DK - ENC003	De ondersteunde data encryption (data versleuteling) algoritmen zijn: 3DES(*) AES128 AES256 - GCM mode (bij toepassing van 2W-be-SE profiel) (*) 3DES-encryptie verouderd: Niet gebruiken. 3DES-decryptie toegestaan voor legacy applicaties
	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)
CN	UBV hanteren; ontbreekt in DK	UBV - Voorschrift: TLS-M2M-06	Maak alleen gebruik van een Fully Qualified Domain Name (FQDN).
PKIoverheid	UBV hanteren; ontbreekt in DK	UBV - Voorschrift: TLS-M2M-08	Het certificaat wordt altijd gecontroleerd, voordat de gegevensuitwisseling plaatsvindt.
PKIoverheid	UBV hanteren; strenger dan DK (PKI002)	UBV - Voorschrift: TLS-M2M-09	Een certificaat dat is verlopen, ingetrokken, of waarvan niet kan worden gecontroleerd of het is ingetrokken, mag niet worden gebruikt.
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.
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.
OIN	DK hanteren; in lijn met UBV (TLS-PKI-01)	DK - Paragraaf 3.1	Verplicht: PKIoverheid certificaten & CRL Profile In productieomgevingen mogen uitsluitend certificaten uit de reguliere PKIoverheid-keten worden gebruikt. Certificaten uit test- of Trial-CA's, of andere certificaten die geen gevalideerde PKIoverheid-identiteit borgen zijn in productie niet toegestaan. Ook de bijbehorende CA-keten mag niet op productieomgevingen aanwezig zijn.
PKIoverheid	DK hanteren (zonder uitzondering); in lijn met UBV (TLS-PKI-02)	DK - PKI005	Het certificaat moet zijn van het type PKIoverheid private root (PKI Staat der Nederlanden Private Root) Voor Serviceaanbieders en Servicegebruikers geldt dat zij vanaf 1-1-2021 gebruik moeten maken van private root certificaten
PKIoverheid	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.
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.
PKIoverheid	UBV hanteren; ontbreekt in DK	UBV - Advies: TLS-PKI-05	Voeg CAA-records toe aan de gebruikte domeinnamen om aan te geven welke CA, welk certificaat (wildcard of gewoon) mag uitgeven. Zorg dat de CAA-records alleen bestaan uit CA's en type certificaten die ook daadwerkelijk gebruikt (mogen) worden voor dat desbetreffende domeinnaam. Voeg tevens per domeinnaam een CAA-record met een e-mailadres voor melding op misbruik toe. (Bv. CAA-record: iodef abuse@domeinnaam.nl)

PKIoverheid	DK hanteren; ontbreekt in UBV	DK - PKI001	Gebruik OIN in subject serial number veld is verplicht
PKIoverheid	DK hanteren; ontbreekt in UBV	DK - PKI004 (WT005)	De betreffende CRL dient zowel voor de versturende als ontvangende partij te benaderen zijn
TLS-bibliotheek	NCSC hanteren o.b.v. UBV (Volgen van bovenliggende voorschriften)	NCSC - Randvoorwaarden: TLS-bibliotheken	Kies voor een betrouwbare TLS-bibliotheek die past bij jouw toepassing.* Zie TLS-Beveiligingsrichtlijnen Hoofdstuk 4. Randvoorwaarden
Toevalsgetallen	NCSC hanteren o.b.v. UBV (Volgen van bovenliggende voorschriften)	NCSC - Randvoorwaarden: Toevalsgetallen	De meeste besturingssystemen en TLS-bibliotheken bevatten een goede, cryptografisch veilige PRNG. Identificeer welke PRNG er gebruikt wordt in jouw TLS-bibliotheek en onderzoek of deze hoge kwaliteits-toevalsgetallen genereert (d.w.z. onvoorspelbare toevalsgetallen). Consulteer hiervoor de (leverancier van) de TLS-bibliotheek die je gebruikt voor jouw toepassing. Van de volgende RNG is bekend dat hij onveilig is: Dual EC DRBG Zie TLS-Beveiligingsrichtlijnen Hoofdstuk 4. Randvoorwaarden