

# Aanmeldformulier

---

Voor : Bureau Edustandaard  
Van : Jordy van den Elshout, namens de Werkgroep UBV  
Datum : 12-1-2021  
Betreft : Verzoek in beheername Uniforme Beveiligingsvoorschriften - TLS v1.0

---

## Toelichting op de toepassing van dit aanvraagformulier

### *Doel*

Op basis van de antwoorden op de vragen in dit aanvraagformulier stelt bureau Edustandaard een advies op. Bij twijfel over de relevantie, het werkingsgebied of kwaliteit kan bureau Edustandaard besluiten een gesprek te voeren met de indiener. Het advies zal aan de indiener aangeboden worden voor een respons en vervolgens aan de Architectuurraad en de Standaardisatieraad worden voorgelegd.

Dit aanvraagformulier kent een *standaard formaat*, zodat de ketenpartijen die aan afspraak in beheer willen brengen, bekend zijn met de vragen en ook de rationale erachter begrijpen. En zodat Architectuurraad, Standaardisatieraad en alle belanghebbende ketenpartijen zich snel en effectief kunnen informeren over hetgeen van belang is met betrekking tot deze nieuwe afspraak. Een belangrijke leidraad voor het advies van Bureau Edustandaard is het document 'Afspraken en handreikingen ten behoeve van ontwikkeling, beheer en implementatie van afspraken in beheer bij Edustandaard', te vinden op [de website van Edustandaard](#).

### *Doelgroepen:*

- **Bureau Edustandaard** beoordeelt op basis van deze vragenlijst in hoeverre aan de criteria is voldaan. Het bureau adviseert hierin de indiener en Standaardisatieraad,
- Andere **standaardisatiewerkgroepen bij Edustandaard** die nu of in de toekomst met deze afspraak te maken zullen krijgen,
- De **Architectuurraad** bewaakt en beoordeelt de samenhang met de andere afspraken (architectuur) die in beheer of geregistreerd zijn bij Edustandaard en brengt hierover advies uit voor de Standaardisatieraad,
- De **Standaardisatieraad** zal op basis van de vragenlijst en de adviezen besluiten om de afspraak al dan niet in beheer te nemen of te laten registreren bij Edustandaard,
- alle **ketenpartijen** die direct of indirect met deze nieuwe afspraak te maken gaan krijgen (informatiepositie, ketentransparantie).

### *Beheer of registratie*

Dit aanvraagformulier wordt in principe gebruikt voor het in beheer laten nemen van een afspraak<sup>1</sup> bij Edustandaard. Alle ketenpartijen verenigd bij Edustandaard hebben zich er ook aan geconformeerd om afspraken tussen partijen die betrekking hebben op uitwisselingen in de ketens, formeel in beheer te brengen bij Edustandaard. Er bestaat ook de mogelijkheid tot registratie van een afspraak, dat is in het algemeen van toepassing op afspraken waar de exacte governance nog moet worden vastgesteld. Vaak is de intentie er wel om het beheer in een later stadium formeel bij Edustandaard onder te brengen.

**Let op: Bij het beantwoorden van de vragen graag verwijzingen naar de documentatie opnemen. De antwoorden moeten terug te vinden zijn in de bijbehorende documentatie.**

---

<sup>1</sup> Waar afspraak staat kan ook (informatie)model, begrippenset of architectuur gelezen worden.

## De vragen

### 1. Om welke afspraak gaat het?

#### 1.1. Wat is de naam en laatste wijzigingsdatum?

Naam	datum
Uniforme Beveiligingsvoorschriften - TLS v1.0	18-12-2020

#### 1.2. Geef een overzicht van de bijbehorende documentatie, online en offline.

titel en/of URL	auteur(s)	versienummer	Status
<a href="#">UBV - TLS v0.5</a>	Jordy van den Elshout	v0.5	Concept
<a href="#">UBV - TLS v0.7</a>	Jordy van den Elshout	v0.7	Concept
<a href="#">UBV - TLS v1.0</a> (online op edustandaard.nl vanaf 2de week februari)	Jordy van den Elshout	v1.0	Definitief

