



Digitaal ondertekenen in het mbo

Ervaringen met het digitaal ondertekenen van de onderwijs-
overeenkomst (OOK) en de praktijkovereenkomst (POK)

Laat ict werken **voor het onderwijs**

Inhoudsopgave

> Inhoudsopgave	2
> Inleiding	3
> 1. Achtergrond	4
> 2. Aandachtspunten bij digitaal ondertekenen	8
> 3. Speelveld	12
> 4. Stappenplan	16
> 5. Digitaal ondertekenen in de praktijk	22
> Tot slot	28
> Colofon	29



Inleiding

Digitale communicatie is breed geaccepteerd en wordt meer en meer de standaard, ook in het onderwijs. Digitalisering maakt stevige efficiencylagen in de administratieve processen van onderwijsinstellingen mogelijk, maar vraagt tegelijkertijd om specifieke aandacht voor wet- en regelgeving, beveiliging en privacy.

Digitaal ondertekenen in het mbo

Een aantal jaar geleden zijn Kennisnet, saMBO-ICT en SURF gestart met een project op het gebied van het digitaal ondertekenen van de onderwijsovereenkomst (OOK) en de praktijkovereenkomst (POK) in het middelbaar beroepsonderwijs. Ze hebben onder andere gekeken naar aandachtspunten op het gebied van documentmanagement, informatiebeveiliging en privacy. Ook hebben ze overlegd met organisaties als de MBO Raad, het ministerie van OCW en de Inspectie van het Onderwijs. Samen met Wellantcollege, ROC de Leijgraaf, het Horizon College en MBO Utrecht hebben ze onderzocht of het mogelijk is de onderwijsovereenkomst en de praktijkovereenkomst digitaal te ondertekenen, op een manier die aan alle eisen voldoet. De bevindingen van het project 'Proof of Concept digitaal ondertekenen mbo' zijn verwerkt in deze publicatie. Mbo-instellingen kunnen hier gebruik van maken; uiteraard heeft elke school zijn eigen verantwoordelijkheid voor de manier waarop digitaal ondertekenen wordt ingericht.

Leeswijzer

Hoofdstuk 1 schetst de achtergrond van het project 'Proof of Concept digitaal ondertekenen mbo'. Daarbij wordt onder andere ingegaan op het ontwerp EduSign, een ontwerp voor een ondertekendienst in het onderwijs. Hoofdstuk 2 gaat over de aandachtspunten op het gebied van documentmanagement, informatiebeveiliging en privacy die een rol spelen bij digitaal ondertekenen. Hoofdstuk 3 laat zien welke organisaties betrokken zijn bij de digitale ondertekening van de onderwijsovereenkomst en de praktijkovereenkomst. Hoofdstuk 4 bevat een overzicht van de stappen die nodig zijn om te komen tot digitaal ondertekenen binnen het middelbaar beroepsonderwijs. Uiteraard varieert de exacte invulling per school. In hoofdstuk 5 is weergegeven hoe de digitale ondertekening in de praktijk werkt aan de hand van de ervaringen van een aantal mbo-instellingen.

Meer informatie

Wil je meer informatie over de mogelijkheden op het gebied van digitaal ondertekenen? Kijk dan op de website van saMBO-ICT, kn.nu/digitaalondertekenenmbo. Hier zijn alle links opgenomen naar de documenten en websites die worden genoemd in deze publicatie.



1 Achtergrond

Dit hoofdstuk schetst de achtergrond van het project 'Proof of Concept digitaal ondertekenen mbo'. Daarbij wordt onder andere ingegaan op EduSign, een ontwerp voor een ondertekendienst in het onderwijs.



Wat was de aanleiding voor het project?

Onderwijsinstellingen zoeken voortdurend naar mogelijkheden om het onderwijs en hun ondersteunende bedrijfsvoering te vernieuwen en verder te verbeteren, onder andere door gebruik te maken van ict-toepassingen. Om het uitwisselen van informatie tussen organisaties te faciliteren, is in 2011 het *Samenwerkingsplatform Informatie Onderwijs (SION)* van start gegaan. SION bestond uit de zes onderwijsraden (waaronder de MBO Raad) en hun uitvoeringsorganisaties (waaronder saMBO-ICT). Een van de activiteiten was de ontwikkeling van de *Referentie Onderwijs Sector Architectuur (ROSA)*. Hierin zijn afspraken vastgelegd over de gegevens die digitaal uitgewisseld kunnen worden tussen (onderwijs)organisaties. Het gaat daarbij om vragen als: wat betekent een gegeven, met wie kan het uitgewisseld worden en op welke wijze kan dit het best gebeuren?

Het rapport '*De juiste informatie als fundament voor goed onderwijs*' is uitgebracht ter afsluiting van SION en doet verslag van de opbrengsten. In het rapport wordt onder





andere ingegaan op de mogelijkheid om de onderwijsovereenkomst en de praktijkovereenkomst digitaal te ondertekenen.

Een van de doelen van het SION-programma was om te bekijken hoe de administratieve lasten in het onderwijs kunnen worden teruggedrongen. Administratieve lasten komen onder meer voort uit de processen rondom overeenkomsten tussen onderwijsinstellingen en onderwijsvolgers. Alleen al in het middelbaar beroepsonderwijs worden op jaarbasis ongeveer 1,1 miljoen documenten ondertekend in het kader van de inschrijving (de onderwijsovereenkomst) en het praktijkdeel van de opleiding (de praktijkovereenkomst). Digitaal ondertekenen levert een forse besparing op; zo is er sprake van minder kosten voor papier, printen, verzenden en scannen. Daarnaast is er minder menscapaciteit nodig dan bij handmatige verwerking. Kennisnet en saMBO-ICT hebben op basis van de situatie bij pilotinstellingen geschat dat voor een roc van gemiddelde omvang de besparing uitkomt op drie tot zes euro per document, afhankelijk van de werkwijze en de gerealiseerde digitalisering van de instelling.

Wellantcollege, ROC de Leijgraaf, Horizon College en MBO Utrecht hebben in het

project 'Proof of Concept digitaal ondertekenen mbo' onderzocht of het mogelijk is de overeenkomsten digitaal te ondertekenen, op een manier die aan alle eisen voldoet. Daarbij is onder andere bekeken hoe het zit met de juridische erkenning van de digitale handtekening en met accountantscontroles. De traditionele controle voor de jaarrekening is vooral gericht op cijfers en op de processen en procedures die een rol spelen bij de totstandkoming daarvan. Naarmate een organisatie verder digitaliseert, zullen de accenten van de accountantscontroles veel meer liggen op informatievoorziening, systemen, privacy en beveiliging.

Substantieel onderdeel van dit onderzoek was een 'Proof of Concept' (PoC). Hierbij is gebruikgemaakt van het ontwerp voor een ondertekendienst in het onderwijs: [EduSign](#).

Wat is EduSign?

EduSign is een ontwerp voor de ondertekening van de onderwijsovereenkomst en de praktijkovereenkomst in het middelbaar beroeps-onderwijs. Daarnaast kan het ontwerp in de Referentie Onderwijs Sector Architectuur worden gebruikt als generieke bouwsteen, bruikbaar voor het ondertekenen van allerlei

documenten in diverse processen binnen verschillende sectoren.

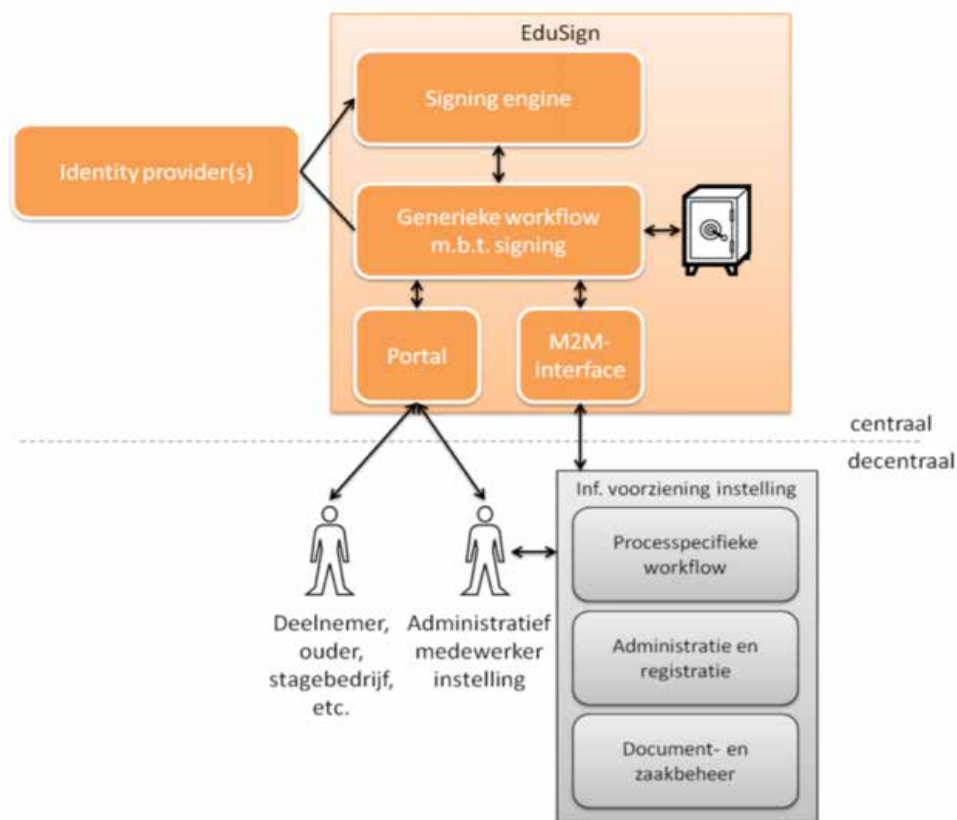
Bij het ondertekenen van de onderwijs-overeenkomst is de procedure is als volgt:

1. Een deelnemer meldt zich aan.
2. De deelnemer wordt uitgenodigd voor een intake en wordt vervolgens geplaatst.
3. De deelnemersadministratie maakt de onderwijsovereenkomst aan en stuurt een pdf plus e-mailadres van de deelnemer naar de dienstverlener.
4. De deelnemer ondertekent de onderwijs-overeenkomst door middel van DigiD.
5. De dienstverlener stuurt de ondertekende onderwijsovereenkomst terug naar de mbo-instelling.

Op basis van deze procedure is een ontwerp gemaakt voor een ondertekenservice, EduSign. De service moet de volgende gebruiksscenario's ondersteunen:

- aanbieden van het te ondertekenen document
- verzamelen van handtekeningen;
- verspreiden van het ondertekende document
- melden van de afsluiting van de workflow met teruglevering van het ondertekende document





Figuur 1: ontwerp EduSign

- inzien van de status
- controleren van en ingrijpen in de workflow
- beheren van de omgeving
- beheren van accounts

Op basis van een analyse van wetgeving is bepaald dat een generieke ondertekenservice voor de onderwijsovereenkomst en de praktijkovereenkomst moet voldoen aan de volgende eisen:

- Ondersteunt ondertekening door individuen en organisaties.
- Biedt de mogelijkheid documenten te ondertekenen met een geavanceerde elektronische handtekening. Dat is een handtekening die op unieke wijze aan de ondertekenaar verbonden is, zodat deze ondertekenaar kan worden geïdentificeerd. Belangrijk is dat elke wijziging van gegevens achteraf kan worden opgespoord.
- Functioneert op STORK-betrouwbaarheidsniveau 3 of vergelijkbaar. Kennisnet en saMBO-ICT hebben een *toolkit* ontwikkeld die mbo-instellingen ondersteunt bij informatiebeveiliging en privacy (IBP). Gerelateerd aan de aanpak vanuit deze toolkit komt STORK-niveau 3 overeen met de classificatie 'midden' (twee-factor authenticatie, oftewel authenticatie in twee stappen). In de Europese regelgeving wordt dit ook wel het niveau 'substantieel' genoemd.
- Waarborgt de 'schriftelijkheid' van een aangegane overeenkomst. Dat houdt in dat alle betrokken partijen de overeenkomst kunnen raadplegen en dat de authenticiteit van de overeenkomst is gewaarborgd. Verder is belangrijk dat het moment waarop





Vertrouwelijkheid

Met het oog op het realiseren van lastenverlichting, betere dienstverlening en een efficiëntere overheid zet de overheid in op grootschalige elektronische dienstverlening aan burgers en bedrijven. Dat stelt eisen aan authenticatie. Het Forum Standaardisatie heeft een kader ontwikkeld voor de inschaling van diensten op verschillende betrouwbaarheidsniveaus. Dit kader is gebaseerd op de nationaal geldende (wettelijke) regels en sluit aan op het Europese STORK-kader voor grensoverschrijdend gebruik van e-diensten. STORK staat voor Secure idenTity acrOss boRders linKed. Er zijn vier niveaus, oplopend van niveau 1 (waarbij er weinig zekerheid over de identiteit van degene die ondertekent nodig is) tot niveau 4 (waarbij tenminste eenmalig fysiek verschijnen van de gebruiker in het registratieproces vereist is).

de overeenkomst tot stand is gekomen en de identiteit van de partijen met voldoende zekerheid kunnen worden vastgesteld.

Bij het ontwerpen van een ondertekenservice voor de onderwijsovereenkomst en de praktijkovereenkomst is uitgegaan van een aantal bouwblokken. Deze verzorgen de interactie met EduSign, de tijdelijke opslag van het te ondertekenen document, de uitvoering van de workflow rondom het verzamelen van de benodigde handtekeningen en de daadwerkelijke ondertekening. Voor het vaststellen van de identiteit van de ondertekenaars maakt EduSign gebruik van externe identity providers. Daarnaast kan het ondertekenenproces worden ondersteund door informatiesystemen, zoals het Student Informatie Systeem (SIS) en andere systemen die zorgdragen voor zaken als administratie, registratie en documentbeheer.

Met welk product is de PoC uitgevoerd?

De projectgroep heeft verkend welke producten er op de markt beschikbaar zijn op het gebied van digitale ondertekening. Via een offertetraject is het product Signhost van Evidos geselecteerd. Er zijn twee manieren waarop Signhost kan worden gebruikt: als online dienst of door middel van een koppeling met het Student Informatie Systeem in de vorm van een application programming

interface (API). Inmiddels hebben Fringe Company (leverancier van onder andere de producten education online en Traject-planner) en Educus (leverancier van onder andere EduArte) voor hun administratiesystemen deze koppeling al gerealiseerd. Meer hierover lees je in hoofdstuk 5, waarin mbo-instellingen aan het woord komen over hun ervaringen. Uiteraard zijn er ook andere partijen op de markt met producten op het gebied van digitale ondertekening. Het is belangrijk dat mbo-instellingen goed onderzoeken wat de consequenties zijn van een keuze voor een oplossing.



2 Aandachtspunten bij digitaal ondertekenen

Dit hoofdstuk gaat over de aandachtspunten op het gebied van documentmanagement, informatiebeveiliging en privacy die een rol spelen bij digitaal ondertekenen.

Wat zijn aandachtspunten op het gebied van documentmanagement?

Het opslaan, beheren en volgen van documenten wordt documentmanagement genoemd. Kennisnet en saMBO-ICT zeggen hierover in de publicatie *'Hoe? Zo! Documentmanagement in het mbo'*: "In een mbo-school ontstaan allerlei documenten, uiteenlopend

van onderwijsovereenkomsten en diploma's tot jaarplannen, begrotingen en werkstukken van studenten. Je wilt deze documenten terug kunnen vinden als dat nodig is, je wilt ze kunnen delen met anderen of er samen met anderen aan werken, je wilt documenten voor langere tijd archiveren omdat je daar wettelijk toe verplicht bent of vernietigen omdat ze niet meer nodig zijn." In de

publicatie komen verschillende stappen aan de orde die van belang zijn bij het documentmanagement van digitaal ondertekende onderwijsovereenkomsten en praktijkovereenkomsten:

1. Breng de huidige situatie in kaart, bijvoorbeeld aan de hand van een Document Structuurplan (DSP). Geef daarbij aan welke eisen er aan het beheer van de documenten worden gesteld; zo geldt voor de onderwijsovereenkomst dat deze zeven jaar na uitschrijving moet worden vernietigd.
2. Bepaal hoe de gewenste situatie eruit ziet. Deze is afhankelijk van wat je wilt bereiken met documentmanagement. Op verschillende typen documenten zijn verschillende eisen en wensen van toepassing. In deze stap wordt bepaald welke oplossingen nodig zijn om aan de wettelijke eisen te voldoen en de wensen te realiseren.
3. Maak een realistische roadmap om daar te komen. Het maken van een roadmap begint met het identificeren van concrete verbeterstappen. Deze verbeterstappen hebben bij voorkeur de vorm van een projectvoorstel, waarin doel en resultaat



Figuur 2: schematisch overzicht documentmanagement





duidelijk is. Hierin moet ook duidelijk zijn welke knelpunten worden opgelost en welk deel van de gewenste situatie wordt gerealiseerd.

4. Voer de verbeterstappen uit.

Wat zijn aandachtspunten op het gebied van informatiebeveiliging?

Het is voor alle organisaties van groot belang dat zij op correcte en respectvolle wijze omgaan met de informatie die zij verzamelen, beheren en gebruiken. De wet- en regelgeving op dit gebied is in januari 2016 aangescherpt met de [meldplicht datalekken](#). Deze houdt in dat organisaties direct een melding moeten doen bij de Autoriteit Persoonsgegevens zodra zij een ernstig datalek hebben. Op Europees niveau zijn nieuwe afspraken vastgelegd in de [Algemene Verordening Gegevensbescherming](#) die per 25 mei 2018 van toepassing is, ook op scholen. Het is belangrijk dat scholen bepalen wat de gevolgen voor hen zijn en welke maatregelen ze moeten treffen.

