UNIFORME BEVEILIGINGSVOORSCHRIFTEN

Datum	23-3-2020
Versie	0.2 Concept
Auteur	Edustandaard werkgroep Uniforme Beveiligingsvoorschriften

INHOUDSOPGAVE

Historie

Versie	Auteur	Toelichting	Datum
0.1	Jordy van den Elshout	Eerste concept o.b.v. GAP-analyse en input tijdens de eerste werkgroepbijeenkomst.	21 januari 2020
0.2	Jordy van den Elshout	Bijgewerkt concept na input van de tweede bijeenkomst. Daarnaast een bijlage toegevoegd voor profielen, waaronder Edukoppeling.	23 maart 2020

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' in het leven te roepen. Deze werkgroep zorgt voor een set uniforme beveiligingsvoorschriften die centraal kunnen worden onderhouden. Verschillende standaarden, zoals OSO, BRON, UWLR en ECK DT, kunnen hier dan naar verwijzen in plaats van dat zij deze zelfstandig definiëren.

1.2 Doel

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

1.3 Doelgroep

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

1.4 Samenhang met andere initiatieven

De transactiestandaard Edukoppeling en andere (gelieerde) standaarden, zoals OSO, BRON, UWLR en ECK DT, moeten hier naar kunnen verwijzen in plaats van zelfstandig definiëren.

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 wezen kan worden.

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, indien nodig nationale afspraken en alleen als die niet voldoen aanvullende afspraken die in deze werkgroep worden gemaakt. Afwijken van bovenliggende afspraken wordt onderbouwd.

2.1.1 TLS-voorschriften NCSC

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

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

2.2 Onderscheid tussen M2M en H2M

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

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

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

2.3 Onderscheid tussen veilige en legacy-configuratie

In legacy-situaties zijn nieuwe beveiligingsopties in veel gevallen niet beschikbaar. Op dat moment moet de meest veilige configuratie gekozen worden, mits deze voldoen aan de voorschriften in dit document. Ondanks dat de configuratie voldoet aan de voorschriften, moet dit 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 een veilige en legacy-configuratie niet vanuit dezelfde bron (FQDN, serverconfiguratie, virtual host) moet komen.

TLS-ALG-03
Gegevensuitwisseling voor legacy-situaties dient op een separaat domein (FQDN) te worden afgehandeld.

3 Machine-to-Machine (M2M)

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

3.1 Volgen van bovenliggende voorschriften

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 Voorschriften

Onderstaande voorschriften zijn specifiek en leidend boven de bovenliggende afspraken.

3.2.1 Versie

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

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

3.2.2 Algoritmeselecties

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

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

TLS-M2M-02 (Interoperabiliteit en veiligheid)
Een Serviceaanbieder is verplicht om alle onderstaande cipher suites <u>in aangegeven volgorde</u> te ondersteunen. *TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384* *TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256* *TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384*

TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256
TLS_DHE_RSA_WITH_AES_128_GCM_SHA256

De cipher TLS_DHE mag alleen onder voorwaarde gebruikt worden:

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

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

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

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

3.2.3 OCSP-Stapling (certificaatcontrole)

Deze functionaliteit zorgt ervoor dat de OCSP-informatie (voor het controleren van de geldigheid van een certificaat) door de server zelf wordt verstrekt. De server heeft hier echter wel een verbinding nodig met de certificaatleverancier, wat een security-risico vormt. De server moet een uitgaande verbinding kunnen maken, wat niet wenselijk is.

TLS-M2M-XX (Veiligheid)

** Hier staat een uitzoek actie voor open. Wanneer deze is uitgevoerd, kan hier een afspraak overleg vastgesteld worden. Wel is de werkgroep ermee eens dat certificaat controle uitgevoerd moet worden. **

3.3 Overige

3.3.1 HTTPS

HTTPS is door het IANA gestandaardiseerd op port 443, waar bij elke keten dan ook gebruik van wordt gemaakt. Hiervan mag om compatibiliteitsredenen niet van afgeweken worden.

TLS-M2M-04 (Interoperabiliteit)

Er moet gebruikgemaakt worden van TCP poortnummer 443 ** Hier staat een actie voor open. Wanneer deze is uitgevoerd, kan de afspraak definitief gemaakt worden. **

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 al payload bevat waar datalekken risicovol kunnen zijn.

