

Ontwerp Edusign

Een generieke voorziening voor digitaal
ondertekenen binnen het onderwijsdomein

versie 1.2, september 2015

SURFnet
Kennisnet

Inhoud

1.	Inleiding	3
1.1.	Aanleiding	3
1.2.	Proces	3
1.3.	Historie	3
1.4.	Structuur document	3
2.	Eisen	5
2.1.	Scenario's	5
2.2.	Afbakening	5
2.3.	Wettelijke eisen	5
2.4.	Randvoorwaarden	6
2.5.	Stakeholders	6
3.	Logisch Ontwerp	7
4.	Procesontwerp	8
5.	Development view	10
5.1.	K1 en K2 koppelvlakken	11
5.2.	Signing Engines en audit trail	11
5.3.	Identiteitsproviders	11
6.	User stories	13
6.1.	Administratief medewerker instelling	13
6.2.	Ondertekenaar	14
6.3.	M2M koppeling SIS	15
6.4.	M2M koppeling Edusign – Signing/IdP leverancier	16
7.	Kwaliteitseisen	18
	Bijlage A: Toelichting begrippen en afkortingen	20
	Bijlage B: Ontwikkeling van Proof of Concept (PoC)	21
	Ervaringen PoC 1 en 2	21
	Uitgangspunten PoC 3	21
	Logisch ontwerp PoC 3	22

1. Inleiding

1.1. Aanleiding

Het terugdringen van administratieve lasten in het onderwijs is een belangrijke doelstelling van het SION-programma¹. Administratieve lasten komen onder meer voort uit 'papieren' processen rondom overeenkomsten en transacties waarvoor documenten moeten worden ondertekend. In de referentiearchitectuur onderwijs² is daarom een *ondertekenservice* benoemd als onderdeel van de generieke basisinfrastructuur. Dit ontwerp betreft een uitwerking van die ondertekenservice.

Digitaal ondertekenen levert een enorme besparing op. Alleen al in het MBO worden er op jaarbasis ongeveer 1,1 miljoen documenten ondertekend in het kader van de inschrijving (Onderwijsovereenkomst) of de stage (BPV-overeenkomst). Dit kan leiden tot een besparing van gemiddeld 12-15 werkweken op jaarbasis per MBO-instelling.

De uitwerking in dit ontwerp wordt gedreven door de concrete behoefte vanuit het project In- en Uitschrijven om het ondertekenen van de onderwijsovereenkomst digitaal te ondersteunen. Dat neemt niet weg dat het ondertekenen van documenten een algemene behoefte binnen het onderwijsdomein is. Vanuit de referentiearchitectuur wordt de ondertekenservice daarom neergezet als een generieke bouwsteen, bruikbaar voor het ondertekenen van allerlei documenten in diverse processen binnen verschillende sectoren.

1.2. Proces

Het ontwerp is tot stand gekomen in samenspraak met saMBO-ICT en een werkgroep van MBO-instellingen. De eerste focus heeft namelijk vooral gelegen op de ondertekening van de onderwijsovereenkomst en de stage-overeenkomst in het MBO. Voor het ontwerp is een Proof of Concept (PoC) gebouwd, die met de instellingen is beproefd. De bevindingen ten aanzien van het ontwerp zijn opgenomen in Bijlage B.

In 2015 is het ontwerp in overleg met Surfnets aangepast waar nodig.

1.3. Historie

Versie	Datum	Wijzigingen
0.4	17 maart 2014	Eerste versie die voorgelegd is aan de werkgroep met MBO-instellingen.
0.5	15 april 2014	Wijzigingen mbt workflow nav Werkgroep overleg
0.6	16 april 2014	Wijzigingen mbt het workflow nav keuzes t.a.v. workflow minderjarigen
1.0	10 juli 2014	Wijzigingen n.a.v. consultatieronde leveranciers zijn verwerkt
1.1	maart 2015	Aanpassingen i.o.m. Surfnets
1.2	September 2015	Aanpassingen n.a.v. gesprekken met MBO-instellingen t.b.v. inkooptraject

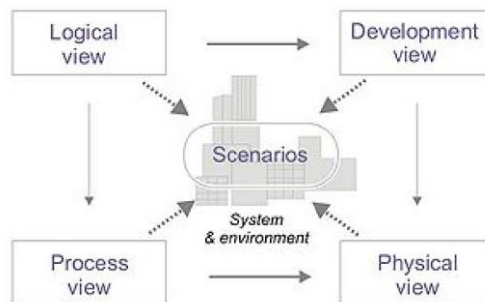
1.4. Structuur document

De structuur van dit document is in grote lijnen gebaseerd op het "4+1 Architectural View Model"³. Met dit model wordt een software-ontwerp vanuit verschillende views beschreven, die elk overeenkomen met de perspectieven van verschillende belanghebbenden.