Kennisnet en saMBO-ICT hebben een [toolkit](#) ontwikkeld die mbo-instellingen ondersteunt bij informatiebeveiliging en privacy (IBP). Deze toolkit, het framework IBP in het mbo, bevat allerlei hulpmiddelen voor diverse doel-

groepen binnen instellingen. Zo is er voor bestuurders een verantwoordingsdocument over IBP in het mbo. Voor de medewerkers die zich bezighouden met informatiebeveiliging en privacy bevat de toolbox veel direct inzetbaar materiaal. Zo maken de toetsingskaders duidelijk welke maatregelen een school moet nemen om optimaal beveiligd te zijn en om de privacy te waarborgen. Het gaat daarbij onder andere om veiligheidsaspecten rond digitaal ondertekenen. De kaders zijn gebaseerd op internationale normen en op de nieuwe Europese wetgeving. Ook bevat de toolbox verschillende modellen, onder meer voor het maken van IBP-beleidsplannen, het sluiten van bewerkersovereenkomsten met leveranciers en het maken van een privacyreglement. Onderdeel van het framework IBP in het mbo is het Toetsingskader Digitaal Ondertekenen. Dit speelt een cruciale rol bij de totstandkoming van digitaal ondertekenen. ROC de Leijgraaf heeft hier ervaring mee opgedaan; in hoofdstuk 5 staat een interview met Eustaach van Lent (manager Informatievoorziening en Cursistenadministratie) over de ervaringen, knelpunten en tips.

Kennisnet en saMBO-ICT hebben niet alleen een toolkit ontwikkeld, maar hebben ook de publicatie [‘Hoe? Zo! Informatiebeveiligings-](#)

[beleid in het mbo’](#) uitgegeven. Hierin gaan ze in op de problemen die kunnen spelen als data die niet op orde zijn of die niet goed beschermd zijn. Als data niet juist zijn, kunnen deelnemers niet voor bekostiging in aanmerking komen. Ook kan de school claims of boetes opgelegd krijgen.

Kennisnet en saMBO-ICT hebben samen met SURF bekeken welke principes en kaders uit de ‘International Standard ISO/IEC 27001’ een rol spelen binnen het onderwijs. Van de principes en kaders zijn normen afgeleid. Of en hoe de school deze normen toepast, wordt getoetst door middel van een assessment of audit. SURF, Kennisnet en saMBO-ICT hebben gezorgd voor checklists, handleidingen, sjablonen en toetsingskaders. Zo is er een [Handboek mbo-audits en een ‘roadmap’](#) op het gebied van informatiebeveiligings- en privacy-beleid in het mbo.

Wat zijn aandachtspunten op het gebied van privacy?

In 2015 gaven Kennisnet en saMBO-ICT de publicatie [‘Hoe? Zo! Privacy in het mbo’](#) uit. Bij privacy gaat het om het respecteren en beschermen van het privéleven van studenten en medewerkers; scholen moeten op





een zorgvuldige manier omgaan met de persoonsgegevens van en over studenten en medewerkers. Dat was altijd al aan de orde, maar door de digitalisering van de maatschappij en daarmee ook van het onderwijs vraagt dit onderwerp steeds meer aandacht. Als scholen geen rekening houden met privacyaspecten, kan dat negatieve gevolgen hebben. Zo kan de Autoriteit Persoonsgegevens een boete opleggen wegens het niet voldoen aan de wetgeving.

Ook bij digitaal inschrijven en ondertekenen speelt privacy een rol. De mbo-instelling is verplicht het burgerservicenummer te gebruiken en mag dit nummer opvragen bij de student. Op basis van dit nummer (en andere gegevens) kan de school de student inschrijven. Persoonsgegevens kunnen alleen worden verwerkt op basis van een rechtmatig (wettelijk bepaald) doel. In het geval van een mbo-opleiding van een student is er sprake van de uitvoering van een overeenkomst. De school informeert de betrokkenen over welke persoonsgegevens worden verzameld, wat hiermee gebeurt en welke rechten en plichten gelden. Zorgvuldig omgaan met persoonsgegevens is belangrijk. Deze gegevens moeten zijn beschermd en er moeten maatregelen zijn genomen tegen

verlies en onbevoegde toegang. Hierbij gelden algemeen geaccepteerde organisatorische en technische beveiligingsnormen (zoals ISO-normen).

De school moet zowel in beleid als in uitvoering de privacy van studenten waarborgen, zeker wanneer de school overstapt op digitaal ondertekenen. Met de leveranciers van ondersteunende software wordt een bewerkersovereenkomst afgesloten waarin afspraken staan over privacy. Privacy is de (eind)verantwoordelijkheid van het college van bestuur; dat zal een aantal taken delegeren. De verantwoordelijkheid voor privacy kan op een aantal manieren worden geregeld. Bijvoorbeeld bij een afdeling control, juridische zaken, personeel & organisatie of kwaliteitszorg. Ook moet de instelling een functionaris gegevensbescherming onder het college van bestuur benoemen.

Hoe zit het met cloud computing?

In het onderwijs wordt vaak gebruikgemaakt van cloud computing. Er zijn bijvoorbeeld online faciliteiten voor de elektronische leeromgeving, de studentenadministratie, de financiële administratie en (digitaal) samenwerken. Het grote voordeel van cloud

computing is dat de school zelf geen servers meer nodig heeft en geen software hoeft aan te schaffen en te onderhouden. Ook kunnen cloudleveranciers beveiligingsmiddelen snel en dynamisch inzetten en beschikken ze vaak over diep inhoudelijke beveiligingskennis. Tegelijkertijd brengen clouddiensten specifieke risico's met zich mee; zo kan een cloudleverancier gebruikmaken van diensten van derden waarmee de klant geen afspraken heeft gemaakt op het gebied van beveiliging. Daarom is het van belang om afspraken over privacy vast te leggen in een bewerkersovereenkomst. Het is niet voldoende om alleen te kijken naar de kwaliteit en de maatregelen van de provider. Ook de school moet beveiliging goed organiseren en uitvoeren. Verder is het belangrijk dat medewerkers weten wat van hen verwacht wordt op het gebied van de beveiliging van overeenkomsten.

Welke juridische aspecten spelen een rol bij digitaal ondertekenen?

Kennisnet en de MBO Raad hebben zich verdiept in de eisen van digitale ondertekening. Dit zijn de belangrijkste bevindingen:

- Overeenkomsten, waaronder onderwijs-overeenkomsten, zijn in principe vormvrij.





Dit betekent dat ze niet alleen schriftelijk, maar ook mondeling of via internet kunnen worden gesloten. Ook digitale ondertekening is toegestaan. Een digitale handtekening heeft dezelfde juridische status als een handgeschreven handtekening, mits de digitale handtekening voldoende betrouwbaar is voor het doel waarvoor de ondertekening wordt gebruikt (Burgerlijk Wetboek artikel 3:15A).

- De documenten met digitale handtekening worden door de instellingen opgesteld en ondertekend met een 'gewone elektronische handtekening' zoals gedefinieerd in de Europese richtlijn 1999/93/EG. Deze handtekening bestaat uit elektronische gegevens, die vastgehecht zijn aan – of logisch geassocieerd zijn met – andere elektronische gegevens. Deze worden gebruikt als middel voor authenticatie. Een voorbeeld hiervan is een ingescande handtekening.
- Bij studenten die de onderwijsovereenkomst en de praktijkovereenkomst ondertekenen, is een systeem met twee-factor-authenticatie (authenticatie in twee stappen) vereist.
- Authenticiteit en identiteit van partijen moeten worden geborgd in de administratieve organisatie van de school.
- Omdat van ouders/wettelijke vertegenwoordigers en medewerkers van leer-

Juridisch normenkader

SURF heeft een **juridisch normenkader** voor cloudservices opgesteld. Dit is gericht op het hoger onderwijs, maar biedt ook veel handvatten voor het middelbaar beroepsonderwijs. In het kader wordt aandacht besteed aan zeggenschap, vertrouwelijkheid en privacy van gegevens die worden opgeslagen in de cloud. Aan het document is een model bewerkersovereenkomst toegevoegd, waarin de privacybepalingen uit het kader zijn opgenomen.

bedrijven het burgerservicenummer niet in de administratie mag worden opgeslagen kunnen zij geen gebruik maken van DigiD voor de ondertekening van respectievelijk de onderwijsovereenkomst en de praktijkovereenkomst. Voor de authenticatie wordt gebruikgemaakt van een e-mail in combinatie met een tweede middel, zoals een sms of 'krabbel' op een touchscreen. De bijbehorende gegevens (zoals een e-mailadres en een mobiel nummer) moeten geborgd zijn in de beheeradministratie.



