VERDONCK KLOOSTER & ASSOCIATES

ADVIES DIGID ASSESSMENT DIGITAAL ONDERTEKENEN MBO

VERDONCK KLOOSTER & ASSOCIATES

ADVIES DIGID ASSESSMENT DIGITAAL ONDERTEKENENEN MBO

Drs. Joep Janssen RE MIM

DATUM	24 maart 2016
STATUS	Definitief
VERSIE	1.0
PROJECTNUMMER	20163050

INHOUDSOPGAVE

1 AANLEIDING EN OPDRACHT

1.1 Aanleiding

SaMBO-ICT, SION en Kennisnet voeren al enige tijd een verkenning uit naar de mogelijkheid tot het digitaal ondertekenen van de onderwijs- en praktijkovereenkomsten in het MBO (op basis van DigiD). Digitaal ondertekenen kan grote voordelen en besparingen opleveren, mits de impact en consequenties beheersbaar en betaalbaar zijn.
Op basis van de referentiearchitectuur onderwijs is een ontwerp van een ondertekendienst gemaakt (Edusign). Het ontwerp van de ondertekendienst vraagt (i.v.m. eisen ministerie en inspectie) niveau Stork-3 waardoor DigiD moet worden gehanteerd als authenticatiemiddel.
Op basis van dit ontwerp is door SURFmarket een offerteprocedure gestart voor de ondertekendienst.

In een samenwerkingsverband met een aantal MBO instellingen is een POC opgezet waarbij enkele scenario's worden getest, zowel in de vorm van een simulatie als voor daadwerkelijk echt gebruik. De service provider Evidos is geselecteerd voor het leveren van de digitale ondertekendienst voor de POC.
De uitkomsten van deze POC dienen tevens als advies aan OCW en de MBO sector over de wijze waarop digitaal ondertekenen kan worden geïmplementeerd in de MBO instelling.
Aandachtspunt binnen deze verkenning/proefopstelling is o.a. de betrouwbaarheid en de beveiliging van het digitaal ondertekenen. In het verlengde hiervan is het ook van belang hoe de accountcontrole in de toekomst zal worden uitgevoerd, indien er sprake zal zijn van digitale ondertekening van de overeenkomsten. Door de toename van digitale administratieve procedures bij instellingen zal het belang van betrouwbare, beveiligde en controleerbare geautomatiseerde informatievoorziening alleen maar toenemen.

Logius vereist dat een instelling die gebruikt maakt van de ondertekendienst met DigiD (voor studenten) jaarlijkse een DigiD assessment laat uitvoeren.
Daarbij wordt nagegaan of de webapplicatie en het beheer daaromheen voldoet aan een 28 tal door het Nationaal CyberSecurityCenter (NCSC) ontwikkelde richtlijnen voor beveiliging van webapplicaties. Op de Logius site wordt het DigiD assessment toegelicht.
Evidos heeft aangegeven een zogenaamde Third Party Mededeling (TPM) te kunnen afgeven, waarin ze aantoont te voldoen aan de DigiD normen. De exacte invulling daarvan moet nog vastgesteld worden.
Het samenwerkingsverband wil goed inzicht hebben in de impact en consequenties van de diverse inrichtingsalternatieven voor het DigiD assessment.

1.2 Opdracht

Stel een beknopt advies op aan de instellingen voor de inrichting van digitaal ondertekenen in hun applicatiearchitectuur, waardoor bij het uitvoeren van een jaarlijkse DigiD assessment zoveel

mogelijk DigiD normen getoetst worden bij de service provider en bij de scholen slechts een beperkt aantal normen getoetst hoeft te worden.
Aandachtspunt is dat de totstandkoming van dit advies zoveel mogelijk steunt op een gezamenlijke aanpak van de deelnemers.

2 WERKWIJZE

De volgende stappen zijn doorlopen:

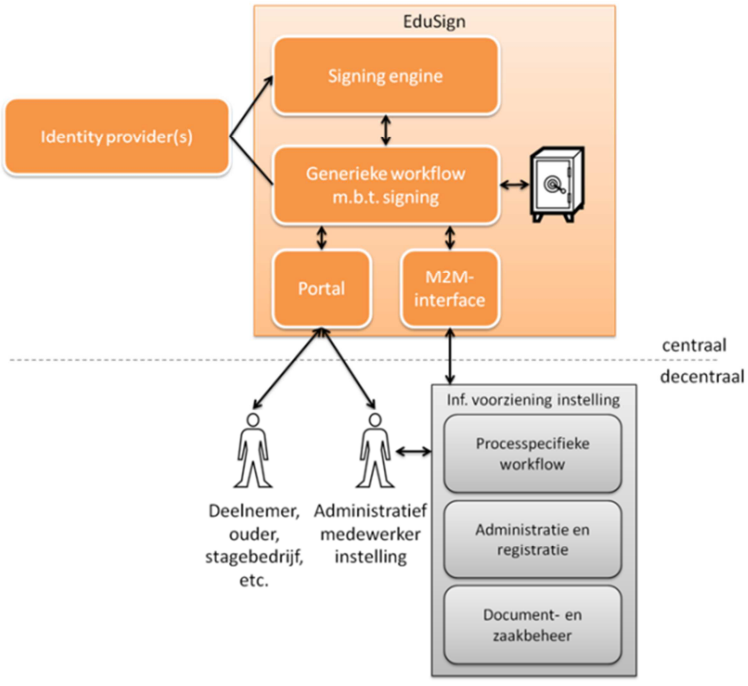
- Bestuderen ontwerp, aanbod en overeenkomst van de ondertekendienst.
- Gesprek met een instelling (ROC De Leijgraaf) over hun opstelling en inrichtingskeuzes.
- In beeld brengen van de inrichtingsalternatieven bij andere instellingen.
- Gesprek met Evidos over hun DigiD assessment en consequenties daarvan voor deelnemende instellingen.
- Analyseren van de opzet van de TPM van Evidos.
- Gesprek met SURfmarket over de bemiddelingsovereenkomst en het Juridische Normenkader Cloudservices Hoger Onderwijs voor Evidos.
- Opstellen globaal concept rapport met bevindingen uit voornoemde gesprekken en analyse en advies voor mogelijke scenario's voor het voldoen aan de DigiD normen
- Bespreken globaal concept rapport met groep participanten/belanghebbenden.
- Opstellen beknopt concept rapport.
- Per mail één reviewronde door werkgroep van definitief rapport.