¹ <http://www.sionderwijs.nl/>

² http://www.wikixl.nl/wiki/rosa/index.php/Referentie_Architectuur_Onderwijs

³ http://en.wikipedia.org/wiki/4%2B1_architectural_view_model



Figuur 1 4+1 model

In dit document wordt elk perspectief een aparte sectie behandeld, zij het dat voor de views in een aantal gevallen andere beschrijvingswijzen zijn toegepast dan wat het standaard 4+1 Model voorschrijft.

Hoofdstuk 2 geeft het Scenario view weer, en beschrijft de functionele basiseisen, randvoorwaarden en eisen vanuit de omgeving van de ondertekenservice. Hoofdstuk 3 geeft een logische indeling (Logical view) van de Ondertekenservice op hoofdlijnen. Hoofdstuk 4 proces ontwerp (Process view) beschrijft op hoog niveau het proces van het ondertekenen van een document. Hoofdstuk 5 biedt een aanzet voor een verdere uitwerking van de logische indeling naar componenten (Development view). Hoofdstuk 6 keert terug naar het scenario perspectief en werkt de basisscenario's in meer detail uit.

De Physical view is in deze versie van het ontwerp nog niet beschouwd.

2. Eisen

2.1. Scenario's

De ondertekenservice ondersteunt de volgende gebruiksscenario's:

1. Aanbieden van te ondertekenen document
2. Verzamelen van handtekeningen
3. Verspreiden ondertekend document
4. Melden afsluiting workflow met teruglevering ondertekend document
5. Inzien status
6. Controleren en ingrijpen in workflow
7. Beheer omgeving
8. Beheren accounts

2.2. Afbakening

De voorziening richt zich op:

- gebeurtenissen met groot volume, ofwel met (potentiële) besparing op administratieve lasten
- het digitaliseren van processen waarin papieren documenten worden ondertekend.
- ondertekening waarbij een zeker betrouwbaarheidsniveau wordt gevraagd
- meerdere partijen die een rol hebben die (deels) buiten de professionele context staat, zoals studenten, ouders en de stagebedrijven

De voorziening richt zich NIET op:

- buitenlandse studenten
- elektronisch betalen
- processen die al gedigitaliseerd zijn, maar onvoldoende betrouwbaar zijn (bijvoorbeeld cijferadministratie)

2.3. Wettelijke eisen

Op basis van een analyse van wetgeving kunnen we stellen dat een generieke ondertekenservice voor het onderwijsdomein moet voldoen aan de volgende eisen:

- ondersteunt ondertekening door individuen en organisaties
- biedt de mogelijkheid documenten te ondertekenen met een geavanceerde elektronische handtekening, dat wil zeggen een elektronische handtekening die
 - o op unieke wijze aan de ondertekenaar verbonden is;
 - o het mogelijk de ondertekenaar te identificeren;
 - o tot stand gekomen is met middelen die de ondertekenaar onder zijn uitsluitende controle kan houden;
 - o op zodanige wijze verbonden is aan de gegevens waarop zij betrekking heeft, dat elke wijziging achteraf van gegevens achteraf kan worden opgespoord.
- functioneert op STORK betrouwbaarheidsniveau 3 of vergelijkbaar
- waarborgt de 'schriftelijkheid' van een aangegane overeenkomst, dat wil zeggen dat
 - o de overeenkomst raadpleegbaar is door partijen
 - o de authenticiteit van de overeenkomst in voldoende mate gewaarborgd is
 - o het moment van totstandkoming van de overeenkomst met voldoende zekerheid kan worden vastgesteld
 - o de identiteit van de partijen met voldoende zekerheid kan worden vastgesteld

2.4. Randvoorwaarden

De voorziening voor digitaal ondertekenen:

- Voldoet aan het ontwerp dat door SURFnet en Kennisnet is/wordt vastgesteld
- maakt gebruik van DigiD (voor studenten), maar moet ook in staat zijn om andere authenticatiemiddelen te gebruiken, waaronder in ieder geval SURFconext, de Kennisnet Federatie (voor instellingen) en e-mail in combinatie met SMS codes (voor stagebedrijven).
- maakt zoveel mogelijk gebruik van bouwblokken die in de markt worden aangeboden
- is koppelbaar met bestaande Student Informatie Systemen
- is in staat documenten in PDF formaat te ondertekenen
- voldoet aan erkende beveiligingseisen

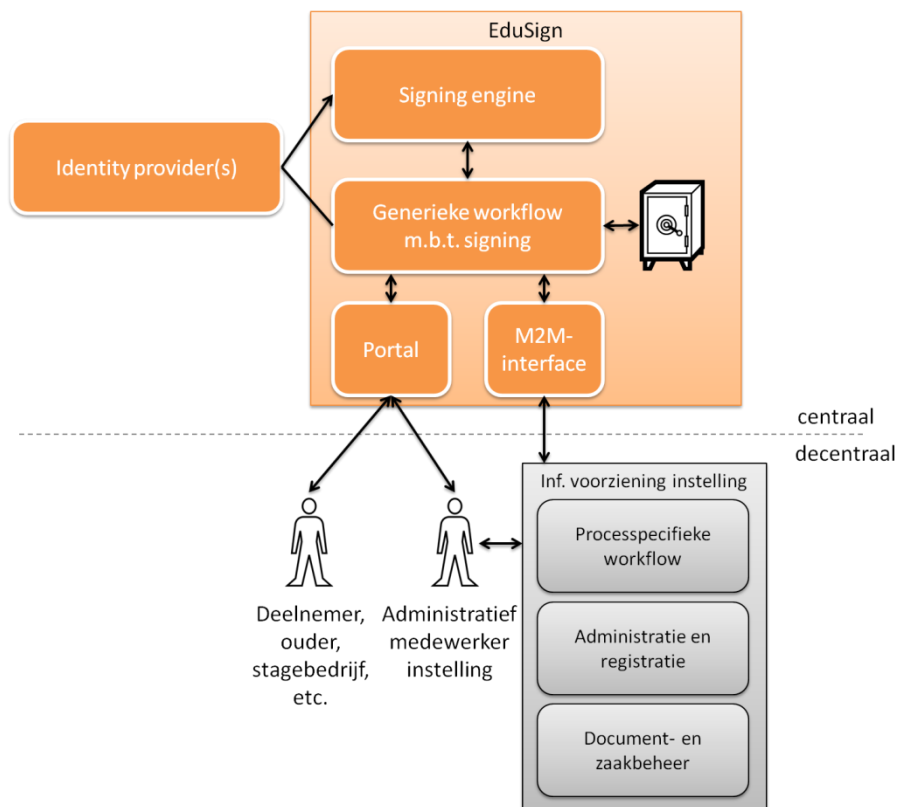
2.5. Stakeholders

Hieronder wordt een overzicht gegeven van de stakeholderbelangen, zoals die gelden in het toepassingsgebied van de Proof of Concept. In latere toepassingen zullen de specifieke stakeholders wijzigen of zullen er andere stakeholders en belangen van belang kunnen zijn.

Stakeholder	Belang	Interactie met systeem
Student	OOK en BPVO betrouwbaar, op tijd en veilig geregeld	Ondertekenen overeenkomst Invoeren ouder gegevens
Onderwijsinstelling	OOK en BPVO betrouwbaar, op tijd en veilig geregeld met minimale administratieve lasten, geen problemen in workflow	Niet van toepassing
Administratieve medewerker	Bruikbaar en betrouwbaar systeem, integratie met eigen SIS	Initiatie workflow
Ouder	Inschrijving/stage zoon/dochter goed geregeld, eenvoudige interactie met systeem, veilige omgang met BSN	Tekenen overeenkomst (buiten scope)
Stagebedrijf	BPVO door alle partijen op tijd ondertekend, minimale administratieve lasten	Tekenen overeenkomst
Medewerker stagebedrijf	Bruikbaar en betrouwbaar systeem, minimale extra inspanning	Tekenen overeenkomst
Leverancier identiteitsprovider (IdP) component	Eigen IdP oplossing zonder grote inspanning aansluitbaar op Edusign, geen voor-/nadeel concurrent	Leverancier component
Leverancier signing component	Eigen signing oplossing zonder grote inspanning aansluitbaar op Edusign, geen voor-/nadeel concurrent	Leverancier component
SIS leverancier	Eigen SIS oplossing zonder grote inspanning aansluitbaar op Edusign, geen voor-/nadeel concurrent	Koppelt met of integreert Edusign met eigen systeem
Functioneel applicatie beheerder	Minimale werklust door stabiele applicatie, heldere mogelijkheden om in te grijpen indien nodig	Installatie en configuratie van systeem, ingrijpen in workflow
Beheerpartij	Applicatie passend in hosting omgeving, beveiliging ingericht	
Eigenaar service	Betrouwbare omgeving tegen redelijke kosten die voldoet aan wettelijke eisen	

