FAQ DigiD assessment

Basis: Update van de testaanpak DigiD-assessment (1.0) d.d. 26 mei 2020

FAQ versie: 1.3 d.d. 1 juli 2021

Naar aanleiding van de gestelde vragen aan de werkgroep DigiD over de update van de testaanpak DigiD-assessment (1.0) d.d. 26 mei 2020 van NOREA en de FAQ's van 14 oktober 2020 en 1 februari 2021, brengen we onderstaande nieuwe FAQ uit om de vragen van een eenduidig antwoord te voorzien.

Ten opzichte van de vorige versie zijn de volgende FAQ's aangepast:

- U/PW.03: toelichting op gebruik Nonce uitgebreid;
- U/PW.03: Binnen situatie 3, bij het niet voldoen aan CSP, aanvullende maatregelen ten aanzien van het tegengaan van XSS toegevoegd;
- U/PW.03: nieuwe FAQ m.b.t. cookies toegevoegd;

De belangrijkste aanpassingen zijn **blauw gekleurd**.

Beveiligingrichtlijn	Vraag	Antwoord
Algemeen	Hoe gebruik je de TPM van authenticatievoorzieningen die gekoppeld zijn met DigiD?	*Probleemschets* Er is een aantal leveranciers dat een authenticatievoorziening levert, welke is gekoppeld met DigiD waardoor de aansluithouder o.a. het aantal enkelvoudige DigiD aansluitingen zou kunnen beperken en een betere routering kan bewerkstelligen. Sommige van deze leveranciers leveren een ISAE-3000 rapport (TPM) op basis van het DigiD-normenkader over de beveiliging van deze voorziening. De functionaliteit van deze voorzieningen is echter beperkt tot de rol van een intelligent doorgeefluik en het is dan ook maar de vraag of het gebruik van een dergelijke TPM wel zinvol is. Daarnaast vragen verschillende auditors zich af of een dergelijke authenticatie-voorziening wel tot de scope van het DigiD-assessment behoort. *Argumentatie* Bij al deze authenticatievoorzieningen passeert het BSN de voorziening. Daarmee is de authenticatievoorziening per definitie binnen scope van het DigiD-assessment en wordt deze derhalve opgenomen in de beschrijving van het object van onderzoek.

Beveiligingrichtlijn	Vraag	Antwoord
		Als de authenticatievoorziening niet meer functionaliteit heeft dan de bovengenoemde routering, dan wordt het deel van assurance-onderzoek, dat deze authenticatievoorziening betreft, “inclusive” uitgevoerd. Een eventuele TPM van de authenticatievoorziening wordt niet als “carve-out” behandeld.
Algemeen – Bij gebruik van Routeringsvoorziening	Wordt er ook een DigiD assessment uitgevoerd bij een aansluiting via een routeringsvoorziening zoals TVS	*Probleemschets* Wanneer een partij besluit om DigiD te ontsluiten via een Routerings Voorziening (= RV) dan geldt hiervoor ook een assessmentplicht voor op basis van de aansluitvoorwaarden van bijvoorbeeld TVS. Aansluiten op de RV kan direct maar ook via een Clusteraansluiting. Verantwoording kan via een assessment enkelvoudige aansluiting of een assessment meervoudige aansluiting. De scope is exact hetzelfde als bij een “normaal” DigiD assessment. Zie ook website van Logius voor de aansluitvoorwaarden.
Algemeen	Wordt een CDN gezien als een authenticatie-voorziening?	*Probleemschets* Aansluithouders met veel dataverkeer gebruiken in toenemende mate CDN (= Content Delivery Network)-diensten van externe providers. Wordt dit ook gezien als een “authenticatievoorziening”? *Argumentatie* Een CDN is een connectiviteitsdienst, die o.a. kan worden ingezet om DDOS-aanvallen te kunnen pareren. Een CDN wordt *niet* beschouwd als een authenticatievoorziening.
Algemeen	Versienummer in de TPM	*Probleemschets* In sommige TPM’s staat een versie, de release of build-indicatie en in andere TPM’s ontbreekt dit volledig. Wat is de ratio hierachter? Argumentatie Sommige leveranciers onderhouden slechts 1 versie van de software in productie. Zeker bij Agile software-ontwikkeling ligt de opleverfrequentie zodanig hoog, dat er geen twee versies tegelijk in productie worden genomen. In dit geval is vermelding van de versie van de software minder relevant, aangezien de auditor van de aansluithouder erop kan vertrouwen dat de juiste versie van de software is getest door de auditor van de serviceorganisatie. Hogere versies van de software vallen immers onder het wijzigingsbeheer. Indien meer dan één versie van de software in productie-omgevingen in de praktijk kan voorkomen, dan dient de auditor van de aansluithouder vast te stellen of de TPM ook geldt voor de versie die aansluithouder actief in productie heeft. In dat geval dient de auditor van de service-