3 UITGANGSPUNTEN

Onderstaande uitgangspunten beschrijven de reeds vastgestelde onderwerpen die voor het DigiD-assessment een gegeven zijn. De impact van het DigiD-assessment voor de instellingen is dan ook op deze uitgangspunten gebaseerd.

3.1 De ondertekendienst:

- Verzorgt de tijdelijke opslag van het te ondertekenen document, de uitvoering van de (generieke) workflow rondom het verzamelen van de benodigde handtekeningen en het daadwerkelijke ondertekenen.
- Functioneert op STORK betrouwbaarheidsniveau 3 of vergelijkbaar.
- Maakt gebruik van DigiD (voor studenten), maar moet ook in staat zijn om andere authenticatiemiddelen te gebruiken, waaronder in ieder geval SURFcontext, de Kennisnet Federatie (voor instellingen) en e-mail in combinatie met SMS codes (voor stagebedrijven).
- Kan rechtstreeks via het portal benaderd worden.
- Is in staat documenten in PDF formaat te ondertekenen.
- Is koppelbaar met bestaande Student Informatie Systemen SIS), die 'binnen de muren van de instelling' zorg dragen voor zaken als administratie en registratie, documentbeheer, zaakbeheer, en uitvoering van proces-specifieke workflow, logisch ontwerp.
- Schematisch ziet de ondertekendienst er als volgt uit:



3.2 De afnemer van de DigiD aansluiting

Indien een instelling afnemer is van de DigiD aansluiting dan dient deze te voldoen aan de aansluitvoorwaarden voor DigiD. Kernpunten daaruit zijn:

- Afnemer is zelf verantwoordelijk voor het bepalen van het gewenste Zekerheidsniveau voor zijn Afnemersdiensten (webdiensten).
- Afnemer is verplicht te voldoen en blijvend te voldoen aan de geldende “Norm ICT-beveiligingsassessments DigiD”, en dit jaarlijks per DigiD aansluiting aan te tonen door middel van een verklaring die is afgegeven door een Register EDP-auditor. De periode waarin deze verklaring jaarlijks bij Logius dient te worden ingediend is van 1 januari tot 1 mei (art 5.5).
- Voor elke nieuwe aansluiting van Afnemer op de productieomgeving van DigiD dient binnen 2 maanden na aansluiting een aparte verklaring te worden ingediend. De eerstvolgende verklaring dient te worden ingediend conform de regeling in artikel 5.5, met dien verstande dat in de eerste 12 maanden na aansluiting hooguit eenmaal een verklaring hoeft te worden ingediend.
- Een in het kader van het DigiD assessment afgegeven Third Party Mededeling is maximaal 12 maanden geldig en kan slechts eenmaal gebruikt worden.
- De kosten voor het DigiD assessment en de verklaring komen volledig voor rekening van Afnemer.
- Indien uit de verklaring blijkt dat niet of niet volledig wordt voldaan aan de geldende “Norm ICT-beveiligingsassessments DigiD” heeft Logius het recht zonder aankondiging vooraf de levering van DigiD op te schorten. (In de praktijk zendt Logius eerst een verzoek tot opstellen van een Verbeterplan en vraagt om binnen een nader te bepalen termijn een heraudit naar doorgevoerde verbeteringen.)