3. Logisch Ontwerp

EduSign bestaat uit een aantal logische bouwblokken die centraal aangeboden worden. Deze bouwblokken verzorgen de interactie met EduSign, 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. Voor het vaststellen van de identiteit van de ondertekenaars maakt EduSign gebruik van externe identity providers. Daarnaast kan het ondertekenproces verder ondersteund worden door informatiesystemen zoals het Student Informatie Systeem (SIS) en andere systemen daaromheen die 'binnen de muren van de instelling' zorg dragen voor zaken als administratie en registratie, documentbeheer, zaakbeheer, en uitvoering van proces-specifieke workflow.



Figuur 2 EduSign Logisch Ontwerp

4. Procesontwerp

Het proces dat Edusign ondersteunt kent op hoog niveau een aantal stappen:

- Een instelling genereert een document en verstuurt dit met de nodige gegevens naar een voorziening voor digitaal ondertekenen
- Deze voorziening bewaart het document tijdelijk en verstuurt een mail met uitnodiging tot ondertekening
- De ondertekenaar ontvangt de mail en klikt op de link. Hij/zij logt in.
- De ondertekenaar bekijkt het document en klikt op de knop ondertekenen binnen de voorziening
- Tijdens het proces kan de medewerker van de instelling inloggen bij de voorziening en de voortgang bewaken, zo nodig kan er een herinneringsmail gestuurd worden
- Zodra alle handtekeningen zijn gezet wordt het document verspreid naar alle ondertekenaars door de voorziening en hieruit verwijderd.

Hieronder wordt dit proces in meer detail uitgewerkt. Er wordt uitgegaan van een implementatie waarbij de student identificeert en ondertekent met DigiD. Voor de vertegenwoordigers van het stagebedrijf en de onderwijsinstelling is de keuze van Identity Provider (IdP) nog vrij.

0. Configureren workflow

- a. Een onderwijsinstelling stelt de stappen van de workflow voor een bepaald ondertekenenproces in. Een stap bestaat uit het ondertekenen in een bepaalde rol van het document. Een workflow is de specifieke volgorde waarin het ondertekenen plaats vindt, bijvoorbeeld eerst de student/ouders, vervolgens het stage bedrijf en afsluitend een medewerker namens de onderwijsinstelling.

1. Aanbieden van te ondertekenen document

- b. Een onderwijsinstelling biedt bij Edusign een document in PDF⁴ aan en de relevante gegevens van de partij(en) (onderwijsinstelling, student, stagebedrijf) die het document moet(en) ondertekenen. Dit gebeurt bij voorkeur op basis van een machine-machinekoppeling of anders vanuit het Edusign webportaal. Een onderwijsinstelling moet eventuele e-mailadressen via de m2m koppeling of in het portaal kunnen toevoegen, wijzigen of verwijderen.
- c. De PDF wordt door Edusign lopende het proces bewaard in een veilige 'kluis'.

2. Verzamelen van handtekeningen

- a. De student ontvangt een mail met een gepersonaliseerde link naar het document. De student volgt de link en identificeert zich met DigiD. Als BSN matcht, wordt document getoond.
- b. De student tekent de overeenkomst door op een knop 'ondertekenen' te drukken (actieve handeling). De student hoeft hiervoor niet opnieuw in te loggen, tenzij de DigiD-sessie is verlopen. Edusign verzendt mail(s) naar emailadressen met een gegenereerde unieke (voor de combinatie eindgebruiker-document-workflow) link naar het document.
- c. Het stagebedrijf ontvangt een mail met gepersonaliseerde link naar het document. De bijbehorende gebruiker volgt de link en identificeert zich (via hiervoor ingestelde inlogprocedure).
- d. Een vertegenwoordiger van het stagebedrijf kan het document inzien en tekent het document door op een knop 'ondertekenen' te drukken.
- e. De onderwijsinstelling logt in op Edusign waar alle documenten voor de onderwijsinstelling zijn verzameld voor ondertekening (via hiervoor ingestelde inlogprocedure).
- f. Een vertegenwoordiger van de onderwijsinstelling kan documenten inzien en tekent een of meerdere documenten door op een knop 'ondertekenen' te drukken.
- g. Na ondertekening, verbindt Edusign de identiteit van de ondertekenaars aan de PDF in de vorm van een elektronische handtekening. In de handtekening zijn de volgende gegevens zichtbaar op het document: naam, BSN rol, tijd, datum en middel ondertekening.

