edustandaard

Concept Verslag werkgroep Uniforme Beveiligingsvoorschriften (augustus 2020)

Maandag 31 augustus 2020, 13:00 – 14:30. Locatie: online.

Aanwezig: Arnold Greving (DUO), Dirk Linden (Kennisnet, voorzitter), Jaap Mooij (Kennisnet), Joost van Dijk (Surfnet), Jordy van den Elshout (Kennisnet, verslag), Marten Bakker (The Learning Network), Rimmer Hylkema (ThiemeMeulenhoff) en Robert Klein (Kennisnet)

Afwezig: Olav Loite

1. Opening

a. Verslag voorgaande bijeenkomst(en)

Toelichting: Het concept verslag van de voorgaande bijeenkomst is eerder toegestuurd en zonder aanvulling als concept op Edustandaard geplaatst.

De voorzitter vraagt of iemand op- of aanmerkingen heeft op het verslag. Die zijn er niet. Het verslag mei 2020 wordt daarmee vastgesteld.

b. Actielijst

Toelichting: op één actie na, zijn alle acties opgepakt en afgehandeld. De laatste actie die open staat betreft het verzamelen van best practices. Dit is één van de eerste punten, waarvan de voortgang eerder expliciet te sprake is geweest. Toen is besloten om hier document voor te starten met structuur, waarin de best practices door iedereen toegevoegd kan worden. Dit is onder de aandacht gebracht, echter zijn er nog geen best practices toegevoegd.
Doel: informeren over de status en waar nodig zorgen voor voortgang.

Afspraak

Afgesproken wordt om deze laatste actie af te sluiten. Wanneer naar best practices gevraagd wordt, zullen we dit behandelen in de werkgroep. Wanneer iemand uit de werkgroep een best practices voorhanden heeft, kan deze in het reeds aanwezige document geplaatst worden en besproken worden in de werkgroep. Arnold draagt daarbij het idee aan om dit via GitHub aan te bieden. Dat wordt als goed idee gezien en kan opgepakt worden als een best practices zich voordoet.

2. Uniforme Beveiligingsvoorschriften

a. Uitkomst ROSA-scan en bespreking Architectuurraad 2 juli 2020

Toelichting: de versie UBV TLS v0.5 is onderworpen aan de ROSA-scan (zie ROSA Architectuurscan UBV v2), waarbij o.a. geadviseerd wordt om te beschrijven waarom bepaalde standaarden bij naam worden genoemd. Daarnaast om een basis-profiel op te nemen. De ROSA-scan en de laatste versie van UBV is tevens besproken in de Architectuurraad (zie punt 5. in Verslag Architectuurraad 2-7-2020). De architectuur heeft het advies uit de ROSA-scan overgenomen met een aantal aandachtspunten, zoals voor de verplichting van poort 443: "het is poort 443, tenzij bij bilaterale uitwisselingen anders wordt afgesproken". Verder is besloten dat een "brede consultatie noodzakelijk is" en "proces tot definitief advies in de

Architectuurraad van oktober, en vaststellen in de Standaardisatieraad van november lijkt goed haalbaar".
Doel: informeren; geeft ook de verklaring voor de wijzigingen in de nieuwe versie van UBV TLS.

Naast de toelichting zijn er geen opmerkingen of vragen.

b. Certificaat controle

Toelichting: tijdens de vorige bijeenkomst is besloten om het deel omtrent certificaat controle apart op te pakken. Eerst bepalen we 'wat' en vervolgens 'hoe' dit moet gebeuren. Dat wordt vervolgens verwerkt in de laatste versie van UBV TLS.
Doel: de voorschriften voor certificaatcontrole behandelen, zodat deze in een nieuwe versie van UBV TLS meegenomen kunnen worden.

Het document is integraal doorgenomen met de werkgroep. Over het 'wat' is de werkgroep het eens:

Certificaat controle dient altijd plaats te vinden. Een certificaat dat is ingetrokken, of waarvan niet kan worden gecontroleerd of het is ingetrokken, mag niet worden gebruikt. Dat geldt ook voor een verlopen certificaat.

Wat betreft de wijze van certificaatcontrole zoals OCSP moeten niet verplicht maar als voorkeur voorgeschreven worden. Het zijn met name maatregelen die bijdragen in onafhankelijkheid van de CSP en dus beschikbaarheid voor het kunnen controleren van het certificaat.
Het kan voorkomen dat dit standaard niet ondersteunt wordt in applicaties. Daarnaast kan CRL volstaan in een gecontroleerde keten, zoals met PKIoverheid certificaten.

Afspraak
De voorschriften voor certificaat controle worden toegevoegd aan de nieuwe versie UBV TLS (v0.7), welke ook als consultatie wordt aangeboden. Verplichtend wat betreft de 'Wat' en bij voorkeur wat betreft de 'Hoe', zoals OCSP-stapling.

Aanvullende voorschriften voor certificaat controle in een H2M situatie zijn er niet, anders dan reeds opgenomen. Zoals de voorschrift voor het toepassen van HSTS.

c. Laatste wijzigingen

Toelichting: naar aanleiding van bovenstaande punten, zoals de ROSA-scan en Architectuurraad zijn de laatste wijzigingen aangebracht in de laatste versie van de UBV. Deze versie is voorafgaand toe gestuurd. Tijdens dit agendapunt bespreken we de laatste op- en aanmerkingen.
Doel: eventuele op- en aanmerkingen bespreken, zodat de nieuwe versie vastgesteld kan worden.