4 DE IMPACT VOOR DE INSTELLING

4.1 Het DigiD assessment in vogelvlucht

Instellingen zijn en blijven eigenaar van de gegevens in de ondertekendienst. Een instelling moet over deze gegevens kunnen beschikken wanneer dit nodig blijkt. De instelling is verantwoordelijk voor de risicobeheersing en beveiliging van de elektronische dienstverlening.
De instelling die gebruikt maakt van de ondertekendienst met DigiD dient jaarlijkse een DigiD assessment uit te laten voeren.
Evidos biedt de ondertekendienst “Ondertekenen.nl” aan. Hiervoor is ten behoeve van de instellingen door SURFmarket een bemiddelingsovereenkomst **met** een Juridische Normenkader Cloudservices Hoger Onderwijs met Evidos gesloten.
In de bemiddelingsovereenkomst is opgenomen dat Evidos voldoet aan beveiligingseisen en een TPM (“Third Party Memorandum”) over haar dienstverlening oplevert. SURFmarket en Evidos hebben aangegeven in nadere afspraken vast te leggen dat Evidos jaarlijks een DigiD assessment rapport oplevert over haar DigiD dienstverlening (een zogenaamd “DigiD TPM”).
De DigiD TPM heeft betrekking op de huidige ondertekendienst. Indien er grote wijzigingen in de dienst optreden dan kan dit tot aanpassing van de huidige TPM leiden. Dit is ter beoordeling van Evidos en de auditor die de TPM afgeeft.
De bemiddelingsovereenkomst geeft de algemene voorwaarden aan voor de levering van de ondertekendienst. De instelling sluit op basis van de bemiddelingsovereenkomst zelf een gebruikersovereenkomst af met Evidos waarmee de algemene voorwaarden van toepassing worden verklaard op de dienstverlening van Evidos aan de instelling. Deze overeenkomsten vormen in opzet een goede basis voor het DigiD assessment.

De instelling dient ook zelf aan een aantal DigiD normen te voldoen. Een aantal maatregelen om aan deze normen te voldoen wordt ook beoordeeld in het onderzoek dat in het kader van de jaarrekeningcontrole door de accountant wordt uitgevoerd naar de geautomatiseerde informatiesystemen. Doel daarvan is vast te stellen of voldoende algemene maatregelen binnen de (automatiserings-)organisatie zijn genomen om de betrouwbare en continue werking van de geautomatiseerde informatiesystemen te waarborgen. Zie voor verdere details hierover paragraaf 5.3.

Een DigiD-assessment dat is gebaseerd op deze uitgangspunten kost plm. 5000 euro (excl BTW)
Alle andere combinaties (o.a. zelfbouw door leveranciers) kunnen afwijkende situaties tot gevolg hebben

4.2 Bij een koppeling van de ondertekendienst aan een SIS

Bij de koppeling van een SIS aan de ondertekendienst (d.m.v. een API) valt alleen het koppelvlak van Ondertekenen.nl tot verantwoordelijkheid van Evidos.

Het DigiD-assessment moet altijd worden aangevraagd door de instelling, ook bij integratie met “SIS uit de cloud”
Eigen gemaakte koppelingen en alle overige keten-applicaties blijven verantwoordelijkheid instellingen en vallen onder de reguliere accountantscontroles IT controls (waarbij o.a. ISAE 3402-certificering type-2 van service providers kan worden gebruikt)

5 HET DIGID ASSESSEMENT

5.1 De stappen

Het stappenplan omvat 4 stappen voor het uitvoeren van een DigiD assessment. In de praktijk blijkt dat vaak een groot aantal beheertaken voor webapplicaties is ondergebracht bij IT leveranciers. Tijdens de voorbereiding wordt met de instelling vastgesteld welke van de in totaal 28 normen onder de verantwoordelijkheid vallen van de instelling vallen en welke onder de verantwoordelijkheid van de IT leveranciers.

Stap1. Zelf toetsen a.d.h.v. de richtlijnen.
In deze stap wordt een proefaudit uitgevoerd met de volgende resultaten. De proefaudit kan door (de auditor van) de instelling zelf uitgevoerd worden of door de DigiD auditor.
Indien het DigiD assessment voor het eerst wordt uitgevoerd dan wordt deze stap dringend geadviseerd. Bij vervolg assessments kan deze stap, indien er weinig wijzigingen in de processen en organisatie zijn geweest, worden overgeslagen.

1. Bepalen scope en verdeling DigiD verantwoordelijkheid

Resultaat: Inzicht in de verdeling van verantwoordelijkheden tussen de instelling en de IT leveranciers. Inzicht in welke normen door de instelling zelf worden ingevuld.

2. Voorbereiding proefaudit

Resultaat: Voor de interviews zijn de juiste personen bekend en te bestuderen documentatie is beschikbaar. Interviewpartners zijn voorbereid. De interviews zijn ingepland.

3. Uitvoeren proefaudit

Resultaat: De uitkomsten van de proefaudit bestaan uit bevindingen en aanbevelingen over de mate waarin de maatregelen in de instelling in overeenstemming zijn met de vereisten van de DigiD norm.

4. Presenteren resultaten

Resultaat: Een presentatie waarin op managementniveau inzicht geboden wordt in de achtergrond en aanleiding van de DigiD audit, de mate van conformiteit aan de normen voor de DigiD audit, de mate waarin aangesloten kan worden op de reguliere accountantscontrole, sterkten en zwakten en benodigde vervolgacties.

Stap 2: Maatregelen treffen
In deze stap worden eventuele tekortkomingen aangepakt. Nagegaan wordt welke maatregelen de hoogste prioriteit hebben en hoe snel en met welke diepgang de verbeteringen moeten worden doorgevoerd. Adviseurs kunnen de instelling adviseren bij deze stap.

Resultaat: Verbeterde beveiligingsmaatregelen met in acht name van het ambitieniveau van de instelling.

Stap 3: Audit uitvoeren

In deze stap voert de auditor de feitelijke DigiD audit uit conform de auditprotocollen zoals deze geldig zijn. Dit dient plaats te vinden door een door de NOREA gecertificeerde Register EDP auditors (RE).
De auditor bestudeert de documentatie en houdt interviews.
De auditor beoordeelt de opzet (documentatie) en het bestaan (feitelijk uitgevoerde activiteiten) en velt een oordeel per norm, met een gedetailleerde onderbouwing van de argumentatie. De werking, het uitvoeren van beheersmaatregelen over een langere periode, wordt niet getoetst.

