Ministerie van Binnenlandse Zaken en Koninkrijksrelaties

Aanbiedingsformulier Overheidsbreed Beleidsoverleg Digitaal Overheid

1. Korte titel	Plaatsing van REST API Design Rules en NL GOV Assurance Profile for OAuth 2.0 op de 'pas toe of leg uit'-lijst. Plaatsing van OAuth 2.0, CAA en EPUB 3.2 op de lijst van aanbevolen standaarden. Ter kennisname: Microsoft ondersteunt DANE.
2. Datum behandeling	OBDO: 9 juli 2020
3. Aard van de behandeling: *(dubbelklikken op vakje en 'ingeschakeld' aanvinken)*	☐ Scrum **X** Hamerstuk ☐ Ter besluitvorming ☐ Ter bespreking ☐ Ter kennisname ☐ Anders: …….
4. Eerder behandeld in:	☐ PL ☐ ICM ☐ MFG ☐ MT- DO i.o. ☒ Anders: Forum Standaardisatie Uitkomst behandeling in bovenstaand gremium: ☐ Overeenstemming *(geen toelichting vereist)*
5. Voorgeschiedenis / context: *6. Samenvatting/toelichting:*	Mutaties lijsten open standaarden: A) REST API Design Rules: deze standaard helpt REST API's (koppelvlakken over internet voor het bevragen van databronnen) op een uniforme en voorspelbare manier te ontsluiten. REST API's van de overheid krijgen door toepassing van deze standaard een eenduidigere structuur, wat wildgroei voorkomt. B) NL GOV Assurance profile for OAuth 2.0: dit is een beveiligingstandaard voor het autoriseren van toegang tot REST API's, die nauw samenhangt met de bovengenoemde REST API Design Rules. NL GOV Assurance profile for OAuth 2.0 is een Nederlands overheidsprofiel op OAuth 2.0. OAuth 2.0: een generieke en gangbare beveiligingstandaard voor het autoriseren van toegang tot API's. C) CAA: een standaard voor extra controle op uitgifte van digitale certificaten. D) EPUB: een digitoegankelijkheidsstandaard voor het publiceren van niet-reviseerbare elektronische documenten in e-book formaat, geoptimaliseerd voor gebruik op -maar niet beperkt tot- draagbare apparaten zoals e-readers, tablets en smartphones. Ter kennisname: E) Microsoft kondigt ondersteuning voor DANE (beveiliging mailverkeer) aan Microsoft heeft aangekondigd per eind 2021 volledige ondersteuning te bieden voor DANE op Office 365 Exchange Online. DANE is een voor de overheid verplichte open standaard die voorkomt dat aanvallers e-mailverkeer onderweg kunnen afluisteren of aanpassen. Strategisch Leveranciersmanagement Rijk (SLM Rijk) heeft samen met Forum Standaardisatie bij Microsoft aangedrongen op ondersteuning van de standaard. Forum Standaardisatie adviseert overheidsorganisaties, die willen overstappen op Office 365 Exchange Online, te wachten totdat Microsoft

	de standaard daadwerkelijk heeft geïmplementeerd óf om een voorziening (mail-gateway) die DANE ondersteunt vóór Office 365 Exchange Online te plaatsen. Overigens zijn er reeds verschillende andere e-mailleveranciers die ondersteuning bieden voor DANE. Uit de laatste meting informatieveiligheidsstandaarden (begin 2020) blijkt dat inmiddels 50% van de overheidsdomeinen beveiligd is met DANE.
7. Beslispunten/discussiepunten	Instemmen met plaatsing van: A) REST API Design Rules op de 'pas toe of leg uit'-lijst. B) NLGOV Assurance profile for OAuth op de 'pas toe of leg uit'-lijst en OAuth 2.0 op de lijst van aanbevolen standaarden. C) CAA op de lijst aanbevolen standaarden. D) EPUB versie 3.2 op lijst aanbevolen standaarden.
8. Contactgegevens	A t/m D: Redouan Ahaloui, senior adviseur standaardisatie Telefoonnummer: 06-15642325 E: Bart Knubben, coördinerend/specialistisch adviseur standaardisatie Telefoonnummer: 06-21162373 Algemene inlichtingen: Ludwig Oberendorff, hoofd BFS Telefoonnummer: 06-52311217

notitie

Standaardisatie
Agendapunt Mutaties lijsten open standaarden

Hamerstuk

U wordt gevraagd om in te stemmen met de volgende adviezen:

A. Het OBDO stemt in met de plaatsing van de **REST API Design Rules** op de ‘pas toe of leg uit’-lijst.

B. Het OBDO stemt in met de plaatsing van de **NL GOV Assurance profile OAuth 2.0** op de ‘pas toe of leg uit’-lijst en **OAuth 2.0** op de lijst aanbevolen standaarden.