Beveiligingrichtlijn	Vraag	Antwoord
		organisatie bij het object van onderzoek zo goed als mogelijk te beschrijven vanaf welke versie, release, modificatie, update, build en/of Forms-cycle de TPM geldig is.
U/NW.06	DNSSEC wordt niet ondersteund door sommige cloud computing dienstverleners. Wat nu?	*Probleemschets* Grote cloud computing dienstverleners zoals Microsoft Azure ondersteunen (nog) geen DNSSEC. Is dit dan toch toegestaan? *Argumentatie* De norm wordt onverkort gehandhaafd. Om aan DNSSEC te voldoen moet dit dan (tijdelijk) via derden worden geregeld door de aansluithouder of serviceorganisatie.
U/PW.03	De applicatieleverancier kan (tijdelijk) niet voldoen de verplichte CSP waarden “unsafe-eval” “'unsafe-inline” voor scripts en/of stylesheets,	*Probleemschets* Sommige webapplicaties werken functioneel niet langer, als inline scripts en/of de eval() functie niet meer kunnen worden aangestuurd. Indien deze instellingen wel actief zijn, dan voldoet de webapplicatie niet aan de aangescherpte CSP-eisen bij beveiligingsrichtlijn U/PW.03, zoals die gelden sinds 1 juni 2020. De Content-Security-Policy (CSP) policy is een in-depth beveiligingsmaatregel welke XSS exploits tegengaat. **Let op! Om vast te kunnen stellen of de CSP headers correct zijn geconfigureerd, is het gebruik van online scanners niet voldoende. Afgezien van de vraag of deze tooling een juiste beoordeling maakt, bekijken deze scanners niet het gedrag na DigiD-authenticatie, hetgeen het object is van onderzoek is. Er is dus zoals altijd handmatig onderzoek nodig om ‘false positives’ en/of ‘false negatives’ uit te kunnen sluiten.** De CSP script-src moet als geldige waarde “self” hebben als bron voor JavaScripts. De CSP directives 'unsafe-eval' en/of 'unsafe-inline' zijn onveilig. Met 'unsafe-eval' kan arbitraire code worden uitgevoerd. Met 'unsafe-inline' kunnen scripts uitgevoerd worden die potentieel uit onbetrouwbare bronnen komen. Beide directives zouden daarom niet gebruikt moeten worden. **Om toch gebruik te kunnen maken van inline scripts en stylesheets, moet de 'nonce' directive gebruikt worden. Met een nonce kunnen specifieke inline script en stylesheet elementen gewhitelist worden om te voorkomen dat inline scripts of stylesheets buiten eigen beheer uitgevoerd kunnen worden. Gebruik een sterke random hash als nonce-waarde en zorg er voor dat deze bij iedere request uniek is.**

Beveiligingrichtlijn	Vraag	Antwoord
		In de praktijk is overigens gebleken dat 'unsafe-inline' in combinatie met een Nonce door de browser wordt genegeerd. Het doorvoeren van aanpassingen in de CSP-waarden kan tijdrovend zijn omdat in sommige situaties (legacy) scripts moeten worden herschreven of zelfs een migratie naar een andere technologie noodzakelijk is. <u>Argumentatie</u> Complicerend hierbij is dat bij sommige webservers de CSP-waarden kunnen verschillen per HTML-pagina. Formeel gelden de eisen van het DigiD-assessment alleen voor de pagina's na de DigiD-authenticatie. Hoewel het uiteraard aan te bevelen is voor alle HTML-pagina's de correcte CSP-waarden te configureren, maken verschillende leveranciers (tijdelijk) gebruik van het uitsluitend configureren van de vereiste CSP-configuratie voor de pagina's ná DigiD authenticatie, dit is toegestaan vanwege de scope van het object van onderzoek. Het onderstaande geldt voor de situaties ná DigiD-authenticatie: We onderscheiden drie verschillende situaties, met als basisvoorwaarde dat aan de overige vereisten van de U/PW.03 beveiligingsrichtlijn wordt voldaan: **<u>Situatie 1. Gebruik van "unsafe-inline" en/of "unsafe-eval" vanuit niet-functioneel oogpunt</u>** De CSP bevat "unsafe-inline" en/of "unsafe-eval". Door de auditor wordt vastgesteld dat de reden voor het gebruik van "unsafe-inline" en/of "unsafe-eval" geen functionele reden is. Ook zonder het gebruik van "unsafe-inline" of "unsafe-eval" zou de webapplicatie functioneren of met eenvoudige middelen en inspanning werkend kunnen worden gemaakt. De auditor beoordeelt de norm U/PW.03 met een "voldoet niet". In deze situatie kan Logius de normale oplostermijn hanteren. Indien voor het einde van de door Logius gegeven oplostermijn door de auditor wordt verklaard, dat de situatie 2 of 3 alsnog van toepassing is, dan kan daar wel een verlenging van de oplostermijn uit volgen.