### 2. Beschrijf de afspraak:

#### 2.1. Waar gaat de afspraak over?

Antwoord	Verwijzing
<i>“...set uniforme beveiligingsvoorschriften die centraal kunnen worden onderhouden. Verschillende standaarden, zoals <a href="#">Edukoppeling</a>, <a href="#">Uitwisseling Leerlinggegevens en Resultaten (UWLR)</a> en <a href="#">Educatieve Distributie en Toegang (ECK DT)</a>, 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.”</i>	UBV TLS v1.0, Paragraaf 1.1

#### 2.2. Wat is de aanleiding geweest? (Bijv. wettelijke kaders, een projectdoelstelling of vanuit een bedrijfs- of ketenmissie.)

Antwoord	Verwijzing
<i>“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.”</i>	UBV TLS v1.0, Paragraaf 1.1  <b>Voor meer informatie, zie:</b> <a href="#">20190528 Memo - Uitnodiging werkgroep 'Uniforme Beveiligingsvoorschriften'</a>

#### 2.3. Wat is het doel?

Antwoord	Verwijzing
<i>“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 de interoperabiliteit van de gegevensuitwisseling en anderzijds in de efficiëntie van implementatie en beheer.”</i> <i>“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.”</i>	UBV TLS v1.0, Paragraaf 1.2 en 1.4.

#### 2.3.1. Wat gaat er fout als de afspraak niet geaccepteerd wordt door het veld?

Antwoord	Verwijzing
	Staat niet expliciet beschreven. Kan afgeleid

<p>Wanneer de afspraken niet worden gevolgd worden, heeft dat impact op drie onderdelen:</p> <ol style="list-style-type: none"> <li>Betrouwbaarheid en Veiligheid: risico vormen voor de beschikbaarheid, integriteit of vertrouwelijkheid van (persoons)gegevens die worden uitgewisseld. Wat kan leiden tot een beveiligingsincident en in geval van persoonsgegevens, een datalek.</li> <li>Interoperabiliteit: (nieuwe) uitwisselingen kunnen niet plaatsvinden als de partijen verschillende instellingen hanteren. Zoals voor SNI.</li> <li>Efficiëntie: onnodig veel configuratiemogelijkheden in stand houden voor de interoperabiliteit.</li> </ol>	worden van het Doel, paragraaf 1.2 van UBV TLS v0.9
--	---

### 2.3.2. Hoe urgent is de afspraak?

Antwoord	Verwijzing
Belangrijk, maar niet urgent. Beveiligingsstandaarden zijn nu in afzonderlijke afspraken vastgelegd.	

### 2.3.3. Biedt de afspraak een volledige oplossing voor het beoogde doel en de beoogde doelgroep?

Antwoord	Verwijzing
Het doel is dat andere standaarden hierna kunnen verwijzen en is daarmee volledig. Bij implementatie kunnen ontbrekende items opgepakt worden.	

### 2.4. Wat is het werkingsgebied? (Bijv. onderwijssectoren, organisaties.)

Antwoord	Verwijzing
<p><i>“Deze voorschriften zijn bedoeld voor organisaties die ict-toepassingen leveren en/of beheren voor gegevensuitwisseling in het onderwijs. Dat geldt (lees: toepasselijk) voor de hele onderwijssector (PO, VO, MBO, HO en WO).”</i></p> <p><i>“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).”</i></p> <p><i>“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).”</i></p>	UBV TLS v1.0, Paragraaf 1.1 en 1.3.

### 2.5. Wat is het toepassingsgebied? (Bijv. administratieve domein, onderzoek, leermiddelendomein.)

Antwoord	Verwijzing
<p>Voorschriften in zijn algemeen voor alle toepassingsgebieden, als deze passen in de soort gegevensuitwisseling. Er wordt onderscheid gemaakt tussen machine to machine (M2M) en human to machine (H2M)</p> <p><i>“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).”</i></p> <p><i>“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.”</i></p>	UBV TLS v1.0, Paragraaf 1.1 en hoofdstuk 3 (M2M) en hoofdstuk 4 (H2M).

## 2.6.

Op welke (keten)processen heeft de afspraak betrekking? (Bijv. in- en uitschrijfprocessen tussen instellingen.)