⁴ Alternatief: Het document wordt door Edusign omgezet naar PDF-formaat

3. Verspreiden ondertekend document

- a. Zodra alle handtekeningen zijn gezet, wordt de PDF afgesloten zodat ook de handtekeningvelden niet meer bewerkbaar zijn.
- b. De definitieve afgesloten versie van de PDF wordt per mail naar alle partijen verstuurd.

4. Melden afsluiting workflow met teruglevering ondertekend document

- a. De afgesloten versie van de PDF wordt door Edusign aan het bronsysteem van de onderwijsinstelling aangeboden.
- b. Na een afgesproken periode na de verzending wordt de door Edusign in bewaring genomen PDF uit de kluis gehaald en vernietigd.

5. Inzien status

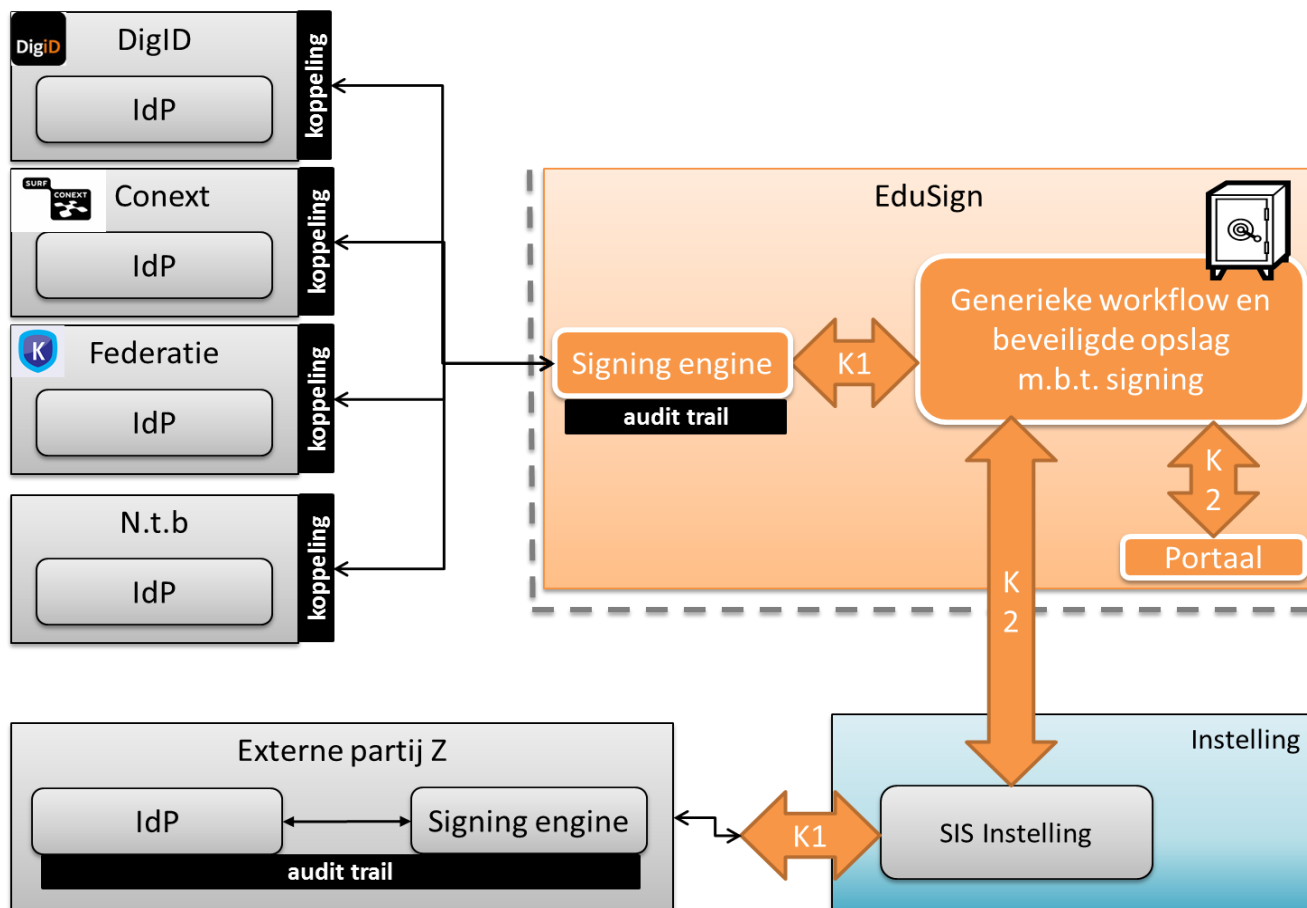
- a. Partijen kunnen aangeven dat zij op de hoogte willen worden gehouden van het plaatsen van nieuwe handtekeningen. Zodra een nieuwe handtekening is geplaatst, wordt dat per mail kenbaar gemaakt (dit is ook via het statusoverzicht zichtbaar en via de M2M interface opvraagbaar).
- b. Zolang nog niet alle handtekeningen zijn gezet, is de PDF inclusief de tot dan geplaatste handtekeningen in te zien vanuit het Edusign portaal.