3 Speelveld

Dit hoofdstuk laat zien welke organisaties betrokken zijn bij de digitale ondertekening van de onderwijsovereenkomst en de praktijkovereenkomst. Daarbij gaat het niet alleen om organisaties als de MBO Raad, het ministerie van OCW en de Onderwijsinspectie, maar ook om Logius, de dienst digitale overheid die verantwoordelijk is voor DigiD. Belangrijk bij digitaal ondertekenen is dat de ondertekenaars kunnen worden geïdentificeerd. Verder moet kunnen worden vastgesteld (geauthenticeerd) dat die en alleen die persoon de ondertekening uitvoert. Hiervoor zijn veel uiteenlopende middelen en methoden beschikbaar. Afhankelijk van het betrouwbaarheidsniveau van het document dient die authenticatie strenger te zijn. DigiD is een veilig en betrouwbaar authenticatiemiddel.

Op welke manier is de MBO Raad betrokken?

De MBO Raad heeft een [Servicedocument Onderwijsovereenkomst](#) en een [Servicedocument Praktijkovereenkomst](#) ontwikkeld. De versies van 2017-2018 zijn aangevuld met informatie over de digitale ondertekening. In deze versies staat: "Steeds vaker worden documenten digitaal ondertekend. Een digitale handtekening heeft dezelfde juridische status als een handgeschreven handtekening, mits de digitale handtekening voldoende betrouwbaar is voor het doel waarvoor de ondertekening wordt gebruikt (Burgerlijk Wetboek





artikel 3:15A). Voor het ondertekenen van de overeenkomsten zijn er geen nadere vormvereisten beschreven. Dat betekent dat het is toegestaan de overeenkomsten – in plaats van met een handgeschreven handtekening – ook digitaal of elektronisch te ondertekenen. Er zijn verschillende vormen van digitaal ondertekenen. Een eenvoudige variant is de gescande handtekening. Een elektronische handtekening is geavanceerder en bestaat uit elektronische gegevens die onlosmakelijk verbonden zijn aan een digitaal document. Hiermee kan de identiteit van de ondertekenaars worden vastgesteld. Voor de mbo-sector is een methode voor elektronische ondertekening ontwikkeld die voldoende betrouwbaar is en past binnen de wettelijke onderwijskaders.”

De Servicedocumenten zijn afgestemd met het ministerie van OCW. René Loep (MT-lid mbo bij het ministerie): “Digitalisering van het ondertekenen van onderwijs- en praktijkovereenkomsten biedt instellingen de kans om mee te gaan met de tijd en processen te vergemakkelijken, ook voor de student. Uiteraard wel met voldoende waarborgen ten aanzien van privacy en veiligheid.”



Hoe kijkt de Onderwijsinspectie naar de digitale ondertekening?

De onderwijswetgeving vereist slechts dat partijen een rechtsgeldige praktijkovereenkomst en onderwijsovereenkomst sluiten. De eisen aan en consequenties van digitale ondertekening worden geregeld door het privaatrecht. Controle van de ondertekening van de onderwijsovereenkomst en de praktijkovereenkomst laat de inspectie normaal gesproken over aan de instellings-

accountant. Als er twijfels of signalen zijn, wordt er nader onderzoek gedaan.

Op welke manier is de accountantsdienst van de instelling betrokken?

De instellingsaccountant toetst bij de reguliere jaarcontrole of de onderwijs- en praktijkovereenkomsten op de juiste wijze zijn ondertekend. De voorziening voor digitaal ondertekenen wordt aan dezelfde eisen getoetst als andere digitale voorzieningen





voor de bedrijfsvoering van de school. Speciaal punt van aandacht is de overlap tussen de reguliere jaarcontrole door de instellingsaccountant en het DigiD-assessment. Scholen die gebruikmaken van DigiD, moeten hun systemen en procedures via een initieel assessment en daarna jaarlijks laten toetsen. In het rapport '[Aanpak DigiD-assessment digitaal ondertekenen](#)' zijn de impact en mogelijke kansen van deze overlap beschreven. Meer informatie hierover staat verderop in dit hoofdstuk.

Op welke manier zijn ouders / wettelijke vertegenwoordigers betrokken?

Bij studenten die jonger zijn dan 18 jaar, moet de onderwijsovereenkomst worden meeondertekend door de ouders. De ouderhandtekening op de POK is formeel niet meer nodig, mits de ouders daarmee via ondertekening van de onderwijs-overeenkomst hebben ingestemd. Om de ouder met DigiD te laten ondertekenen, heeft de school het burgerservicenummer van de ouder nodig. Scholen mogen echter het burgerservicenummer van ouders niet gebruiken of registreren. Voor de authenticatie wordt gebruikgemaakt van een e-mail

in combinatie met een tweede factor (zoals een sms of 'krabbel' op een touchscreen). Daarbij moet worden aangemerkt dat ouders niet kunnen worden verplicht:

- over een e-mailadres en mobiel nummer te beschikken;
- deze informatie beschikbaar te stellen en eventuele wijzigingen door te geven;
- bereid te zijn om digitaal bereikbaar te zijn voor deze doeleinden.

Als ouders hun gegevens niet (willen) doorgeven, moeten zij fysiek een handtekening zetten op de overeenkomst.

Op welke manier zijn leerbedrijven betrokken?

De praktijkovereenkomst moet worden ondertekend door de tekenbevoegde van een leerbedrijf. Voor deze ondertekening kan gebruik worden gemaakt van een e-mail in combinatie met een tweede factor (zoals een sms of 'krabbel' op een touchscreen). Aandachtspunt is nog wel dat de digitale overeenkomst naar één mailadres wordt verstuurd. Dat vereist dat het bestand met mailadressen van tekenbevoegde medewerkers van leerbedrijven actueel is.

Wat is de rol van Logius?

Voor het authenticeren met DigiD wordt gebruikgemaakt van de onafhankelijke partij Logius, de dienst digitale overheid die verantwoordelijk is voor DigiD. Instellingen die gebruikmaken van DigiD als authenticatiemiddel, moeten hun systemen en procedures laten toetsen via een initieel assessment en een jaarlijks assessment.

Meer informatie over het assessment staat op de website van [Logius](#).

De projectgroep 'Proof of Concept digitaal ondertekenen mbo' heeft onderzoek laten doen naar de impact van het assessment voor de mbo-instelling. Daarbij is gekeken wie verantwoordelijk is voor het voldoen aan een norm: de leverancier of de school. Daarnaast is een analyse uitgevoerd om te bepalen waar de overlap zit tussen de reguliere jaarcontrole door de instellingsaccountant en het DigiD-assessment. Het rapport '[Aanpak DigiD-assessment digitaal ondertekenen mbo](#)' is raadpleegbaar via de website van [saMBO-ICT](#). In het rapport is een gedetailleerd werkblad opgenomen van werkzaamheden die de school moet uitvoeren.





Wie is verantwoordelijk voor het voldoen aan een norm?

In het kader van het programma 'IBP in het mbo' is een Toetsingskader Digitaal Ondertekenen ontwikkeld. Hierin staat aan welke normen een school moet voldoen in het kader van DigiD:

kader Digitaal Ondertekenen; dit is document IBPDO9 van het *framework IBP in het mbo*.

Op welke manier is SURFmarket betrokken?

SURFmarket levert licenties, ondersteuning en diensten aan aangesloten onderwijs-

onderwijsinstellingen meer zekerheid. Ook kan in het geval van omvangrijke contracten het doen van een aanbesteding worden voorkomen door in te kopen via SURFmarket (inbesteding). Ondersteuning wordt met name geleverd door het onderhandelen/aanbesteden en beschikbaar stellen van bemiddelingsovereenkomsten die met leveranciers zijn gesloten op basis van het *Juridisch Normenkader Cloudservices Hoger Onderwijs*.

B0-5	Alle wijzigingen worden altijd eerst getest voordat deze in productie worden genomen en worden via wijzigingsbeheer doorgevoerd.
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.
B2-1	Maak gebruik van veilige beheermechanismen.
B5-3	Sla gevoelige gegevens versleuteld of gehashed op.
B7-9	Governance, organisatie, rollen en bevoegdheden inzake preventie, detectie en response inzake informatiebeveiliging dienen adequaat te zijn vastgesteld.

Tabel 1: Normen verantwoordelijkheid instellingen

Voor een aantal andere normen is de serviceprovider verantwoordelijk. Deze moet in een 'Third Party Memorandum' (TPM) aangeven dat hij voldoet aan deze normen. Voor het totaaloverzicht van normen zie het Toetsings-

instellingen. Het voordeel is dat licenties voordeliger te verkrijgen zijn. Daarnaast moeten leveranciers zich door het afsluiten van een bemiddelingsovereenkomst kwalificeren als betrouwbare partner; dit geeft



4 Stappenplan



Kennisnet en saMBO-ICT hebben een overzicht gemaakt van de stappen die worden doorlopen bij de implementatie van digitaal ondertekenen binnen het middelbaar beroepsonderwijs. Uiteraard kan de exacte invulling variëren.

Stap 0 Businesscase

Het maken van een businesscase helpt bij het beantwoorden van de vraag of de digitale ondertekening van de onderwijs-overeenkomsten en de praktijk-overeenkomsten voordelig is voor de mbo-instelling. Het is daarom aan te bevelen deze vooraf op te stellen. De businesscase zal per school verschillen. Dat komt onder andere doordat de kosten voor het gebruik van de ondertekendienst afhankelijk zijn van het soort contract. Verder verschillen de kosten van het DigiD-assessment per auditor.