Antwoord	verwijzing
Zie antwoord bij vraag 2.5.	

## 2.7. Wie is de doelgroep? (Bijv. DUO, onderwijsinstellingen, LAS-systemen, uitgevers.)

Antwoord	Verwijzing
<i>"Deze voorschriften zijn bedoeld voor organisaties die ict-toepassingen leveren en/of beheren voor gegevensuitwisselingen in het onderwijs. Dat geldt voor de hele onderwijssector (PO, VO, MBO, HO en WO)."</i>	UBV TLS v1.0, paragraaf 1.3

### 2.7.1. Bestaat de afspraak uit verschillende delen die zich op verschillende doelgroepen richten en zo ja, welke?

Antwoord	Verwijzing
Ja, zie antwoord bij vraag 2.5.	

## 2.8. Wat is de samenhang van deze afspraak met andere afspraken en standaarden?

### 2.8.1. Is de afspraak gebaseerd op (afgeleid van of gerelateerd aan) (inter)nationale standaarden en zo ja, welke?

naam standaard + wat is de samenhang	versie	Datum	verwijzing
Edukoppeling moet verwijzen naar UBV			Link
UWLR moet verwijzen naar UBV			Link
ECK DT moet verwijzen naar UBV			Link
UBV maakt gebruik van het 'Cert. schema IBP ROSA' voor de BIV-classificatie. Daarnaast moet het Cert. schema ook verwijzen naar UBV, zodat de invulling daarmee concreet wordt aangewezen.	maart 2018	maart 2018	Link
Afspraken OSO			

## 3. Is de afspraak breed geaccepteerd door de doelgroep?

### 3.1. Welke partijen en welke personen waren betrokken bij de ontwikkeling?

antwoord	verwijzing
<p>Werkgroep</p> <ul style="list-style-type: none"> <li>- Kennisnet</li> <li>- DUO</li> <li>- The Learning Network</li> <li>- Surfnets</li> <li>- Thieme Meulenhof</li> <li>- Topicus</li> </ul> <p>Geïnformeerd:</p> <ul style="list-style-type: none"> <li>- VDOD</li> </ul> <p>Afstemming met</p> <ul style="list-style-type: none"> <li>- Edukoppeling</li> </ul>	Zie voor de partijen

### 3.2. Wie zijn op welke manieren ingelicht over de afspraak? (Bijv. bijeenkomsten, seminars, FAQ's op websites, fora, papers.)

antwoord	verwijzing
Genoemde partijen zijn onderdeel van de werkgroep en hebben hun achterban gevraagd te reageren op openbare consultatie. Daarnaast is VDOD	

geïnfomeerd. Ook heeft afstemming plaatsgevonden met Edukoppeling en OSO.	
---	--

- 3.3.** Zijn er openbare verslagen en/of besluitenlijsten van bijeenkomsten die aantonen dat de afspraak breed is geaccepteerd en zo ja, welke? Verwijs eventueel naar personen waar de betreffende schriftelijke vastleggingen kunnen worden opgevraagd

<b>antwoord</b>	<b>verwijzing</b>
Alle afspraken en voorschriften zijn expliciet nagelopen tijdens de bijeenkomsten met de werkgroepen.	Zie verslag van de bijeenkomsten UBV op Edustandaard.

- 3.4.** Zijn er toepassingsvoorbeelden waarin de afspraak al is gebruikt en zo ja, welke?

<b>antwoord</b>	<b>Verwijzing</b>
Kennisnet heeft voor haar diensten de meeste voorschriften toegepast op diensten, zoals OSO en websites van Kennisnet. Kijkend naar Edukoppeling dan zijn veel voorschriften gelijk.	Niet aanwezig. Website van Kennisnet kan gecontroleerd worden met de test op internet.nl

- 4.** Hoe ziet de implementatie of toepassing van de afspraak eruit?

- 4.1.** Is er een implementatiehandleiding en/of andere implementatieondersteuning beschikbaar en zo ja, welke?