C. Het OBDO stemt in met de plaatsing van **CAA** op de lijst van aanbevolen standaarden.

D. Het OBDO stemt in met het vervangen van **EPUB versie 3.0 door versie 3.2** op de lijst aanbevolen standaarden.

Ad. A) Plaatsing van REST API Design Rules op de ‘pas toe of leg uit’-lijst *(een standaard die helpt REST API’s , koppelvlakken over internet voor het bevragen van databronnen, op een uniforme en voorspelbare manier te ontsluiten)*

Het OBDO wordt gevraagd om in te stemmen met het volgende advies:

A) Plaatsing van REST API Design Rules op de ‘pas toe of leg uit’-lijst.

Om de dienstverlening van de digitale overheid te verbeteren vindt er een transitie plaats in het gegevenslandschap. Initiatieven zoals Common Ground, Haal Centraal en het Digitaal Stelsel Omgevingswet (DSO) willen de digitale overheid efficiënter, veiliger en beter beheersbaar maken door applicaties beter te scheiden van de gegevens en de gegevens alleen bij de bron te beheren. Hierdoor hoeven gegevens niet meer op grote schaal gedupliceerd en gesynchroniseerd te worden. In deze ambitie spelen API’s als ondersteunende technologie een belangrijke rol.

Een API is een koppelvlak dat applicaties met elkaar verbindt over het internet. In de laatste tien jaar heeft ‘Representational state transfer’ (REST) zich ontwikkeld tot een bepalend principe voor het realiseren van API’s. Eenvoudig gezegd doen REST API’s voor applicaties wat websites voor mensen doen. Websites presenteren informatie aan mensen, REST API’s maken gegevens over het internet beschikbaar voor andere applicaties.

REST API’s worden op steeds grotere schaal gebruikt voor koppelingen tussen overheden onderling, tussen overheden en bedrijven en indirect tussen overheden en burgers, bijvoorbeeld via mobiele apps die aangeboden worden door bedrijven of overheden zelf. De overheid moet REST API’s op een veilige, gebruikersvriendelijke en geharmoniseerde manier aanbieden. Omdat de overheid steeds meer REST API’s ontwikkelt en ontsluit, dreigt wildgroei te ontstaan. Zonder afspraken vinden organisaties van de overheid het wiel steeds opnieuw uit en richten ze hun API’s op eigen manier in. Voor ontwikkelaars die (bij bedrijven of bij de overheid) met API’s van de overheid moeten werken, wordt het snel een oerwoud van verschillende implementaties die niet op elkaar aansluiten.

De standaard REST API Design Rules legt een aantal basisafspraken vast om REST API’s op een eenduidige manier te structureren. Dit moet wildgroei tegengaan en zorgen voor een consistenter gegevenslandschap bij de digitale overheid. De standaard maakt minimale, noodzakelijke afspraken over zaken als het identificeren van de ‘resources’ (gegevens), het documenteren van het koppelvlak en het versiebeheer. REST API Design Rules is een Nederlandse standaard die is ontwikkeld in het Kennisplatform API’s en beheerd wordt door Logius.

Advies en gevraagd besluit

Na consultatie van onafhankelijke experts en organisaties die door de standaarden geraakt worden, adviseert het Forum Standaardisatie om REST API Design Rules op de ‘pas toe of leg uit’-lijst te plaatsen. REST API’s van de overheid krijgen door toepassing van deze standaard een eenduidiger structuur, wat wildgroei voorkomt.

Het volledige Forum-advies is te vinden op de website van het Forum Standaardisatie.

Ad. B) Plaatsing van NL GOV Assurance profile OAuth 2.0 op de ‘pas toe of leg uit’-lijst en plaatsing van OAuth 2.0 op de lijst aanbevolen standaarden (*autorisatiestandaarden voor met name webbased applicaties die gegevens uitwisselen met behulp van API’s*)

Het OBDO wordt gevraagd om in te stemmen met de volgende adviezen:

B) Het OBDO stemt in met de plaatsing van de NL GOV Assurance profile OAuth 2.0 op de ‘pas toe of leg uit’-lijst en plaatsing van de OAuth 2.0 op de lijst aanbevolen standaarden.