TLS-M2M-05 (Veiligheid)

Er **mag geen** gebruik gemaakt worden van redirects die vanaf HTTP redirecten naar HTTPS

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

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

3.3.2 SNI

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

TLS-M2M-07 (Interoperabiliteit)
ServerNameIndication (SNI) **moet** door elk systeem dat acteert als client geïmplementeerd zijn ** wacht op reactie leden van de werkgroep, na informeren achterban over impact **

3.4 PKIoverheid certificaat

Bij een PKIoverheid certificaat is er bij de CSP 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 CSP's is dit niet geregeld en kent men ook het OIN waarschijnlijk niet en kunnen andere key usages (combi's) toegepast worden.

TLS-M2M-08 (Betrouwbaarheid)
Indien een OIN verplicht en de integriteit daarvan noodzakelijk (niveau 3) is, dient de authenticatie met een certificaat van PKIoverheid plaats te vinden.

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

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 uitfasering (met de sector) gemaakt zijn.
- 'Voldoende' **mag** gebruikt worden,
- 'Goed' heeft de **voorkeur**

4.2 Nadere invulling

4.2.1 Versie

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

4.2.2 Algoritmeselecties

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

Cipher suites met classificatie 'Voldoende' **mag** gebruikt worden, echter heeft 'Goed' de **voorkeur.**

4.2.3 OCSP-Stapling

Deze functionaliteit zorgt ervoor dat de OCSP-informatie (voor het controleren van de geldigheid van een certificaat) door de server zelf wordt verstrekt. Hierdoor hoeft de cliënt geen verzoek te doen bij de certificaatleverancier, wat een privacy-risico kan zijn. De certificaatleverancier ontvangt hiermee surfgedrag. Keerzijde is dat de server deze verbinding moet opzetten met de certificaatleverancier, wat een security-risico vormt. De server moet een uitgaande verbinding kunnen maken, wat niet wenselijk is.

TLS-H2M-01
** keuze maken evt. o.b.v. BIV-classificatie, of afspraak maken dat een ketenpartij deze afweging expliciet moet afwegen. **

4.3 Overige

4.3.1 HTTPS

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

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

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

Een PKIoverheid valt officieel niet onder EV, echter vindt hier wel op eenzelfde niveau de validatie plaats. Bij PKIoverheid wordt ook gecontroleerd of de aanvrager een bevoegd persoon is. Daarnaast kent PKIoverheid ook een EV variant, echter is deze niet geschikt voor M2M-communicatie waarbij een OIN verplicht is.

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

TLS-PKI-01 (Betrouwbaarheid)
Het certificaat moet ondertekend zijn door een CA en de cliënt moet deze kunnen controleren op geldigheid.

De validatie van een DV verloopt via een DNS-record of website. Wanneer gekozen wordt voor een DV is de betrouwbaarheid afhankelijk van de toegangsbeveiliging tot het domein-, dns- en websitebeheer. 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.

BIJLAGE: 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.

Edukoppeling

Categorie	Onderwerp	Status	Referentie	#	Edukoppeling (O.b.v. UBV)
0. TLS Versie	Versie	UBV hanteren; overgenomen van DK	UBV	TLS-M2M-01	Een Serviceaanbieder is verplicht TLS versie 1.2 te ondersteunen, daarnaast is het aanbevolen voor een Serviceaanbieder om TLS versie 1.3 te ondersteunen. Als een Serviceaanbieder TLS versie 1.3 aanbiedt dan is het aanbevolen voor Serviceafnemers om TLS 1.3 te gebruiken TLS 1.0 en TLS 1.1 zijn niet meer toegestaan
1. TLS	Cipher Suites	UBV hanteren; specifieker dan DK	UBV	TLS-M2M-02	Een Serviceaanbieder is verplicht om alle onderstaande cipher suites 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 Een Serviceafnemer mag een selectie hiervan gebruiken uit oogpunt van efficiëntie. Daarbij wordt aanbevolen om de meest veilige te kiezen (de hoogste in de lijst).
1. TLS	Poortnummer	UBV hanteren; overgenomen van DK; tegenstrijdig met EK	UBV	TLS-M2M-04	Er moet gebruikgemaakt worden van TCP poortnummer 443
1. TLS	Onderscheid tussen M2M en H2M	UBV hanteren; ontbreekt in DK	UBV	TLS-ALG-02	Gegevensuitwisseling voor M2M en H2M dient op separate domeinen (FQDN) te worden afgehandeld
1. TLS	Onderscheid tussen veilige en legacy-configuratie	UBV hanteren; ontbreekt in DK	UBV	TLS-ALG-03	Gegevensuitwisseling voor legacy-situaties dient op een separaat domein (FQDN) te worden afgehandeld.
1. TLS	TLS-richtlijn NCSC	UBV hanteren; in lijn met DK	UBV	TLS-ALG-01	Het is verplicht te voldoen aan de ‘ICT-beveiligingsrichtlijnen voor Transport Layer Security (TLS)’ van NCSC.