De auditor toetst de auditrapportage van de leverancier aan de algemene richtlijnen voor de rapportage over DigiD audits en op de volledigheid van de overeengekomen te toetsen normen.

De bevindingen legt de auditor vast in een rapportage.
Resultaat: DigiD assessment rapportage, bestaande uit:

1. totaaloverzicht van de scores per norm, maar geen samenvattend oordeel;
2. per norm een uitspraak of de interne beheersingsmaatregelen, - in audit termen - 'in alle van materieel belang zijnde aspecten, op afdoende wijze qua opzet en bestaan zijn ingeregeld';
3. per norm een toelichting op de uitspraak en eventueel voorstellen voor verbetering;
4. een beschrijving van de onderzochte dienst en de betrokken leveranciers

Resultaat: Uitgevoerde DigiD assessment, leidend tot een auditrapport welke voldoet aan de eisen van Logius.

Stap 4: Bevindingen naar Logius sturen

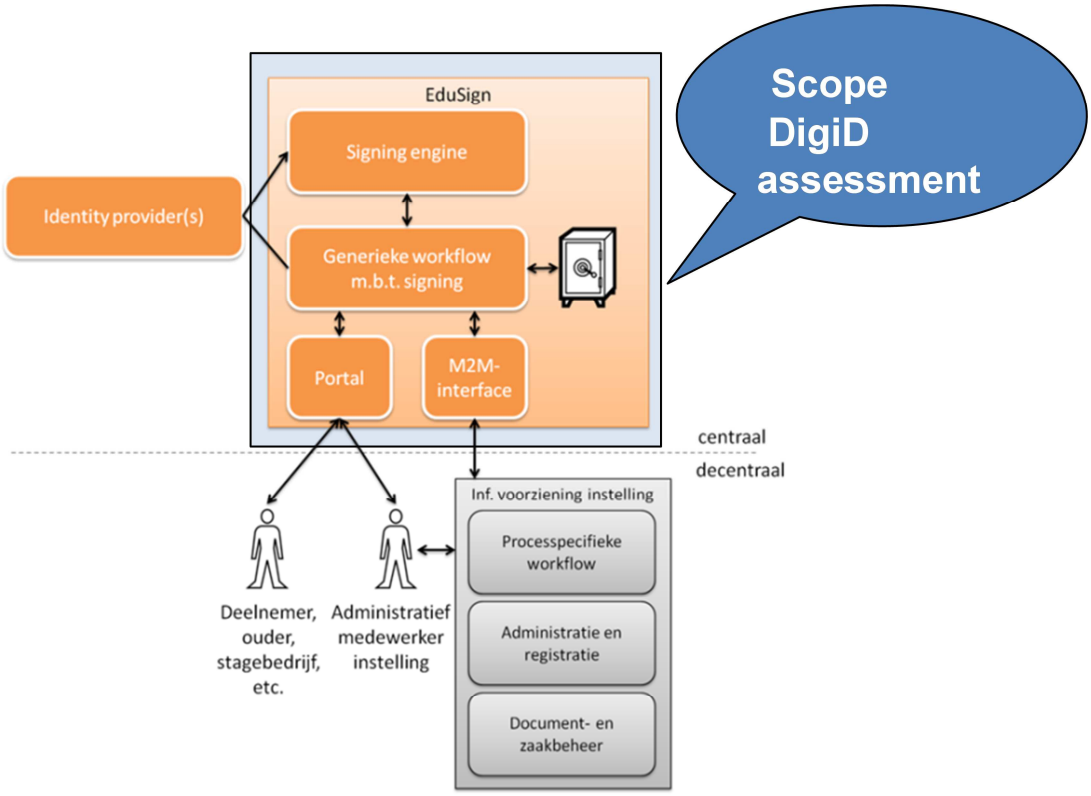
Het rapport van de auditor en het TPM rapport van de IT service organisatie worden door de instelling aangeboden aan Logius. Logius zendt vervolgens haar reactie terug aan de instelling. Indien niet aan alle DigiD normen wordt voldaan, dan zal Logius om een verbeterplan vragen. Soms vraagt Logius bij onduidelijkheden om een nadere toelichting van de auditor.

5.2 De scope

Het DigiD assessment is gericht op de ‘webfacing’ onderdelen van de digitale dienstverlening aan burgers.

Voor de ondertekendienst houdt dit in dat het object van onderzoek is de webomgeving van de DigiD aansluiting. Het onderzoek richt zich op de webapplicatie, de URLs waarmee deze kunnen worden benaderd, de infrastructuur (binnen de DMZ waar webapplicaties zich bevinden) en een aantal ondersteunende processen conform de “Norm ICT-beveiligingsassessments DigiD” van Logius.

Schematisch:



5.3 De DigiD normen

De normen voor het DigiD assessment zijn een subset van 28 beveiligingsrichtlijnen uit de Nationaal Cyber Security Centrum (NCSC) richtlijn.

De normen betreffen de governance, het applicatie- en infrastructuurbeheer van de ondertekendienst bij de instelling en de IT serviceprovider.
In bijlage A is een overzicht van de 28 normen opgenomen.