Ad A) beschrijft hoe API’s steeds prominenter worden ingezet bij de digitale Nederlandse overheid om gegevens bij de bron te kunnen beheren. Net als bij websites speelt beveiliging ook een belangrijke rol bij API’s. Om via een API bij gegevens te komen, moet er eerst authenticatie en autorisatie plaatsvinden.

OAuth 2.0 is een gangbare beveiligingstandaard voor het autoriseren van toegang tot API’s. Deze standaard heeft een generiek karakter en geeft nog veel vrijheid om autorisatieprocedures te implementeren voor verschillende domeinen. Meestal wordt de standaard toegepast met een aanvullend profiel voor een specifiek domein.

NL GOV Assurance profile for OAuth 2.0 is een Nederlands overheidsprofiel op OAuth 2.0, ontwikkeld in het Kennisplatform API’s en beheerd door Logius. Dit profiel is tot stand gekomen in brede samenwerking met belanghebbende organisaties van de overheid, gebaseerd op het internationale overheidsprofiel en toegespitst op de Nederlandse overheid. Zo stelt het profiel bijvoorbeeld dat organisaties van de overheid (met een OIN) PKIOverheid certificaten moeten gebruiken in OAuth. NL GOV Assurance profile for OAuth 2.0 moet gezien worden als een ‘standaard op de standaard’ OAuth 2.0. De verplichting van het overheidsprofiel weegt zwaarder dan de verplichting van de onderliggende gangbare standaard OAuth 2.0. Daarom adviseert Forum Standaardisatie om het profiel op de ‘pas toe of leg uit’ lijst te plaatsen en de onderliggende generieke standaard op de lijst aanbevolen standaarden.

Advies en gevraagd besluit

Na consultatie van onafhankelijke experts en organisaties die door de standaarden geraakt worden, adviseert het Forum Standaardisatie om NL GOV Assurance profile for OAuth 2.0 op de ‘pas toe of leg uit’-lijst te plaatsen. Tevens adviseert het Forum Standaardisatie om OAuth 2.0 te plaatsen op de lijst aanbevolen standaarden. De standaarden dragen bij aan de veiligheid en interoperabiliteit van de digitale Nederlandse overheid.

Het volledige Forum-advies is te vinden op de website van het Forum Standaardisatie.

Ad. C) Plaatsing van CAA op de lijst aanbevolen standaarden (*een standaard voor extra controle op uitgifte van digitale certificaten*)

Het OBDO wordt gevraagd om in te stemmen met het volgende advies:
C) Het OBDO stemt in met de plaatsing van de CAA op de lijst van aanbevolen standaarden.

Sinds het DigiNotar-incident in 2011 zijn er vele ontwikkelingen geweest rond het versterken van het digitale certificatenstelsel. Het heeft geleid tot inzichten die beheerders en gebruikers van certificaten helpen om hun stelsel van maatregelen te toetsen en aan te scherpen. De standaard CAA *(Certification Authority Authorization Resource Record)* is een DNS-record dat domeineigenaren extra controle geeft over SSL-certificaten, die worden uitgegeven voor diens domeinen. Met een CAA-record geeft een domeineigenaar aan welke certificate authority (CA) certificaten uit mag geven voor zijn domeinen. Een domeineigenaar kan dit zelf regelen zonder dat medewerking vanuit de CA hiervoor nodig is. De standaard verkleint de kans dat iemand onterecht een certificaat kan verkrijgen voor domeinen van bijvoorbeeld overheidsinstellingen of banken. Dit biedt extra bescherming tegen aanvallen waarbij de aanvaller zich voordoet als bijvoorbeeld een overheidspartij middels phishing. De CAA-standaard biedt certificate authorities ook de mogelijkheid om melding te maken van foutief aangevraagde certificaten. Hierdoor krijgen domeineigenaren meer inzicht in eventuele foutieve of frauduleuze aanvragen voor het domein. Sinds 2017 moeten CA's bij uitgifte van een certificaat verplicht de CAA-records van het bijbehorende domein controleren, wat de standaard meer effectief maakt.
CAA heeft ook beperkingen. Zo gaat het uit van vertrouwen in de CA: een kwaadwillende CA kan CAA immers ook negeren. Gegeven de beperkte toegevoegde waarde van de standaard is een aanbevolen standaard een passend middel om adoptie te bevorderen. Binnen de overheid is er draagvlak voor het opnemen van CAA op de lijst aanbevolen standaarden.