Wat de verschillen ook zijn, de overeenkomst is dat digitaal ondertekenen een enorme besparing oplevert; zo is er sprake van minder kosten voor papier, printen, verzenden en scannen. Maar vooral is er minder menscapaciteit nodig dan bij handmatige verwerking. Kennisnet en saMBO-ICT hebben op basis van de situatie bij pilotinstellingen geschat dat de besparing bij een roc van gemiddelde omvang tussen de drie en zes euro per document is, afhankelijk van de werkwijze en de al





gerealiseerde digitalisering van de instelling. Anderzijds zijn er kosten gemoeid met digitaal ondertekenen. Zo betaal je licentiekosten voor het gebruik van een ondertekendienst. Ook kost het uitvoeren van een DigiD-assessment geld; in het rapport 'Aanpak DigiD-assessment digitaal ondertekenen mbo' wordt uitgegaan van 3.000 tot 5.000 euro (exclusief btw) per assessment.

Stap 1 Voorbereiding

Stap 1.1: Bepaal het 'digitale applicatielandschap'. Dat is de context waarbinnen digitale ondertekening moet gaan plaatsvinden. Het gaat hierbij niet alleen om de plek waar de handtekeningen worden gezet, maar ook om het archief waarin de overeenkomsten worden opgeslagen.

Stap 1.2: Van belang is dat de processen binnen de school en de beschrijving van de Administratieve Organisatie en Interne Controle (AO/IC) worden aangepast op digitaal ondertekenen. Zo moeten de e-mailadressen en mobiele nummers van ouders / wettelijke vertegenwoordigers en van tekenbevoegden binnen leerbedrijven op een goede manier worden beheerd.

Stap 1.3: Bepaal welke medewerkers verantwoordelijk zijn voor procesoverstijgende aspecten, bijvoorbeeld op het gebied van informatiebeveiliging en privacy. Werk hier in het vervolg van het traject nauw mee samen. Op de website van [saMBO-ICT](#) staan documenten die deze functionarissen kunnen ondersteunen.

Stap 1.4: Bepaal welke administratieve medewerkers verantwoordelijk worden voor de digitale ondertekening en zorg ervoor dat ze voorbereid zijn op wat hen te wachten staat. De afwezigheid van fysieke papieren documenten vereist een andere inrichting en organisatie van processen en werkwijzen. Wellicht moeten de medewerkers worden opgeleid om geautomatiseerde informatiesystemen effectief en efficiënt te kunnen gebruiken. Ook moeten ze zich bewust worden van de consequenties van digitaal werken. Onder andere vanuit wet- en regelgeving zijn er eisen aan informatiebeveiliging, toegangscontrole en privacy. Waar voorheen papieren documenten fysiek op het bureau lagen en via de reguliere postvoorziening werden gedistribueerd, moeten nu informatiesystemen en digitale informatiedistributie worden beveiligd.

Stap 1.5: Zorg voor een overheidsidentificatienummer (OIN). Dat is het identificatienummer voor niet-natuurlijke personen ten behoeve van het digitale berichtenverkeer met de overheid. Meer informatie hierover staat op [logius.nl](#) (navigeer naar het kopje ondersteuning).

Stap 1.6: Zorg voor PKI-certificaten. PKI staat voor Public Key Infrastructure en is de internationale standaard voor beveiligen van gegevens en berichten. Als een overheidsorganisatie of bedrijf gebruik wil maken van een digitale dienst van een (andere) overheidsorganisatie, moet worden vastgesteld of dat is toegestaan. De organisatie die de dienst aanbiedt, moet eerst identificeren welke organisatie de dienst wil afnemen, voordat zij kan vaststellen of de organisatie en/of het bedrijf geautoriseerd mag worden. Op [sambo-ict.nl](#) staat een link waarin wordt uitgelegd hoe je deze certificaten aanvraagt. Let op: het aanvragen van een certificaat kan enkele weken doorlooptijd vergen. Het aanvragen van een PKI-certificaat kan worden gedaan via een Certification Service provider (CSP). Een instelling kan zelf een CSP kiezen. Op [logius.nl](#) is een actueel overzicht te vinden.



De CSP naar keuze levert alle benodigde ondersteuning voor het certificaat; van aanvraagproces, sleutelgeneratie tot aan installatie. De kosten bedragen indicatief € 500,- voor een certificaat dat drie jaar geldig is en eenmalig tussen de € 100,- en € 200,- voor administratiekosten.

Stap 1.7: Sluit een contract met een leverancier die producten of diensten voor het digitaal ondertekenen levert die de gevraagde functionaliteit levert en die aantoonbaar aan alle wettelijke vereisten voldoet. Zorg voor een Third Party Memorandum (TPM) en voor een actuele bewerkersovereenkomst. De mbo-sector kan gebruikmaken van de diensten van SURF-market in dezen.

Stap 1.8: Maak een keuze voor de manier waarop de ondertekendienst wordt gebruikt. Bij Signhost bijvoorbeeld zijn er twee mogelijkheden: gebruikmaken van de online dienst Ondertekenen.nl of een koppeling van het studentadministratiepakket aan de ondertekendienst door middel van een application programming interface (API). Hiertoe dient dus ook het studentadministratiepakket te worden aangepast en de functionaliteit mogelijk nog moet worden 'aangezet'. Voor deze functionali-



teit in het studentadministratiepakket zijn mogelijk extra licentiekosten verschuldigd.

Stap 2 Aansluiting op DigiD

Stap 2.1: Aanvragen aansluiting op pre-productieomgeving Logius. Op logius.nl staat een aanvraagformulier waarmee je toegang krijgt tot de preproductieomgeving van DigiD. Deze omgeving is bedoeld om de koppeling van de ondertekenservice met DigiD te testen. Als de koppeling goed

functioneert, wordt de aansluiting goedgekeurd door Logius.

Stap 2.2: Aanvragen aansluiting op productieomgeving Logius. Vervolgens vul je een aanvraagformulier in voor de productieomgeving van DigiD. Het is verplicht om binnen twee maanden na aansluiting op de productieomgeving een DigiD-assessment uit te voeren en erover te rapporteren aan Logius. Hierbij spelen vier stappen een rol:





Stap 2.2.1: Uitvoeren proefaudit (aanbevelen!) In deze stap toetst de school zelf de inrichting, processen en procedures aan de hand van beveiligingsrichtlijnen. Ook wordt een proefaudit uitgevoerd.

- Bepalen scope en verdeling DigiD verantwoordelijkheid
Resultaat: inzicht in de verdeling van verantwoordelijkheden tussen de school en de IT-leveranciers. Inzicht in welke normen door de instelling zelf worden ingevuld.
- Voorbereiding proefaudit
Resultaat: voor de interviews die deel uitmaken van de audit zijn de juiste personen bekend en te bestuderen documentatie is beschikbaar. Interviewpartners zijn voorbereid. De interviews zijn ingepland.
- 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.
- 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 de benodigde vervolgacties.

Stap 2.2.2: Maatregelen treffen

In deze stap pakt de school eventuele tekortkomingen aan. Nagegaan wordt welke maatregelen de hoogste prioriteit hebben en hoe snel en met welke diepgang de verbeteringen moeten worden doorgevoerd. Resultaat: verbeterde beveiligingsmaatregelen met inachtnaam van het ambitieniveau van de instelling.

Stap 2.2.3: Audit laten uitvoeren

In deze stap voert de auditor de DigiD-audit uit conform geldige auditprotocollen. De auditor moet een door de NOREA gecertificeerde Register EDP-auditor (RE) zijn. De auditor bestudeert de documentatie en houdt interviews. Hij 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-assessmentrapportage, bestaande uit:

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

Stap 2.2.4: Bevindingen naar Logius sturen
De instelling biedt het rapport van de auditor en het TPM-rapport van de IT-serviceorganisatie aan aan Logius.

Stap 3 Uitvoering

Als alle voorbereidende werkzaamheden zijn uitgevoerd en de aansluiting op DigiD is gerealiseerd, kunnen de onderwijsovereenkomst en de praktijkovereenkomst digitaal worden ondertekend. Dit gaat als volgt:



Stap 3.1: De instelling biedt bij de ondertekendienst een document aan, tegelijkertijd met de contactgegevens van de partijen die het document moeten ondertekenen.

Stap 3.2: De ondertekendienst certificeert de pdf, zodanig dat de inhoud van het document niet langer kan worden veranderd en er alleen nog digitale handtekeningen aan kunnen worden toegevoegd.

Stap 3.3: Alle partijen ontvangen een mail met een gepersonaliseerde link naar het document in de ondertekendienst. Deze partijen volgen de link en identificeren zich met een voldoende betrouwbaar middel bij de ondertekendienst.