1. TLS	Hashfuncties voor bulkversleutel ing en het genereren van random numbers	NCSC hanteren o.b.v. UBV	NCSC	Hashfuncties voor bulkversleutelin g en het genereren van random numbers	Voorkeur: HMAC-SHA-256, -384 en -512 Mag: HMAC-SHA-1
1. TLS	Hashfuncties voor sleuteluitwiss eling	NCSC hanteren o.b.v. UBV	NCSC	Hashfuncties voor sleuteluitwisseli ng	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	NCSC	Lengte van RSA-sleutels	Voorkeur: minimaal 3072 bit Mag: 2048 - 3071 bit
1. TLS	Ondersteund e elliptische krommen	NCSC hanteren o.b.v. UBV	NCSC	Ondersteunde elliptische krommen	Voorkeur: secp384r1, secp256r1, x448, x25519 Mag: secp224r1
1. TLS	Authenticatie	DK hanteren; ontbreekt in UBV	DK	TLS001	Authenticatie is verplicht met TLS en PKIoverheid certificaten
1. TLS	Tweezijdige TLS	DK hanteren; ontbreekt in UBV	DK	TLS002	Tweezijdig TLS is verplicht
1. TLS	Terugvallen op eerdere versies	DK hanteren; in lijn met UBV	DK	TLS003	De TLS implementatie mag niet op SSL v3 en eerdere versies terugvallen
1.1 TLS Opties	Redirect	UBV hanteren; ontbreekt in DK	UBV	TLS-M2M-05	Er mag geen gebruik gemaakt worden van redirects die vanaf HTTP redirecten naar HTTPS
1.1 TLS Opties	SNI	UBV hanteren; ontbreekt in DK	UBV	TLS-M2M-07	ServerNameIndication (SNI) moet door elk systeem dat acteert als client geïmplementeerd zijn
1.1 TLS Opties	0-RTT	NCSC hanteren o.b.v. UBV	NCSC	0-RTT	Uit
1.1 TLS Opties	Client-initiate d renegotiation	NCSC hanteren o.b.v. UBV	NCSC	Client-initiated renegotiation	Uit
1.1 TLS Opties	Compressie	NCSC hanteren o.b.v. UBV	NCSC	Compressie	Voorkeur: Geen compressie Mag: Compressie op applicatieniveau
1.1 TLS Opties	Insecure renegotiation	NCSC hanteren o.b.v. UBV	NCSC	Insecure renegotiation	Uit
1.1 TLS Opties	OCSP stapling	NCSC hanteren o.b.v. UBV	NCSC	OCSP stapling	Voorkeur: Aan Mag: Uit

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	PKI002	PKIoverheid certificaat moet geldig zijn (het mag niet zijn verlopen of ingetrokken)
PKI	PKIoverheid	DK hanteren; ontbreekt in UBV	DK	PKI003	De geldigheid van het certificaat wordt getoetst met betrekking tot de geldigheidsdatum en de Certificate Revocation List(CRL) die voldoet aan de eisen van PKI-overheid.
PKI	PKIoverheid	DK hanteren; ontbreekt in UBV	DK	PKI004	De betreffende CRL dient zowel voor de versturende als ontvangende partij te benaderen zijn
PKI	PKIoverheid	DK hanteren; ontbreekt in UBV	DK	PKI005 (Concept)	Het certificaat moet zijn van het type PKIoverheid public root (PKI Staat der Nederlanden Root) of PKIoverheid private root (PKI Staat der Nederlanden Private Root)
PKI	OIN	DK hanteren; in lijn met UBV	DK	Paragraaf 3.1	Verplicht: PKIoverheid certificaten & CRL Profile
PKI	CN	UBV hanteren; ontbreekt in DK	UBV	TLS-M2M-06	Maak alleen gebruik van volledige en traceerbare domeinnamen, Fully Qualified Domain Names (FQDN)
PKI	Certificaat	NCSC hanteren o.b.v. UBV	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.