Advies en gevraagd besluit

Na consultatie van onafhankelijke experts en organisaties die door de standaarden geraakt worden, adviseert het Forum Standaardisatie om de standaard op de lijst van aanbevolen standaarden te plaatsen. Toepassing van de standaard CAA verkleint de kans dat iemand onterecht een certificaat kan verkrijgen voor domeinen van bijvoorbeeld overheidsinstellingen of banken. Desalniettemin is de toegevoegde waarde van de standaard beperkt, omdat deze zelfstandig geen significante beveiligingszekerheid biedt. Gelet hierop is een status als aanbevolen standaard een passend middel om adoptie van CAA te bevorderen.

Het volledige Forum-advies is te vinden op de website van het Forum Standaardisatie.

Ad. D) Vervanging van EPUB versie 3.0 door versie 3.2 op de lijst van aanbevolen standaarden (*een digitoegankelijkheid standaard voor het publiceren van niet-reviseerbare elektronische documenten in e-book formaat, geoptimaliseerd voor gebruik op -maar niet beperkt tot- mobiele apparaten*)

Het OBDO wordt gevraagd om in te stemmen met het volgende advies:

D) Het OBDO stemt in met het vervangen van EPUB versie 3.0 door versie 3.2 op de lijst aanbevolen standaarden.

Door de toenemende digitale dienstverlening vanuit de Nederlandse overheid krijgen steeds meer mensen elektronische documenten vanuit de overheid. Momenteel moeten nieuwe websites van de Nederlandse overheid voldoen aan de toegankelijkheidseisen uit het Tijdelijk Besluit Digitale Toegankelijkheid Overheid. Vanaf juni 2025 moet er in Nederland wetgeving zijn om de European Accessibility Act te implementeren. In dat kader en mede de aandacht voor het onderwerp digitale toegankelijkheid moet het advies voor vervanging van versie 3.0 door 3.2 van EPUB worden bezien.

EPUB is een formaat voor distributie en uitwisselbaarheid van digitale publicaties en documenten. De standaard draagt bij aan het vergroten van de digitale toegankelijkheid binnen de Nederlandse overheid en maakt het mogelijk om documenten, die niet voor bewerking door de ontvanger bestemd zijn, te downloaden, lokaal op te slaan en offline te lezen. Deze weergave is ‘reflowable’, dat wil zeggen dat de weergave zich aanpast aan het type apparaat dat hiervoor gebruikt wordt en waarbij de gebruiker kan kiezen hoe de inhoud gepresenteerd wordt. Digitale documenten in EPUB-format kunnen daardoor op een breed scala aan apparaten (zoals PC’s, e-readers, tablets en smartphones) optimaal worden weergegeven.

De standaard ondersteunt de digitale toegankelijkheid (bijvoorbeeld ten behoeve van mensen met een leesbeperking) door de mogelijkheid om audio en video in te sluiten en te synchroniseren met de tekst. De standaard heeft niet alleen toegevoegde waarde als open e-book standaard, maar ook als breder inzetbare documentstandaard die een alternatief biedt voor PDF in toepassingen waar weergave op mobiele apparaten en digitale toegankelijkheid belangrijk zijn. De geringe marktacceptatie is nog een struikelblok voor een concretere inzet van EPUB als alternatief voor PDF.

Advies en gevraagd besluit

Na consultatie van onafhankelijke experts en organisaties die door de standaarden geraakt worden, adviseert het Forum Standaardisatie om de huidige versie van de standaard op de lijst van aanbevolen standaarden te actualiseren naar versie 3.2. Ten opzichte van EPUB 3.0 heeft EPUB 3.2 geen belangrijke wijzigingen buiten de nodige updates om de standaard actueel te houden. Wel is het in EPUB 3.2 mogelijk metadata over toegankelijkheid volgens de standaard toe te voegen. De gebruiker wordt dan gericht geïnformeerd over de mate van toegankelijkheid.

Het volledige Forum-advies is te vinden op de website van het Forum Standaardisatie.