Stap 3.4: De partijen krijgen de vraag zich akkoord te verklaren met de inhoud van het document. Na akkoord verbindt de ondertekendienst de identiteit van deze partij aan de pdf in de vorm van een geavanceerde elektronische handtekening. Hiertoe genereert de ondertekendienst voor deze partij een 'Digital ID', die alleen voor deze ene sessie gebruikt wordt. Bovendien plaatst de ondertekendienst de naam van de ondertekenaar en de datum van ondertekening zichtbaar op de pdf.

Stap 3.5: Zodra alle handtekeningen zijn gezet, wordt de pdf afgesloten. Hierdoor zijn de handtekeningvelden niet meer bewerkbaar. De pdf wordt per mail naar alle partijen verstuurd.

Stap 3.6: De door alle partijen ondertekende pdf wordt teruggezonden naar alle partijen die het hebben ondertekend.

Stap 3.7: Tot slot wordt een transactiebon aangemaakt waarop identificerende gegevens komen te staan, de tijdstippen van daadwerkelijke ondertekening en IP-nummers van de aansluiting die bij de ondertekening zijn gebruikt. Deze transactiebon dient voor de instelling primair als bewijslast in mogelijke conflicten. Het gaat om privacygevoelige informatie, dus moet de school daar dienovereenkomstig mee omgaan.





Stap 0: businesscase	Stap 1: voorbereiding	Stap 2: aansluiting op DigiD	Stap 3: uitvoering
	<p>1.1: bepaal het 'digitale applicatielandschap'</p> <p>1.2: pas de processen en de AO/IC aan op digitaal ondertekenen</p> <p>1.3: bepaal wie verantwoordelijk zijn voor procesoverstijgende aspecten</p> <p>1.4: bepaal wie verantwoordelijk zijn voor de digitale ondertekening en bereid hen voor</p> <p>1.5: zorg voor een overheids-identificatienummer</p> <p>1.6: zorg voor PKI-certificaten</p> <p>1.7: sluit een contract met een leverancier</p> <p>1.8: maak een keuze voor de manier waarop de ondertekendienst wordt gebruikt</p>	<p>2.1: vraag de aansluiting op de preproductieomgeving van Logius aan</p> <p>2.2: vraag de aansluiting op de productieomgeving van Logius aan</p> <p>2.2.1: voer een proefaudit uit</p> <p>2.2.2: pak tekortkomingen aan</p> <p>2.2.3: laat een audit uitvoeren</p> <p>2.2.4: stuur de bevindingen naar Logius</p>	<p>3.1: school biedt te ondertekenen document aan bij ondertekendienst</p> <p>3.2: ondertekendienst certificeert de pdf</p> <p>3.3: partijen ontvangen mail met gepersonaliseerde link naar document en identificeren zich</p> <p>3.4: partijen krijgen vraag zich akkoord te verklaren met inhoud document en ondertekenen</p> <p>3.5: zodra alle handtekeningen zijn gezet, wordt de pdf afgesloten</p> <p>3.6: partijen ontvangen ondertekende pdf</p> <p>3.7: transactiebon wordt aangemaakt en dient als bewijslast voor school</p>

Tabel 2: stappen implementatie digitaal ondertekenen



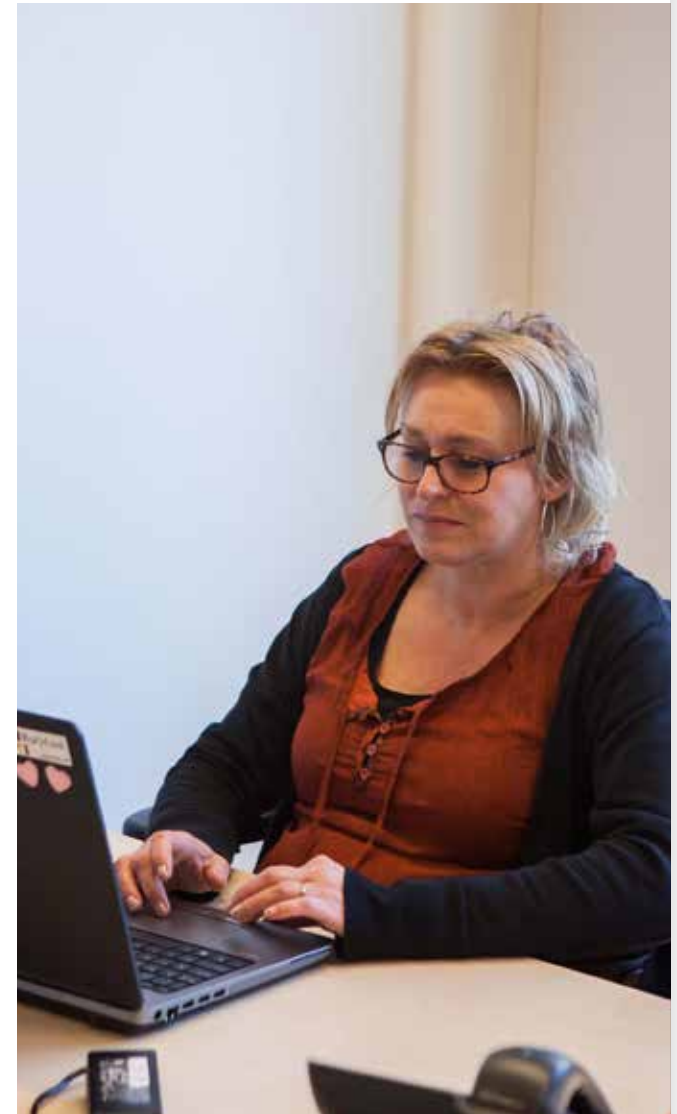
5 Digitaal ondertekenen in de praktijk

In dit hoofdstuk komen drie mbo-instellingen aan het woord die ervaringen hebben opgedaan met het digitaal ondertekenen van onderwijsovereenkomsten en praktijkovereenkomsten. Het gaat om mbo-instellingen die hebben meegedaan aan het project 'Proof of Concept digitaal ondertekenen mbo'. In het project is bekeken welke producten er op de markt beschikbaar zijn op het gebied van digitale ondertekening. Hieruit is het product Signhost van Evidos geselecteerd. Signhost kan als online dienst (Ondertekenen.nl) worden gebruikt, maar kan ook door middel van een API met het Student Informatie Systeem communiceren. Inmiddels hebben Fringe Company en Educus voor hun administratiesystemen deze koppelingen gerealiseerd. Voor een grotere gebruiksvriendelijkheid en efficiency heeft Wellantcollege een extra functionaliteit tussen Signhost en Trajectplanner laten bouwen, die inmiddels door Fringe Company breder beschikbaar is gesteld. Het Horizon College werkt met een koppeling tussen Signhost en EduArte.

Wat zijn de ervaringen van ROC de Leijgraaf?

ROC de Leijgraaf is in 2015 op zoek gegaan naar een ander leerlingvolgsysteem. Een voorwaarde daarbij was dat de primaire en secundaire processen zo op elkaar af zijn gestemd, dat gegevens slechts eenmaal

digitaal worden vastgelegd. In mei 2016 is gestart met de digitale ondertekening van de onderwijsovereenkomst door meerderjarige studenten, in april 2017 gevolgd door minderjarige studenten. Hiervoor wordt gebruik gemaakt van Ondertekenen.nl van Evidos. Eustaach van Lent, manager Informatievoorziening en Cursusadministratie:





Type	Transactiestatus	Ondertekenaar	Status	Gemaakt op	Overige Ondertekenaar(s)	Transactie
OOK 18+ Toelating	Nog niet verzonden			06-06-2017		
OOK 18+ Toelating	Kompleet			08-06-2017		
OOK 18+ Toelating	Onderhand			08-06-2017		
OOK 18+ Toelating	Onderhand			09-06-2017		
OOK 18+ Toelating	Wachtend op ondertekenaar			06-06-2017		
OOK 18+ Toelating	Wachtend op ondertekenaar			06-06-2017		
OOK 18+ Toelating	Wachtend op ondertekenaar			06-06-2017		
OOK 18+ Toelating	Wachtend op ondertekenaar			06-06-2017		
OOK 18+ Toelating	Wachtend op ondertekenaar			06-06-2017		
OOK 18+ Toelating	Wachtend op ondertekenaar			06-06-2017		
OOK 18+ Toelating	Kompleet			08-06-2017		
OOK 18+ Toelating	Kompleet			08-06-2017		

Figuur 3: screenshot overzicht digitaal te ondertekenen overeenkomsten

Inloggen bij Leijgraaf - Ondertekenen.nl

Verplichte velden *

Inlogmethode *

Ik wil inloggen met alleen gebruikersnaam en wachtwoord

Ik wil inloggen met een extra controle via sms

DigiD gebruikersnaam *

Wachtwoord *

U kunt tot 10:44 uur (Nederlandse tijd) inloggen. Daarna verloopt uw sessie.