Beveiligingrichtlijn	Vraag	Antwoord
		<u>Situatie 2. Gebruik van “unsafe-inline” en/of “unsafe-eval” vanuit functioneel oogpunt, met niet-afdoende aanvullende maatregelen.</u> De CSP bevat “unsafe-inline” en/of “unsafe-eval”. De reden voor het gebruik van “unsafe-inline” en/of “unsafe-eval” is functioneel. Zonder het gebruik van “unsafe-inline” of “unsafe-eval” kan de applicatie niet werken en ook niet met eenvoudige middelen of inspanning werkend worden gemaakt. Er zijn echter naar het oordeel van de auditor geen aanvullende maatregelen zoals genoemd in situatie 3, die het risico van het gebruik van “unsafe-inline” en/of “unsafe-eval” beperken. De auditor zal de norm U/PW.03 met een “voldoet niet” beoordelen. In deze situatie kan Logius besluiten tot het hanteren van een langere oplostermijn. Daarvoor moet worden voldaan aan de volgende drie voorwaarden: 1. De norm U/PW.03 voldoet niet aan de eisen voor “unsafe-inline” en/of “unsafe-eval” vanwege functionele vereisten. 2. Er is een aantoonbaar ontwikkelplan om vóór *1 november 2021* alsnog te voldoen aan de eisen betreffende “unsafe-inline” en “unsafe-eval”, dan wel dat er voor die termijn afdoende mitigerende maatregelen zijn genomen. 3. De auditor geeft hier een verklaring over, door middel van het opnemen van de volgende tekst onder paragraaf “1.5 Oordelen” van het assurancerapport, dan wel in een aanvullende verklaring: *Voor de norm U/PW.03 geldt dat aan de testaanpak wordt voldaan, behalve op de eisen voor “unsafe-inline” en/of “unsafe-eval”. [Naam organisatie] heeft voor het gebruik van “unsafe-inline” en/of “unsafe-eval” een aantoonbaar ontwikkelplan waarbij redelijkerwijs kan worden aangenomen dat vóór 1 november 2021 aan de gehele testaanpak voor de norm U/PW.03 wordt voldaan, dan wel dat er afdoende maatregelen zijn genomen om het risico van het gebruik van “unsafe-inline” en “unsafe-eval” te mitigeren.* Mede op basis hiervan, kan Logius besluiten of de aansluithouder in aanmerking komt voor een aangepaste oplostijd.

Beveiligingrichtlijn	Vraag	Antwoord
		Situatie 3. Gebruik van "unsafe-inline" en/of "unsafe-eval" vanuit functioneel oogpunt, met afdoende aanvullende maatregelen. De CSP bevat de "unsafe-inline" en/of "unsafe-eval". De reden voor het gebruik van "unsafe-inline" en/of "unsafe-eval" is functioneel. Zonder het gebruik van "unsafe-inline" of "unsafe-eval" kan de applicatie niet werken en ook niet met eenvoudige middelen of inspanning werkend worden gemaakt. De auditor stelt vast dat er afdoende aanvullende maatregelen zijn genomen die het risico van het gebruik van "unsafe-inline" en/of "unsafe-eval" (ten dele) beperken, zoals: I. Het aantoonbaar uitvoeren van code reviews, waarbij alleen door de applicatieleverancier geverifieerde externe bronnen voor externe scripts en stylesheets worden toegestaan en het aantoonbaar implementeren van frameworks in de code voor het opbouwen van HTML structuur zoals bijvoorbeeld Knockout (https://knockoutjs.com/) dat 'secure binding' (https://github.com/brianmhunt/knockout-secure-binding) als een vangnet dwingend toepast. Deze binding voorkomt het ongeautoriseerd samenstellen van HTML code, of: **II. Het aantoonbaar implementeren van een Web Application Firewall (WAF) waarbij (eveneens aantoonbaar) policies worden toegepast om cross site scripting aanvallen tegen te houden.** Mits alle andere instellingen voor U/PW.03 correct zijn ingesteld, zorgen deze aanvullende maatregelen er voor dat de restrisico's tot een minimaal niveau worden beperkt. Formeel blijft het oordeel echter bij U/PW.03 "Voldoet niet" aangezien de CSP-waarden afwijken van de voorgeschreven waarden. In deze situatie kan Logius besluiten tot een reguliere toetsing in het volgende tijdvak. Daarvoor moet worden voldaan aan de volgende voorwaarden: 1. De norm U/PW.03 voldoet niet aan de eisen voor "unsafe-inline" en/of "unsafe-eval" vanwege functionele vereisten.