Evidos levert naar verwachting een TPM waarin alle 28 DigiD normen zijn opgenomen. Een aandachtspunt is nog B0-13. Aanvankelijk was deze norm niet door Evidos opgenomen. De norm vereist dat ook dat de serviceprovider maatregelen treft om op een gecontroleerde wijze websites

te verwijderen. Evidos heeft aangegeven bij deze norm zelf een procedure te zullen hanteren voor het op een gecontroleerde wijze verwijderen van een website. Evidos geeft tevens aan welke normen bij de instelling getoetst moeten worden. Deze komen overeen met de normen die bij de instelling getoetst moeten worden. Evidos heeft aangegeven de TPM binnen 2 maanden na live gaan van de dienst te kunnen opleveren.

De instelling is zelf verantwoordelijk voor 6, en in een enkel geval, 7 DigiD normen.
In onderstaand schema zijn de normen die voor de instelling gelden aangegeven.

Tevens is aangegeven is welke norm in de bemiddelingsovereenkomst en het Juridische Normenkader Cloudservices Hoger Onderwijs met Evidos is belegd. Indien de instelling op basis van deze bemiddelingsovereenkomst een gebruikersovereenkomst sluit met Evidos, dan is daarmee norm B0-14 (Leg afspraken met leveranciers vast in een overeenkomst.) afdoende afgedekt.

Enkele van deze normen kunnen ook als onderdeel van de jaarrekeningcontrole door de accountant zijn onderzocht. De accountantscontrole is onder andere gericht op het vaststellen van de betrouwbaarheid van de financiële informatie/verslaggeving van de instelling. Aangezien deze financiële informatie in de meeste gevallen rechtstreeks afkomstig is uit geautomatiseerde informatiesystemen, is de betrouwbare en continue werking van die systemen van direct belang voor de jaarrekeningcontrole.
Het doel van het onderzoek naar de geautomatiseerde informatiesystemen is om vast te stellen of voldoende algemene maatregelen binnen de (automatiserings-)organisatie zijn genomen om de betrouwbare en continue werking van de geautomatiseerde informatiesystemen te waarborgen (de zogenaamde General Computer Controls; GCC). Hiervoor bestaat echter geen standaard normenkader. De vier deelgebieden die hierbij doorgaans onderwerp van onderzoek zijn:

1. Geautomatiseerde gegevensverwerking: het waarborgen dat de operationele informatiesystemen blijven werken zoals bedoeld en dat problemen (tijdig) kunnen worden hersteld;
2. Informatiebeveiliging: het waarborgen dat toegang tot systemen en gegevens uitsluitend geautoriseerd plaatsvindt;
3. Onderhoud*: het waarborgen dat gewijzigde informatiesystemen blijven voldoen aan de eisen op het gebied van interne beheersing / financiële rapportage;
4. Ontwikkeling en implementatie**: het waarborgen dat informatiesystemen zodanig worden ontwikkeld/geselecteerd en geïmplementeerd dat ze voldoen aan de eisen op het gebied van interne beheersing / financiële rapportage.

   *) Alleen van toepassing als belangrijke wijzigingen aan informatiesystemen worden doorgevoerd.

   **) Alleen van toepassing als onlangs (binnenkort) een nieuw informatiesysteem is/wordt ingevoerd.

Indien het oordeel van de accountant positief is over deze maatregelen, dan kan een aantal van deze maatregelen tevens ingezet worden voor de DigiD audit. Daarbij dient wel opgemerkt te

worden dat door de toenemende digitalisering van de administratieve processen van de instellingen het belang van de GCC steeds groter wordt. Dit geldt zeker voor de digitale ondertekendienst. Het DigiD assessment stelt hoge eisen aan op orde hebben van de GCC. De DigiD auditor (RE) zal hier altijd een eigen oordeel vormen over de kwaliteit van de beheersmaatregelen.

Nummer	Omschrijving DigiD norm	In Bemiddelings-overeenkomst	In onderzoek General Computer Controls
B0-5	Wijzigingenbeheer/testen	Nee	Ja
B0-12	Toegangsbeveiliging	Nee	Ja
B0-13	Verwijderen oude websites/content	Nee	Nee
B0-14	Afspraken met leveranciers	Ja	Ja
B5-3	Bescherming gevoelige gegevens	Nee	Nee
B7-9	Governance beveiliging	Nee	Ja

Indien de instelling zelf sleutels beheert is ook normen B5-1 (Geen onversleutelde sleutels op de server) van toepassing.

In bijlage B is een gedetailleerd werkblad opgenomen van werkzaamheden die bij de instelling moeten worden uitgevoerd om voor de normen de opzet en het bestaan van de beheersmaatregelen vast te stellen.

6 AANBEVELINGEN

In de vorige hoofdstukken zijn de uitgangspunten en randvoorwaarden voor een uit te voeren DigiD assessment uitgewerkt.
Onderstaand volgen een aantal nadere aanbevelingen om de voorbereiding en uitvoering van het DigiD assessment zo succesvol en doelmatig mogelijk te maken.