[Annuleren](#)

[Wachtwoord vergeten?](#)

[Nog geen DigiD? Vraag uw DigiD aan](#)

Figuur 4: screenshot koppeling Ondertekenen.nl met DigiD

“Het mooie is dat de overeenkomst binnen een dag door een kwart van de studenten was ondertekend. Na een week was dat gedaan door 68% en na twee weken door 87% van de studenten. Dat percentage is hoger dan bij de ondertekening op papier. Eventuele vertraging zit in het (opnieuw) aanvragen van de DigiD. Problemen die we voorzien hadden, bleken er niet te zijn. Zo hebben studenten geen bezwaar tegen de ondertekening met DigiD en zien virusscanners en studenten de mail met de digitale versie van de overeenkomst niet als spam. Een tip is wel om in de begeleidende mail een telefoonnummer op te nemen, zodat studenten bij twijfels en vragen eenvoudig contact op kunnen nemen. Een andere tip is om de mail te laten versturen vanaf een mailadres van de instelling zelf en niet van bijvoorbeeld de ondertekenservice; die kennen studenten namelijk niet van naam. Verder is het handig om studenten en hun ouders tegelijk een mail te sturen over het te ondertekenen document; je krijgt er dan vanzelf gesprekken over bij mensen thuis, wat de betrokkenheid ten goede komt.”

In een overzicht wordt getoond of studenten de overeenkomst hebben geopend en ondertekend. Een reminder wordt automatisch verstuurd. Als alle betrokken partijen hebben ondertekend, krijgt de student automatisch een mail met het ondertekende document. Aandachtspunt is waar de documenten worden gearchiveerd. Eustaach van Lent: “Op dit moment slaan we alles zowel in het documentmanagementsysteem als in de kernregistratie deelnemers (KRD) op, maar we willen naar één systeem





toe. Over systemen gesproken: let erop dat de overeenkomsten in verband met privacy-wetgeving na een bepaalde periode moeten worden verwijderd uit de ondertekenapplicatie. ROC de Leijgraaf heeft een audit laten uitvoeren om te bekijken of de digitale overeenkomsten en alle processen daarmee voldoen aan alle vereisten. Een van de bevindingen was dat we nog geen informatiebeveiligingsplan hadden. Een ander punt was dat we ons wachtwoordbeleid moesten aanscherpen. De audit moet voor 1 juni zijn uitgevoerd, dus het is verstandig om in januari of februari al een afspraak te maken met de auditor; over het algemeen is dat de accountant.”

Eustaach van Lent is van mening dat mbo-instellingen kosten kunnen besparen als het gaat om de administratieve lasten. “Het overstappen op digitaal ondertekenen helpt daarbij. Het is een traject dat tijd nodig heeft, onder andere doordat je te maken hebt met een audit en doordat je certificaten moet inregelen. Wel kunnen scholen het traject voorbereiden, onder andere door contact op te nemen met de leverancier van het Student Informatie Systeem en te vragen naar de mogelijkheden van een koppeling met een ondertekenapplicatie. Ook kun je de deel-

nemersadministratie voorbereiden. De nieuwe manier van ondertekenen past binnen de digitalisering die al gaande is,

Jan Bartling, algemeen manager van saMBO-ICT, zegt dat de eerste resultaten veelbelovend zijn: een aanzienlijke lastenvermindering is het resultaat. “Bij bijvoorbeeld ROC de Leijgraaf merken men het gemak waarmee studenten zich aanpassen aan deze ‘nieuwe’ werkwijze. Binnen een week zijn vrijwel alle handtekeningen binnen, terwijl dit normaal weken duurt en er veel achteraan gezeten moet worden.”

Bron: ‘De juiste informatie als fundament voor goed onderwijs. De opbrengsten van SION’ (2016)

maar kent ook een aantal specifieke aandachtspunten. Het gaat eigenlijk om een soort verandermanagement; met de deelnemersadministratie willen we van administratieve taken naar een meer monitorende taak. Mijn advies aan andere mbo-instellingen is: zorg voor een goede voorbereiding op de digitale ondertekening van de onderwijs-

overeenkomst en de praktijkovereenkomst en zet door! Want de voordelen zijn evident: minder administratieve lasten, een veel snellere doorlooptijd van het ondertekenen van overeenkomsten en een besparing op papierkosten, verzendkosten en de kosten voor het scannen van de ondertekende documenten. Daarnaast is er sprake van een kwaliteitsaspect; het is lastiger om te sjoemelen met een digitale handtekening dan met een handtekening op papier.”

Wat zijn de ervaringen van Wellantcollege?

Wellantcollege biedt zowel vmbo- als mbo-opleidingen aan. Informatiemanager Bert van Daalen vindt het opvallend dat leerlingen in het vmbo geen overeenkomst hoeven te ondertekenen, maar studenten in het mbo wel. “Dat staat in de Wet Educatie en Beroepsonderwijs. Toen we startten met het project op het gebied van digitaal ondertekenen hebben we nog overwogen om in te zetten op een wetswijziging. We hebben hier destijds niet voor gekozen, omdat zo’n wijzigingstraject heel lang duurt. Maar uiteindelijk heeft het project van Wellantcollege, Horizon College, MBO Utrecht en ROC de Leijgraaf al jaren in beslag genomen.





Eenzijds is dat begrijpelijk, omdat de digitale ondertekening van de onderwijsovereenkomst en de praktijkovereenkomst veel voeten in de aarde heeft. Anderzijds is het risico dat er onevenredig veel aandacht is voor de haken en ogen en te weinig voor de voordelen, zoals de efficiëncyslag. En eigen-

lijk gaat het niet eens zozeer om die voordelen; digitaal werken wordt steeds meer gemeengoed in de maatschappij, dus waarom nog niet in het mbo?" Naar de mening van Bert van Daalen zit de weerstand tegen digitaal ondertekenen niet bij de studenten en hun ouders, maar bij de

scholen zelf. "De medewerkers moeten eraan wennen. Het is belangrijk om je te realiseren dat zo'n omslag wel wat vraagt van de administratie. Je bent er niet met het maken van een instructie, want de reikwijdte en houdbaarheid daarvan zijn beperkt, waardoor het risico ontstaat dat mensen zelf workarounds gaan bedenken. Aangezien het gaat om enorme aantallen overeenkomsten, heeft een foutje al snel grote gevolgen. Het werken met digitale ondertekeningen vraagt echt een ander type vaardigheden dan het in Excel bijhouden wie zijn formuliertje heeft ingevuld. Zelfs al zorgt het werken met digitale ondertekeningen voor een efficiëncyslag, als de medewerkers er niet blij van worden heb je er nog weinig aan. Niet elke vernieuwing is een verbetering."

Wellantcollege is nog niet gestart met de implementatie met de digitale ondertekening van de onderwijsovereenkomst en de praktijkovereenkomst. Bert van Daalen: "Dat heeft vooral te maken met het feit dat dit project geen prioriteit heeft. Daarbij speelt mee dat de administratie binnen het aoc decentraal geregeld is, in tegenstelling tot bijvoorbeeld ROC de Leijgraaf. Doordat roc's verschillend georganiseerd zijn, verschillen de implementaties en de bijbehorende



spelregels.” Overigens heeft Wellantcollege wel de omgeving laten bouwen zoals die wordt gebruikt door ROC de Leijgraaf. Bert van Daalen geeft aan dat de gebruiksvriendelijkheid een belangrijke voorwaarde was bij het ontwikkelen van de omgeving. Zo is er een koppeling gemaakt met het Student Informatie Systeem. “Belangrijk is dat er zo min mogelijk stappen zijn bij de digitale ondertekening; het aanmaken, ondertekenen en opslaan van documenten vindt bij voorkeur plaats op die plek waar ook de documenten worden gecreëerd. Hoe eenvoudiger het is, hoe beter het werkt voor medewerkers. En voor studenten; zij hebben eigenlijk geen belang bij het ondertekenen van hun onderwijsovereenkomst en praktijkovereenkomst. Je kunt dreigen met het feit dat studenten geen onderwijs mogen volgen als ze hun onderwijsovereenkomst niet hebben ondertekend, maar daarmee snijdt een onderwijsinstelling alleen zichzelf in de vingers. Het is niet zoals bij de ondertekening van een koopovereenkomst bij een huis; daarbij is er sprake van een eigenbelang. Zonder koopovereenkomst immers geen sleutels en zonder sleutels geen toegang tot de woning. Bij de overeenkomsten in het mbo is dat eigenbelang er niet; belangrijk is dan ook dat er zo min mogelijk romp-



slomp komt kijken bij de ondertekening door studenten. Bij de ondertekening van overeenkomsten door personeel, bijvoorbeeld een arbeidsovereenkomst, ligt dat veel eenvoudiger. Ik zie wel kansen vanuit het project om daar ook iets mee te doen. Een andere kans zit in het werken met meerdere verificatiemethoden. Het voordeel van DigiD is dat moet worden voldaan aan allerlei

voorwaarden; het nadeel is dat deze methode allerlei assessments en audits met zich meebrengt die veel energie kosten. Uiteraard is bijvoorbeeld privacy belangrijk, maar de wetgever schiet soms wel eens beetje door in alles wat daarbij komt kijken! Als het gaat om een papieren overeenkomst, controleert niemand of de handtekening wel echt is; als het gaat om een digitale handte-





kening, hebben we opeens te maken met allerlei verificaties! Wat me ook bevreemdt, is dat een deel van de aandachtspunten per accountant verschilt. Dat geldt bijvoorbeeld voor de vraag waar het originele document wordt opgeslagen en welk document eigenlijk het origineel is. Het is op dit moment aan de accountant om te bepalen of hij met een vergrootglas of met een verrekijker naar de digitale ondertekening kijkt. Het zou mooi zijn als digitaal ondertekenen gemeengoed zou worden binnen het middelbaar beroeps-onderwijs.”