Beveiligingrichtlijn	Vraag	Antwoord
		2. **De auditor constateert dat er afdoende aanvullende maatregelen conform de hiervoor genoemde onder I en/of II voorbeelden zijn genomen om het risico van het gebruik van "unsafe-inline" en "unsafe-eval" te beperken.** 3. De auditor geeft hier een verklaring over, door middel van het opnemen van de volgende tekst onder paragraaf "1.5 Oordelen" in het assurancerapport, dan wel in een aanvullende verklaring": ** T.a.v. norm U/PW.03 merken we op dat één (1) specifiek onderdeel van de gewenste configuratie-items niet op de juiste wijze is geconfigureerd, waarbij naar het oordeel van de auditor de kwetsbaarheden afdoende zijn beperkt en een verbeterplan is opgesteld. Alle andere configuratie-items zijn wel correct geconfigureerd. Voor nadere informatie kan Logius zich wenden tot de auditor.* Mede op basis hiervan, kan Logius besluiten of de aansluithouder in aanmerking komt voor een reguliere toetsing in het volgende tijdvak.
U/PW.03	**In de testaanpak wordt voorgeschreven dat cookies de flags "Http-only" en "Secure" moeten hebben. Gaat het hier om alle cookies en hoe moet dit worden geïnterpreteerd?**	***Probleemschets*** **Volgens de testaanpak 2.0 van juni 2020 moeten cookies de waarde 'HttpOnly' en 'Secure' hebben. Sommige tooling maakt sessiecookies aan, die echter niet de waarde "Http Only" hebben, terwijl het onderliggende risico, het weglekken van persoonsgegevens door een man-in-the-middle attack niet aan de orde is.** ***Argumentatie*** **Met cookies worden in de testaanpak niet alle cookies bedoeld, maar uitsluitend authenticatie cookies en sessie identificerende cookies. Kortom de eis dient zo te worden geïnterpreteerd dat cookies die sessie en/of persoonsgevoelige informatie bevatten de flags 'HttpOnly' en 'Secure' dienen te bevatten.**
U/PW.03	Wat is de minimale waarde bij de CSP header Referrer Policy?	*Probleemschets* Volgens de testaanpak 2.0 van juni 2020 is de verplichte minimale waarde "same-origin" en bij voorkeur de waarde "no-referrer", leverancier kan deze header niet met de minimale waarde configureren.

Beveiligingrichtlijn	Vraag	Antwoord
		Argumentatie Als de referrer policy header niet geconfigureerd is, wordt “by default” (no-referrer-when-downgrade) de volledige URL (incl. querystring) meegestuurd naar **alle** bestemmingen (ook cross-origin) met hetzelfde protocol. De Referrer policy header voorkomt het verspreiden van de querystrings en mede daarom is het opnemen van deze Referrer Policy header met de juiste voorgeschreven waarde een **verplichting**.
U/TV.01	In sommige TPM’s staat in hoofdstuk 4, Verantwoordelijkheid gebruikersorganisatie, de beveiligingsrichtlijn U/TV.01 niet vermeld. Hoe kan dat?	*Probleemschets* Volgens de template voor de DigiD assurance rapportage is beveiligingsrichtlijn U/TV.01 een beveiligingsrichtlijn die mede de verantwoordelijkheid is van de gebruikersorganisatie. Toch zijn er steeds meer TPM’s, waarbij deze beveiligingsrichtlijn niet is opgenomen in hoofdstuk 4 “Verantwoordelijkheid gebruikersorganisatie’. Hoe zit dat? *Argumentatie* Er is in de markt een tendens dat er steeds meer webapplicaties worden uitgeleverd, waarbij de SAAS leverancier het gehele functionele (toegangs-) beheer verzorgt, inclusief het testen van de applicatie. Als de auditor van de service organisatie vaststelt, dat de gebruikersorganisatie geen beheerders noch gebruikers heeft binnen de DigiD scope, ligt het voor de hand dat U/TV-01 niet in hoofdstuk 4 wordt opgenomen van de TPM. Het blijft de verantwoordelijkheid van de auditor van de gebruikersorganisatie om te bepalen of U/TV.01 getest moet worden bij de gebruikersorganisatie.