1. Maak duidelijke afspraken met Evidos over het tijdig aanleveren van de DigiD TPM. De eerste keer binnen 2 maanden na livegang.
2. Steun voor het voldoen aan de DigiD normen zoveel mogelijk op de reeds doorgevoerde beheersmaatregelen (de “General Computer Controls”) in het kader van het onderzoek dat de accountant uitvoert naar de geautomatiseerde informatiesystemen als onderdeel van de jaarrekeningcontrole. Door de toenemende digitalisering van de administratieve processen binnen de instelling zullen deze maatregelen steeds belangrijker worden voor het verkrijgen van een goedkeurende verklaring.
3. Ontwikkel zoveel mogelijk voor de instellingen gestandaardiseerde globale procedures en controlemaatregelen voor de DigiD normen. Maak daarbij onderscheid in procedures voor het rechtstreeks invoeren van gegevens in het portaal en het geautomatiseerd koppelen van het SIS aan de ondertekendienst. Deze kunnen vervolgens door iedere instelling uitgewerkt kunnen worden in specifieke procedures en maatregelen.
4. Indien voor de eerste keer een DigiD assessment uitgevoerd wordt, voer dan voorafgaand aan de formele DigiD audit eerst een proefaudit uit. Op basis hiervan kunnen eventuele ‘kinderziekten’ opgelost worden en kan voorkomen worden dat bij de definitieve DigiD audit tekortkomingen worden geconstateerd, met de verplichting om deze binnen een gestelde termijn te verbeteren en een heraudit te laten uitvoeren.

A Bijlage: DigiD normen

Nr	Beschrijving van de beveiligingsrichtlijn	Oordeel
B0-5	Alle wijzigingen worden altijd eerst getest voordat deze in productie worden genomen en worden via wijzigingsbeheer doorgevoerd.	Voldoet / Voldoet niet
B0-6	Maak gebruik van een hardeningsproces, zodat alle ICT-componenten zijn gehard tegen aanvallen.	
B0-7	De laatste (beveiligings)patches zijn geïnstalleerd en deze worden volgens een patchmanagement proces doorgevoerd.	
B0-8	Penetratietests worden periodiek uitgevoerd.	
B0-9	Vulnerability assessments (security scans) worden periodiek uitgevoerd.	
B0-12	Ontwerp en richt maatregelen in met betrekking tot toegangsbeveiliging/toegangsbeheer.	
B0-13	Niet (meer) gebruikte websites en/of informatie moet worden verwijderd.	
B0-14	Leg afspraken met leveranciers vast in een overeenkomst	
B1-1	Er moet gebruik worden gemaakt van een Demilitarised Zone (DMZ), waarbij compartimentering wordt toegepast en de verkeersstromen tussen deze compartimenten wordt beperkt tot alleen de hoogst noodzakelijke.	
B1-2	Beheer- en productieverkeer zijn van elkaar gescheiden.	
B1-3	Netwerktoegang tot de webapplicaties is voor alle gebruikersgroepen op een zelfde wijze ingeregeld.	
B2-1	Maak gebruik van veilige beheermechanismen.	
B3-1	De webapplicatie valideert de inhoud van een HTTP-request voor die wordt gebruikt.	
B3-2	De webapplicatie controleert voor elk HTTP verzoek of de initiator geauthenticeerd is en de juiste autorisaties heeft.	
B3-3	De webapplicatie normaliseert invoerdata voor validatie.	
B3-4	De webapplicatie codeert dynamische onderdelen in de uitvoer.	
B3-5	Voor het raadplegen en/of wijzigen van gegevens in de database gebruikt de webapplicatie alleen geparametriseerde queries.	
B3-6	De webapplicatie valideert alle invoer, gegevens die aan de webapplicatie worden aangeboden, aan de serverzijde.	
B3-7	De webapplicatie staat geen dynamische file includes toe of beperkt de keuze mogelijkheid (whitelisting).	
B3-15	Een (geautomatiseerde) blackbox scan wordt periodiek uitgevoerd.	
B3-16	Zet de cookie attributen ‘HttpOnly’ en ‘Secure’.	

Nr	Beschrijving van de beveiligingsrichtlijn	Oordeel
B5-1	Voer sleutelbeheer in waarbij minimaal gegarandeerd wordt dat sleutels niet onversleuteld op de servers te vinden zijn.	
B5-2	Maak gebruik van versleutelde (HTTPS) verbindingen.	
B5-3	Sla gevoelige gegevens versleuteld of gehashed op[1].	
B5-4	Versleutel cookies.	
B7-1	Maak gebruik van Intrusion Detection Systemen (IDS).	
B7-8	Voer actief controles uit op logging.	
B7-9	Governance, organisatie, rollen en bevoegdheden inzake preventie, detectie en response inzake informatiebeveiliging dienen adequaat te zijn vastgesteld.	