6. Controleren en ingrijpen in workflow

- a. Een onderwijsinstelling kan de status van een workflow opvragen via het portaal of via de M2M interface in hun eigen systeem.
- b. Een onderwijsinstelling kan een workflow onderbreken via het portaal of via de M2M interface vanuit een eigen systeem. De workflow kan herstart worden of definitief gestaakt, waarna het document uit Edusign verwijderd wordt. Deelnemers krijgen hierover bericht (zonder dat het document wordt meegestuurd).

5. Development view

Deze view beschrijft de software componenten van Edusign. De bouwblokken uit het Logisch ontwerp worden hier verder uitgewerkt.



Figuur 3 Bouwblokken Edusign

Edusign levert een bouwblok dat door scholen en instellingen gebruikt kan worden voor het integreren van het ondertekenen in eigen systemen (SIS Instelling in Figuur 3 Componenten Edusign). Daarnaast wordt er een portaal geleverd voor toepassing van Edusign zonder integratie of koppeling met instellingsystemen.

Zowel het portaal als de systemen bij instellingen maken gebruik van een API, het koppelvlak K2 in de figuur, om opdrachten naar de workflow component van Edusign te geven. Dit betekent dat alle functionaliteit uit het portaal ook beschikbaar is voor koppellende systemen.

De workflow component bewaakt de voortgang van de ondertekening en de benodigde tussenstappen en slaat documenten op een veilige wijze op. Vanuit de workflow wordt via koppelvlak K1 de aangesloten signing engine(s) aangeroepen.

Edusign levert een signing engine als standaard bouwblok en biedt binnen de architectuur ruimte voor andere partijen om een dergelijke voorziening aan te sluiten. De keuze of de standaard signing engine gebouwd of afgenomen wordt en onder welke voorwaarden dient nog te worden gemaakt.

Identity providers (IdP's in figuur 3) koppelen op de signing engine(s) via eigen interfaces. Vanuit de EduSign context worden koppelingen met DigKoppeling, Surf Conext en de Kennisnet Federatie vereist.

5.1. K1 en K2 koppelvlakken

Het K1 koppelvlak koppelt de Edusign workflow aan de signing engine. EduSign zal de interface definitie en randvoorwaarden voor het koppelvlak definiëren. Partijen kunnen wanneer zij voldoen aan deze eisen hun signing engine aansluiten op de EduSign workflow.

Een tweede toepassing van de K1 interface is dat systemen binnen instellingen gebruik maken van het K1 koppelvlak om aan te sluiten op een signing engine. In dat geval zal een het instelling systeem zelf de workflow bewaking moeten regelen

De K2 interface wordt door zowel het eigen Edusign portal als door administratieve systemen binnen instellingen gebruikt met de workflow engine gegevens uit te wisselen. Door het portal ook via de interface aan te sluiten, zal de K2 interface dezelfde functionaliteit beschikbaar kunnen stellen als de portal biedt.