Wat zijn de ervaringen van het Horizon College?

Het Horizon College werkt samen met Educus aan de koppeling tussen Signhost en EduArte. Johan Oudejans, adviseur Informatievoorziening bij de Studenten-administratie: “Ons roc hecht veel waarde aan een goede integratie tussen de ondertekenapplicatie en het Student Informatie Systeem (SIS), zeker omdat het bij de digitale ondertekening van de onderwijs-overeenkomst en de praktijkovereenkomst gaat om grote aantallen. We willen bijvoorbeeld niet de mailadressen van studenten, ouders en leerbedrijven handmatig moeten

overzetten om een document voor digitale ondertekening aan te bieden. De kans op fouten is daarbij te groot. Medio 2016 zijn afspraken gemaakt met Educus om een eerste ‘basisversie’ van de koppeling tussen EduArte en de ondertekendienst van Evidos (Signhost) te ontwikkelen. Deze versie is eind december 2016 opgeleverd. In januari / februari 2017 hebben we op hoofdlijnen getest en daarna meer gedetailleerd. Dat hebben we gedaan met medewerkers van verschillende afdelingen om een goed beeld te krijgen van wat er nodig is in de praktijk en hoe de nieuwe functionaliteit daarop aansluit. De basisfunctionaliteit is als voldoende beoordeeld om een pilot mee te kunnen uitvoeren. Doel van de pilot is om de juiste werking definitief vast te stellen, om de veelbelovende businesscase te bevestigen en om de ‘confrontatie’ met de praktijk te maken op basis waarvan functionele doorontwikkelingswensen kunnen worden bepaald en beargumenteerd. Uiteindelijk worden de bevindingen in een evaluatiedocument opgeleverd, met een advies over mogelijke verdere uitrol binnen het Horizon College. Binnen de scope van de pilot richten we ons op maximaal driehonderd praktijkovereenkomsten (een mix van beroepsopleidende leerweg en beroepsbegeleidende

leerweg) voor twee onderwijssectoren. De pilot wordt uitgevoerd in de periode juli tot en met oktober 2017.”

Johan Oudejans geeft aan dat scholen die willen gaan werken met digitale ondertekening, rekening moeten houden met zowel functionele als technische randvoorwaarden. “Die functionele randvoorwaarden heb je grotendeels zelf in de hand. Denk daarbij vooral aan de impact op een aantal bestaande administratieve werkprocessen (bijvoorbeeld op documentinrichting, opslag van ondertekende documenten, gebruikers- autorisaties, gebruikersinstructies en parameterisering in het Student Informatie Systeem en in de ondertekenservice). Naast de functionele aspecten heb je te maken met veel technische inrichtingen. Hierbij is sprake van een samenspel tussen verschillende externe organisaties (de leverancier van de ondertekenservice, de leverancier van het Student Informatie Systeem en de leverancier van DigiD) die de inrichting van de systemen in een strakke volgorde uitvoeren. Dit gebeurt stap voor stap; een strakke regie vanuit de school en hierbij steeds een stap vooruit denken kan zorgen voor een beduidend kortere doorlooptijd. We maken hierbij gebruik van een overzichtelijk stappenplan dat ons door Evidos is aangereikt.”



Tot slot

Toekomstperspectief

Deze publicatie begint met de uitspraak dat digitale communicatie maatschappelijk en zakelijk breed geaccepteerd is en overal de standaard wordt. In het project 'Proof of Concept digitaal ondertekenen mbo' hebben we bekeken of het haalbaar is om de onderwijsovereenkomst en de praktijkovereenkomst digitaal te ondertekenen. Daarbij hebben we onder andere gekeken aan welke (wettelijke) eisen mbo-instellingen moeten voldoen en welke methoden er kunnen worden gebruikt voor bijvoorbeeld authenticatie. Maar op al deze aspecten zijn er dynamische ontwikkelingen. Zo komen er nieuwe vormen van digitale identificatie, zoals *Idensys*; hiermee wordt het een stuk veiliger en eenvoudiger om online zaken te regelen. Ook wordt gewerkt aan andere middelen waarmee mensen zich laagdrempelig kunnen authenticeren, zoals een identiteitskaart of bankpas. Een andere opkomende vorm van digitale herkenning is *eHerkenning*, waarmee functionarissen veilig en snel kunnen inloggen op webdiensten van (overheids)organisaties.

Er zijn niet alleen veranderingen te verwachten op het gebied van digitale identificatie, maar ook op het gebied van wet- en regelgeving. Hierbij is de implementatie van Algemene Verordening Gegevensbescherming (verplicht voor 25 mei 2018) een belangrijk richtpunt. Informatie hierover staat op de website van [de Autoriteit Persoonsgegevens \(AP\)](#) en [saMBO-ICT](#).

Verder zorgt het overheidsinitiatief '[generieke digitale infrastructuur](#)' (GDI) ervoor dat er steeds eenvoudiger koppelingen tussen systemen kunnen worden geïmplementeerd. De GDI bestaat uit standaarden, producten en voorzieningen die gezamenlijk gebruikt worden door meerdere overheden, vele publieke organisaties en in een aantal gevallen ook door private partijen. Op de website van [Digitale Overheid](#) worden de laatste berichten en ontwikkelingen over stimulering van digitalisering door de overheid voortdurend bijgehouden.

Een wenkend perspectief?

Het toekomstperspectief laat zien dat er allerlei ontwikkelingen zijn op het gebied van digitaal ondertekenen. Is het daarmee ook een wenkend perspectief? Wellicht levert de digitale ondertekening van de onderwijsovereenkomst en de praktijkovereenkomst scholen zo veel (financiële) voordelen op, dat ze ook andere mogelijkheden gaan onderzoeken. Bijvoorbeeld op het gebied van personeelsovereenkomsten. Er komen ongetwijfeld andere verificatiemethoden, die het nóg eenvoudiger maken om digitaal te communiceren binnen het onderwijs en daarmee zorgen voor efficiencylagen in de administratieve processen van onderwijsinstellingen.

Meer informatie

Wil je meer informatie over de mogelijkheden op het gebied van digitaal ondertekenen? Kijk dan op [de website van saMBO-ICT](#). Daar vind je alle links naar de documenten en websites die worden genoemd in deze publicatie.





'Digitaal ondertekenen in het mbo' is een uitgave van Kennisnet in samenwerking met saMBO-ICT

Datum van uitgave
September 2017

Redactie
Leo Bakker (Kennisnet), Henk-Jan van Ginkel
(saMBO-ICT), Twan Smets (saMBO-ICT)
Miranda van Elswijk (Entopic)

Eindredactie
Erik van den Berg (Kennisnet)

Met dank aan
Bert van Daalen (Wellantcollege), Eustaach van
Lent (ROC de Leijgraaf), Johan Oudejans
(Horizon College)

Fotografie
Rodney Kersten, Anne Carolien Kohler,
Etienne Oldeman

Vormgeving
Tappan Communicatie

Hoewel aan de totstandkoming van deze uitgave de uiterste zorg is besteed, aanvaarden de auteur(s), redacteur(s) en uitgever van Kennisnet geen aansprakelijkheid voor eventuele fouten of onvolkomenheden.

Over Kennisnet
Elke leerling verdient eigentijds, veilig en persoonlijk onderwijs. Daarom ondersteunt Kennisnet scholen met ict. We zorgen voor een landelijke ict-basisinfrastructuur, adviseren de sectorraden en delen onze kennis met het primair onderwijs (po), het voortgezet onderwijs (vo) en het middelbaar beroepsonderwijs (mbo). Kennisnet wordt gefinancierd door het ministerie van Onderwijs, Cultuur en Wetenschap (OCW).

Over saMBO-ICT
saMBO-ICT is een zelfstandige organisatie van en voor alle mbo-instellingen en heeft sterke banden met de MBO Raad en met Kennisnet. Belangrijke pijlers zijn belangenbehartiging, kennisdelingen projecten. saMBO-ICT houdt zich bezig met een breed aantal onderwerpen op het gebied van ict en informatievoorziening. saMBO-ICT maakt bij de activiteiten gebruik van de kennis en energie die binnen de instellingen aanwezig zijn en zorgt daarbij voor praktische ondersteuning.



kennisnet.nl sambo-ict.nl



Kennisnet
Paletsingel 32
2718 NT Zoetermeer

T 0800 321 22 33
E support@kennisnet.nl
I kennisnet.nl

Postbus 778
2700 AT Zoetermeer