<b>antwoord</b>	<b>Verwijzing</b>
De wijze van implementatie is per gebruikte software verschillend. Daarentegen zijn veel voorschriften in te stellen door middel van configuraties. In enkele gevallen kan het schrijven van code nodig zijn.  De intentie is wel om best-practices te verzamelen, echter zijn we daarvan afhankelijk van partijen die dit aanleveren. Verzoek hiervoor staat wel uit naar de werkgroepleden, die dit bij hun achterban kunnen opvragen.	<a href="#">Verslag UBV Bijeenkomst November 2019</a>

- 4.2.** Is er een tool beschikbaar om implementatie van (delen van) de afspraak op correct gebruik te toetsen zo ja, welke? Zo nee, voor welke delen zou dit wel denkbaar zijn?

<b>antwoord</b>	<b>verwijzing</b>
Ja, deze zijn ook (als voetnoot) opgenomen in voorschriften. Deels geeft deze direct weer dat er onjuiste configuraties worden gebruikt. Overige punten dienen zelf gecontroleerd te worden o.b.v. de voorschriften.  <i>"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."</i>	UBV TLS v1.0, voetnoot 1 en 2

- 4.3.** Wat is de globale inschatting voor wat de kosten, benodigde tijdsinvestering en/of expertise voor de betrokken partijen zijn voor de implementatie?

<b>antwoord</b>	<b>verwijzing</b>
In geval van nieuwe configuraties, zou dit nauwelijks impact moeten hebben. Ervan uitgaande dat partijen geen TLS-configuraties op default laten staan en direct de juiste instellingen meenemen in het project.  Wanneer een bestaande configuratie aangepast dient te worden, neemt dit werkzaamheden met zich mee. De hoeveelheid is afhankelijk van de situatie, zoals de gebruikte software, omvang en afhankelijkheden.	n.v.t.

5. Hoe zijn het beheer en de doorontwikkeling geregeld?

- 5.1. Onder welke samenstelling gaat het beheer vallen? (Bijv. onder een bestaande werkgroep of een nieuw op te richten werkgroep of is er de wens om het beheer bij een werkgroep van Edustandaard te beleggen.)

<b>Antwoord</b>	<b>verwijzing</b>
"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."	UBV TLS v1.0, paragraaf 1.6

- 5.2. Bij wie kan men terecht voor vragen over beheer, toepassing, doorontwikkeling van de afspraak? (bijv. via [info@edustandaard.nl](mailto:info@edustandaard.nl))

<b>Antwoord</b>	<b>Verwijzing</b>
Mail naar <a href="mailto:info@edustandaard.nl">info@edustandaard.nl</a> , met "Uniforme beveiligingsvoorschriften" in het onderwerp	

- 5.3. Wat is de globale inschatting van wat de kosten, benodigde tijdsinvestering en/of expertise voor de betrokken partijen zijn voor het beheer en doorontwikkeling van de afspraak?

<b>Antwoord</b>	<b>Verwijzing</b>
Dit levert een besparing op. Waar de werkgroepen van standaarden eerst zelf kosten, tijd of expertise moesten inzetten, wordt dit nu centraal gedaan. Benodigde middelen zitten met name op het vlak van tijd en expertise, welke door de werkgroep UBV worden geleverd.	

6. Hoe ziet de geschiedenis en toekomst van de afspraak eruit?

- 6.1. Wat is de **roadmap** m.b.t. de doorontwikkeling van de afspraak? (bijvoorbeeld kunnen andere toepassingsgebieden en sectoren worden voorzien)