[1] Voor zover betrekking hebbend op DigiD

B Bijlage: Werkblad DigiD voor instellingen

NCSC Norm	Omschrijving	Doel	NOREA Categorie	Scope instelling	Tevens af te dekken met audit	Domein	Te interviewen persoon	Gevraagde documentatie	(Deel-) waarnemingen op werking	Vragen audit	Documentatie instelling	Antwoorden interview instelling	Uitkomst deelwaarneming instelling	Oordeel en motivatie	Aanbevelingen
B0-5	Alle wijzigingen worden altijd eerst getest voordat deze in productie worden genomen en worden via wijzigingsbeheer doorgevoerd.	Garanderen van een correcte en veilige werking van ICT-voorzieningen door het op een gecontroleerde manier doorvoeren van wijzigingen.	Governance	Bij nieuwe releases/ grotere patches van de leverancier afwegen maken of een acceptatietest noodzakelijk is. Dit afstemmen in gebruikersgroep. Bij klant specifieke aanpassingen test uitvoeren. Formeel acceptatiebesluit door eigenaar. Bijwerken CMDB.	ISO 27001 Jaarrekening General Computer Controls (GCC)	Applicatie Hosting	Manager beheer	Wijzigingenproces met rollen en verantwoordelijkheden (RACI tabel). Uitgewerkt testproces. Componentenoverzicht en Configuratieleverancier. doorgevoerde wijzigingen.	Nalopen alle stappen van 2-3 doorgevoerde wijzigingen en testen.	Is er een vastgestelde wijzigingenprocedure? Bestaat er een ChangeAdvisoryBoard (CAB) met taken, verantwoordelijkheden en bevoegdheden? Worden alle wijzigingen in de CMDB bijgehouden of in een andere vastlegging? Worden er (security) tests uitgevoerd? Worden de testresultaten beoordeeld en goedgekeurd door de procseigenaar? Is er een OTAP straat? Worden de wijzigingen in prioriteitenklassen verdeeld? Zijn fall back scenario's beschikbaar? Worden systemen gaudit op doorgevoerde wijzigingen?					
B0-12	Ontwerp en richt maatregelen in met betrekking tot toegangsbeveiliging / toegangsbeheer.	Voorkomen van ongeautoriseerde toegang tot netwerken, besturingssystemen, informatie en informatiesystemen en diensten, zodat schade bij misbruik zo veel mogelijk beperkt wordt.	Infra-proces	a. Voor toegang tot applicatie: - voor medewerkers - voor beheerders b. Voor toegang tot infrastructuur indien applicatie draait op infrastructuur installing	ISO 27001 Jaarrekening General Computer Controls (GCC)	Applicatie Framework Hosting Netwerk segment DigiD webservers	Manager beheer Security officer	Architectuur applicatie. Architectuur hosting omgeving. Proces van beheer en periodieke toetsing van toegangsrechten (verstrekken, wijzigen, intrekken). Overzicht van toegekende rechten (per configuratieitem). Afspraken over gebruik wachtwoorden.	Nalopen uitgevoerde periodieke toetsen op toegekende rechten. Nalopen toegekende rechten van de ontwikkelaars en de infra beheerders (beheer-accounts).	Bestaat er een beleid mbt toegangsrechten op basis van need to know need to have? Bestaat en een beleid voor beheer wachtwoorden? Er is periodieke controle op rechten van in-, door- en uitstroom van personeel? Zijn er geen standaard wachtwoorden bij administrator account? Worden shared accounts beperkt? Is een risicoanalyse uitgevoerd? Worden Create, Read, Update and Delete (CRUD) matrixen toegepast voor rechtenbeheer? Is functiescheiding doorgevoerd? Ligt dit vast in CMDB of andersins?					
B0-13	Niet (meer) gebruikte websites en/of informatie moet worden verwijderd.	Voorkomen van misbruik van 'oude' en niet meer gebruikte websites en/of informatie.	Governance	Opdracht verlening aan leverancier. Check door instelling op uitvoering opdracht door leverancier en verlenen decharge. Afspraken over archivering data.		Beheer websites van instelling	Manager beheer Procesmanager	Afspraken met leveranciers over beheer websites. Overzicht van gehoste/ beëindigde websites. Relatie met wijzigingenbeheer nagaan.	Nalopen uitgevoerde toets op gebruik websites. Nalopen actief zijn van beëindigde websites. Nalopen decharge van leverancier op verslag verwijderen website.	Wordt periodiek gecheckt op net gebruikte websites of afgelopen contracten? Wordt gecheckt op verouderde content? Zijn hier afspraken over met klanten. Wordt de naleving periodiek gecontroleerd? Wordt decharge verleend? Er dient een overzicht (of CMDB) zijn van de websites. Elke website moet een eigenaar hebben die verantwoordelijk is dat niet meer gebruikte websites en/of informatie die niet meer wordt gebruikt wordt verwijderd. Daarnaast dient minimaal jaarlijks een controle te worden uitgevoerd of de operationele websites nog worden gebruikt en/of informatie bevat daadwerkelijk is verwijderd.					
B0-14	Leg afspraken met leveranciers vast in een overeenkomst.	Handhaven van het beveiligingsniveau, wanneer de verantwoordelijkheid voor de ontwikkeling van de webapplicatie en/of beheer van de webapplicatie is uitbesteed aan een andere organisatie.	Governance	Standaard overeenkomst leverancier met eisen betreffende audit, security, TPM en SLA.	ISO 27001 Jaarrekening General Computer Controls (GCC)	Housing/ Colocaties Contract-management	Contractmanager Security officer	Contract SLA Rapportages Incidentmeldingen. Met leverancier. Aandacht voor security en auditing (TPM).	Nalopen uitkomsten toetsingen rapportages, afhandeling incidenten en periodieke overleggen.	Is er een contractenregister? Zijn in de contracten eisen over beveiliging, beheer en auditing/ TPM vastgelegd? Wordt jaarlijks een DigiD TPM ontvangen?	Bemiddelingsovereekomst Evidos Ondertekenen.nl Juridische Normenkader Cloudservices Hoger Onderwijs				