De wijzigingen zijn mondeling toegelicht:
(1) De relatie met WDO is beschreven; (2) voorschrift voor poort 443 is aangevuld met "tenzij bij bilaterale uitwisselingen anders wordt afgesproken." waarmee de uitzondering "Als dit een grote impact met zich meebrengt voor bestaande communicatie (voor 1 mei 2020), mag hiervan afgeweken worden en tijdelijk het bestaande poortnummer gebruikt worden." is komen te vervallen; (3) toevoeging van een voetnoot naar Programma van Eisen voor

PKIoverheid; en (4) toevoeging van het basisprofiel voor M2M, een *view* waarin de voorschriften van UBV TLS i.c.m. NCSC uitgeschreven zijn.

Daar zijn verder geen vragen of opmerkingen over, waarmee versie (0.6) is vastgesteld.

e. Vervolg

Toelichting: de UBV TLS wordt voorgelegd aan een breed publiek, die overeenkomt met de doelgroep en scope van de voorschriften. Doel: informeren over het vervolg en officiële vaststelling van de UBV TLS.

De voorschriften zijn verstrekkend en brede consultatie is van belang. Dat blijkt ook uit de ROSA-scan. De voorzitter doet het verzoek aan de werkgroep om dit bij de achterban onder de aandacht te brengen.

Het bericht voor consultatie wordt deze week verstuurd aan alle Edustandaard leden. Ook verschijnt hierover een item in de nieuwsbrief van Edustandaard. Het bericht wordt tevens doorgestuurd naar de werkgroep.

Actie Allen
Consultatie van UBV TLS onder de aandacht brengen bij eigen achterban. Bericht hiervoor wordt naar de werkgroep doorgestuurd.

3. Veilig en betrouwbare e-mail

a. Eerste concept

Toelichting: op basis van een analyse van de standaarden en beschikbare informatie en voorbespreking met Dirk Linden, Rimmer Hylkema en Jordy van den Elshout is een eerste conceptversie uitgewerkt.
Doel: eerste conceptversie bespreken. Op- en aanmerkingen verzamelen voor een volgende versie.

Niet iedereen heeft nog naar deze versie kunnen kijken. Voorgesteld wordt om komende twee weken commentaar aan te leveren in het document. Dat kan vervolgens verwerkt of anders besproken worden, één op één of met de werkgroep.

Actie Allen
Opmerkingen plaatsen in het document ‘UBV Veilig en Betrouwbare e-mail’ ter verbetering of bespreking.

4. Andere beveiligingsstandaarden

a. Security Headers

Toelichting: ‘Security Headers’ is een apart thema, naast de WDO-beveiligingsstandaarden. Zoals besproken in het voorgaande overleg is dit ook belangrijk onderdeel voor de veiligheid van webdiensten. Het is ook onderdeel van de test op internet.nl, echter wordt daar een subset getest. Welke nog meer van belang zijn en op welke wijze deze toegepast moeten worden, is een vraag die open staat. Wellicht dat de werkgroepleden hier de nodige ervaring mee hebben en de werkgroep hierover kan bijpraten.
Doel: bespreken of extra expertise nodig is en wie de werkgroep kan bijpraten op dit thema, om vervolgens het vervolg te bepalen.

Het is met name bedoeld voor H2M. De vraag is of alle headers uitgewerkt moeten worden als voorschrift. Ze lijken nl niet allemaal relevant en aangezien ze aan verandering onderhevig zijn en dat dus veel beheer van de afspraak zou vragen. Wat ze inhouden en bijdragen is wel van belang, om ze in perspectief te plaatsen. Op basis daarvan kunnen sommige verplicht gesteld worden. Expertise inhuren is niet direct nodig. Eerst lezen we onszelf verder in om een volgende bijeenkomst te verdiepen.

Actie Allen
Verdiepen in de toepassing van 'Security Headers', zodat we dit tijdens de volgende bijeenkomst verder kunnen bespreken.

b. Domeinnaambeveiliging

Toelichting: tijdens de vorige bijeenkomst is besloten om dit als apart thema op te pakken. DNSSEC staat hierin centraal en de uitwerking zal beperkt zijn. DNSSEC is een noodzakelijke randvoorwaarden voor de toepassing DANE (gebaseerd op TLS). Daarnaast is een belangrijke randvoorwaarden voor veilige communicatie (UBV TLS). Net als een betrouwbaar certificaat, is een betrouwbare domeinnaam belangrijk. Daarom kan er ook voor gekozen worden om dit onderdeel te laten zijn van UBV TLS.
Doel: besluiten om domeinnaambeveiliging (DNSSEC) onder te brengen in UBV TLS of als apart thema te houden.

Voorzitter stelt voor om dit - net als bij certificaat controle - als apart document te starten. Op basis daarvan bepalen waar dit een plek moet krijgen.

Actie Jordy
Discussiestuk aanmaken voor het thema Domeinnaambeveiliging.

5. Afsluiting

De voorzitter rondt gezien de tijd het overleg af. In afstemming met de werkgroep is een nieuw moment gepland, waarin alle aanwezigen kunnen: maandag 21 september 2020 van 13:00 tot 14:30. Uitnodiging hiervoor is direct verstuurt via Outlook.