<b>antwoord</b>	<b>verwijzing</b>																					
<p>Naast voorschriften voor TLS, zijn er ook andere uniforme beveiligingsvoorschriften. Onder andere die van Forum Standardisatie, die ook opgenomen zijn de Wet Digitale Overheid. Op de planning staat:</p> <table border="1"> <thead> <tr> <th>Standaard</th> <th>Doel standaard</th> <th>Thema (status)</th> </tr> </thead> <tbody> <tr> <td>TLS/HTTPS Het NCSC heeft aanvullende eisen t.a.v. cijfersuites</td> <td>Beveiligde verbinding</td> <td>TLS (Klaar voor goedkeuring)</td> </tr> <tr> <td>DNSSEC</td> <td>Domeinnaambeveiliging</td> <td>Domeinnaambeveiliging (Bezig)</td> </tr> <tr> <td>SPF</td> <td>Anti-phishing email</td> <td>Veilig en betrouwbare e-mail (Bezig)</td> </tr> <tr> <td>DKIM</td> <td>Anti-phishing email</td> <td>Veilig en betrouwbare e-mailverkeer (Bezig)</td> </tr> <tr> <td>DMARC</td> <td>Anti-phishing email</td> <td>Veilig en betrouwbare e-mailverkeer (Bezig)</td> </tr> <tr> <td>HTTPS, HSTS en TLS conform NCSC richtlijn</td> <td>Beveiligde verbinding</td> <td>TLS (Klaar voor goedkeuring)</td> </tr> </tbody> </table>	Standaard	Doel standaard	Thema (status)	TLS/HTTPS Het NCSC heeft aanvullende eisen t.a.v. cijfersuites	Beveiligde verbinding	TLS (Klaar voor goedkeuring)	DNSSEC	Domeinnaambeveiliging	Domeinnaambeveiliging (Bezig)	SPF	Anti-phishing email	Veilig en betrouwbare e-mail (Bezig)	DKIM	Anti-phishing email	Veilig en betrouwbare e-mailverkeer (Bezig)	DMARC	Anti-phishing email	Veilig en betrouwbare e-mailverkeer (Bezig)	HTTPS, HSTS en TLS conform NCSC richtlijn	Beveiligde verbinding	TLS (Klaar voor goedkeuring)	Standaard Agenda UBV
Standaard	Doel standaard	Thema (status)																				
TLS/HTTPS Het NCSC heeft aanvullende eisen t.a.v. cijfersuites	Beveiligde verbinding	TLS (Klaar voor goedkeuring)																				
DNSSEC	Domeinnaambeveiliging	Domeinnaambeveiliging (Bezig)																				
SPF	Anti-phishing email	Veilig en betrouwbare e-mail (Bezig)																				
DKIM	Anti-phishing email	Veilig en betrouwbare e-mailverkeer (Bezig)																				
DMARC	Anti-phishing email	Veilig en betrouwbare e-mailverkeer (Bezig)																				
HTTPS, HSTS en TLS conform NCSC richtlijn	Beveiligde verbinding	TLS (Klaar voor goedkeuring)																				

STARTTLS en DANE. Voor gebruik van DANE gelden strikte policies	Encryptie van mailverkeer	Veilig en betrouwbare e-mailverkeer (Bezig)	
SPF en DMARC	Strikte policies voor emailstandaarden	Veilig en betrouwbare e-mailverkeer (Bezig)	
Security headers*		Security headers (Bezig)	
* Geen onderdeel van de WDO, maar op inzicht van de werkgroep toegevoegd.			

**6.2.** Wat is de roadmap m.b.t. de **implementatie** van de afspraak?

Antwoord	verwijzing
Implementatie bevat het opnemen van de afspraken in de standaard. Hierbij is gestart met Edukoppeling. Vervolgens de volgende standaarden.	

**7.** Welke copyrights en andere voorwaarden zijn van toepassing op de afspraak?

**7.1.** Kan het intellectuele eigendom - m.b.t. mogelijk aanwezige patenten - van de afspraak onherroepelijk op een royalty-free basis aan Edustandaard ter beschikking worden gesteld?

Antwoord	verwijzing
In de meeste gevallen wel, echter zijn sommige afspraken overgenomen van Digikoppeling en NCSC. In deze documenten zijn echter geen rechten aangegeven.	

**7.2.** Is het voor een ieder mogelijk om de afspraak (inclusief alle bijbehorende documentatie) te kopiëren, beschikbaar te stellen en te (her)gebruiken om niet?

Antwoord	verwijzing
<i>"De licentie op de voorschriften is CC BY 4.0 (Attribution 4.0 International). Dit betekent in eenvoudige termen dat je vrij bent om het werk te delen en te bewerken, mits je bronvermelding toepast. Let wel op dat de voorschriften specifiek is ontworpen voor de onderwijssector."</i>	Webpagina UBV TLS