De K1 en K2 koppelvlakken zullen (zoveel mogelijk) in lijn met de Edukoppeling standaard worden opgezet, waarbij SAML zal worden toegepast als protocol voor het uitwisselen van gegevens.

5.2. Signing Engines en audit trail

Uit ervaringen met de PoC's en uit gesprekken met leveranciers blijkt dat eisen aan de beveiliging en het vastleggen van zoveel mogelijk gegevens rond een handtekening voorschrijven dat de integratie van IdP en signing engine heel nauw komt. Leveranciers van signing engines bieden daarom oplossingen waarin deze integratie door hen is uitgevoerd met een aantal IdP leveranciers.

Bij die integratie wordt een 'audit trail' toegepast. Er wordt een zo groot mogelijke collectie data verzameld over het tot stand komen van de elektronische handtekening, zoals ip nummer, tokens, netwerk gegevens, etc. Deze gegevens worden toegevoegd aan de handtekening in het document en vormen zo een steviger basis voor de betrouwbaarheid van de handtekening.

Door de eisen aan de beveiliging en de behoefte om met een audit trail de 'bewijslast' rond een handtekening te verstevigen, zijn de eisen aan de integratie tussen IdP en signing engine hoog. Het aanbieden van een koppelvlak waar 'vrij' IdP's kunnen aansluiten op een leverancier van een engine komen daarom in praktijk nauwelijks voor. Leveranciers leveren complete 'signing blocks', waarbij een of meerdere IdP's worden toegepast.

Voor Edusign zal een dergelijk signing blok met DigiD als basis IdP worden ingericht. Op basis van de behoeften vanuit het veld kunnen andere IdP's worden toegevoegd aan dit blok. Later kunnen signing blokken van andere leveranciers (via het K1 koppelvlak) die voldoen aan de Edusign eisen, toegevoegd worden aan de keten.

5.3. Identiteitsproviders

Voor iedere toepassing (stageovereenkomst MBO, cijferadministratie, etc.) zal een specifieke workflow moeten worden ingericht met daarin eigen rollen (stagebegeleider, student, docent). Voor een rol dient een identiteits verlener (Identity provider, IdP) te worden gevonden die past bij toepassing, workflow en rol.

Uitgangspunt is dat identiteiten geleverd worden met een voldoende betrouwbaarheid (die minimaal het niveau moet halen van het benodigde betrouwbaarheid niveau van het te tekenen document. Dit niveau van betrouwbaarheid zal per toepassing anders zijn en voor iedere workflow vastgesteld en ingericht moeten worden.

6. User stories

6.1. Administratief medewerker instelling

De user stories in dit hoofdstuk betreffen de taken die de Administratief Medewerker van een instelling uitvoert via de portal. Bij een integratie met het SIS van de instelling (met een koppeling via de API) zal (een deel van) deze taken via het SIS worden uitgevoerd.

0. Wat moet een instelling doen voordat deze gebruik kan maken van deze dienst?

1. Inloggen op Edusign

De medewerker logt in met zijn account gegevens. Na verificatie wordt hij geautoriseerd voor de gegevens van zijn instelling.

2. Opvragen Status Overzicht

De medewerker krijgt overzicht van alle documenten van zijn instelling en de voortgang daarvan in de workflow. Dit overzicht is exporteerbaar via de user interface (als csv en xml).

In het overzicht zijn de volgende gegevens zichtbaar:

- Documentnaam: bestandsnaam van document
- Datum initiatie
- Verloop datum (datum waarop document ondertekend moet zijn)
- Link naar document (downloadable)
- Status: In voorbereiding, Compleet, Gestart, Geweigerd, Beëindigd)
- Lijst van ondertekenaars met:
 - o Naam
 - o Emailadres
 - o BSN (optioneel, in geval van 'student')
 - o Rol (student/stagebedrijf)
 - o Datum email verzonden
 - o Status email (wanneer verzonden mail is gebounced)
 - o Datum getekend (indien dit is gebeurd)
 - o Datum geweigerd (indien ondertekenaar dit heeft aangegeven)
 - o Reden geweigerd (indien ondertekenaar dit heeft aangegeven)

Deze lijst is te filteren en te sorteren.