B2-1	Maak gebruik van veilige beheermechanismen.	Voorkomen van misbruik van beheer-voorzieningen.	Infra-proces	Primair bij leverancier. Van toepassing voor installing indien remote toegang door beheerder van applicatie mogelijk is. Voor infrastructuur indien applicatie draait op infrastructuur installing.		Hosting Netwerksegment DigiD webservers	Manager beheer Security officer	Architectuur hosting omgeving. Configuratieoverzicht: netwerkprotocollen, toegangspaden. Gebruik wachtwoorden, VPN, strong authentication en beheer IP adressen	Nalopen instellingen.	Is er een risicoanalyse uitgevoerd? Op welke wijze is dit doorgevoerd? Hoe is dit vastgelegd? Hoe wordt dit gemonitord? Wordt zorg gedragen voor veilige beheermechanismen? Hierbij valt te denken aan strong authentication, sterke wachtwoorden, gebruik VPN verbindingen, afscherming van beheerfunctionaliteit op basis van IP restricties.					
B5-1	Voor sleutelbeheer in waarbij minimaal gegarandeerd wordt dat sleutels niet onversleuteld op de servers te vinden zijn.	Doelmatig gebruik van cryptografische technieken door het beheren van cryptografische sleutels.	Infra-proces	Primair bij leverancier Van toepassing voor installing indien installing zelf sleutels beheert. Voor infrastructuur indien applicatie draait op infrastructuur installing.		Hosting	Manager beheer Security officer	Procedure sleutelbeheer. Architectuur hosting omgeving. Configuratieoverzicht: doorgevoerde instellingen.	Nalopen of privé sleutels niet onversleuteld op de server staan.	Worden versleutelde certificaten gebruikt? Worden sleutels onversleuteld opgeslagen? Is er een risicoanalyse uitgevoerd? Op welke wijze is dit doorgevoerd? Hoe is dit vastgelegd? Hoe wordt dit gemonitord?					
B5-3	Sla gevoelige gegevens versleuteld of gehashed op.	Voorkom misbruik van opgeslagen vertrouwelijke gegevens.	Infra-proces	Voor applicatie uitvoeren risicoanalyse op door installing opgeslagen gevoelige gegevens. In overleg met leverancier. Deze richtlijn geldt voorafdrag uitsluitend voor gegevens die in het DMZ staan. Voor infrastructuur indien applicatie draait op infrastructuur installing.	ISO 27001 Jaarrekening General Computer Controls (GCC) Privacy audit (PIA)	Hosting Afspraken met leverancier?	Manager beheer Security officer	Beleid rondom gevoelige informatie. Architectuur applicatie en hosting omgeving. Uitkomsten uitgevoerde analyse gevoelige (WBP) gegevens en wachtwoorden. Configuratieoverzicht: doorgevoerde instellingen.	Nalopen of gevoelige gegevens (w.o. wachtwoorden) versleuteld opgeslagen zijn.	Bevinden zich gevoelige gegevens in het web facing front end (DMZ)? Is er een risicoanalyse uitgevoerd? Op welke wijze is dit doorgevoerd? Hoe is dit vastgelegd? Hoe wordt dit gemonitord? Nagaan of de procesverantwoordelijke expliciet de gevoeligheid van het (informatie)systeem vaststelt en eventuele aanvullende maatregelen.	Juridische Normenkader Cloudservices Hoger Onderwijs				
B7-9	Governance, organisatie, rollen en bevoegdheden inzake preventie, detectie en response inzake informatiebeveiliging dienen adequaat te zijn vastgesteld.	Managen (sturen en beheersen) van de informatiebeveiliging binnen de organisatie.	Governance	Volledig	ISO 27001 Jaarrekening General Computer Controls (GCC)	Beleid en organisatie	Manager beheer Security officer	Informatiebeleids-organisatie- en planningsdocumenten. Taken, rollen en verantwoordelijkheden voor informatiebeveiliging. Security testprocedure.	Nalopen actualisatie documenten. Nalopen besluitvorming, communicatie, evaluatie, feedback (PDCA). Nalopen afhandeling 2-3 security incidenten door security officer	Nagaan of de volgende verantwoordelijkheden zijn vastgesteld en toegekend: - Directie verantwoordelijkheid (eigenaarschap) voor de webapplicatie die gebruik maakt van DigiD. Veelal zal dit belegd zijn bij een afdelingshoofd. - Eindverantwoordelijkheid voor de informatiebeveiliging binnen de organisatie. Veelal zal dit belegd zijn bij de leiding van de organisatie. - Kaderstellende en toetsende verantwoordelijkheid op het gebied van informatiebeveiliging namens de leiding van de organisatie. Dit omvat ook de verantwoordelijkheid voor het uitdragen van de security kaders, het toetsen van de naleving van de kaders het actieren op security incidenten. Is de security officer betrokken bij de afhandeling van security incidenten? Veelal zal dit belegd zijn bij de security officer. Een uitgewerkt informatiebeveiligingsbeleid en/of een uitgewerkt informatiebeveiligingsplan is bij deze norm geen vereiste, maar biedt wel een goed kader voor het toekennen van de verantwoordelijkheden voor informatiebeveiliging.					