3. Inzien document

Een medewerker van de onderwijsinstelling kan de huidige versie van de (deels ondertekende) documenten downloaden. (Dit geldt alleen voor de documenten binnen workflows van de instelling van de betreffende medewerker. Ook is de bewaarduur van documenten na beëindiging van een workflow na voltooiing of onderbreking gelimiteerd waarna documenten verwijderd worden en niet langer opvraagbaar zijn.)

4. Initiëren en beheren workflow voor document

Een medewerker kan een onderteken workflow beheren en nieuwe opstarten. Hiervoor beschikt hij over de volgende functies:

- Instellen stappen: Hoeveel ondertekenaars met welke rol moeten een document in welke volgorde ondertekenen en met welk authenticatiemiddel worden deze toegelaten.
- Keuze authenticatiemiddel: De medewerker bepaalt per document en per rol welk middel gebruikt dient te worden voor de ondertekening. Voor de ondertekening van onderwijsvolgers is het middel default ingesteld op "DigiD midden".
- Instellen verloopdatum of interval: De medewerker stelt met deze datum het moment in waarop de workflow wordt beëindigd (ongeacht de voortgang) of het maximale tijdsinterval dat beschikbaar is voor de workflow. Wanneer geen datum wordt ingesteld wordt dit automatisch ingesteld op een vast interval. Zolang de workflow nog niet beëindigd is kan de medewerker deze datum opnieuw installen.

- Uploaden bestand: De medewerker kan een PDF bestand uploaden. Zolang de status van de workflow 'In voorbereiding' is, kan dit document vervangen worden. Zodra de workflow gestart wordt, is dit niet langer mogelijk.
- Bijwerken workflow status: De medewerker kan een workflow met status 'In voorbereiding' starten of een reeds gestarte workflow beëindigen (ongeacht de voortgang), waarna er geen handelingen op het document meer mogelijk zijn.
- Beheren ondertekenaars: De medewerker kan de gegevens van ondertekenaars wijzigen. Afhankelijk van het type workflow is een minimum aantal ondertekenaars van specifieke typen vereist (en kan de workflow pas worden gestart na het voldoen aan deze minimum eis). Als een ondertekenaar het document van de workflow heeft ondertekend, kunnen zijn gegevens niet langer gewijzigd worden.

5. Ingrijpen workflow

Een medewerker kan ingrijpen in een lopende workflow. Hiervoor biedt het systeem de volgende mogelijkheden:

- Versturen gepersonaliseerde berichten: Een medewerker kan een bericht sturen aan een of meerdere te selecteren deelnemers van de workflow.
- Instellen automatische herinnering: Een medewerker kan een periode instellen; wanneer een ondertekenaar na het verstrijken hiervan nog niet heeft ondertekend, wordt door het systeem een bericht naar hem verstuurd.
- Stop op verdere stappen: Een medewerker kan de workflow onderbreken (status wordt 'onderbroken'). Vanaf dat moment zijn er geen bewerkingen meer mogelijk op het document.
- Verwijderen document: Een medewerker kan een document verwijderen uit het systeem. Indien de workflow nog niet voltooid of onderbroken is, wordt deze onderbroken (zie boven), waarna het document wordt verwijderd.

6. Einde workflow

Na het ondertekenen van een document door de laatste ondertekenaar in de workflow, komt de workflow ten einde en wordt het ondertekende document opgeslagen in de kluis.

- Bij gebruik van het portaal kan de medewerker (na inloggen) het document downloaden.
- Bij koppeling met een instellingsysteem zal het desbetreffende systeem het document opvragen via de K1 of K2 interface.

7. Bewaken workflow

De workflow engine controleert of het ondertekenen proces nog voorgezet moet worden:

- a. Verstreken verloopdatum: De ingestelde datum waarop document is ondertekend is verstreken zonder dat alle partijen dit getekend hebben. De workflow wordt onderbroken (document wordt niet meer aangeboden ter ondertekening). De medewerker kan via user story .5 de workflow herstarten of definitief beëindigen.
- b. De workflow heeft de mogelijkheid om periodiek na een instelbaar interval partijen die een uitnodiging tot ondertekenen hebben ontvangen automatisch een herinneringsbericht te versturen.

8. Administratieve taken

Medewerkers van onderwijsinstellingen kunnen in de admin omgeving van het webportaal:

- c. Accounts aanmaken voor andere medewerkers
- d. Berichten (mailing) en omgeving personaliseren

6.2. Ondertekenaar

Een ondertekenaar krijgt in Edusign een specifieke rol (Bijvoorbeeld: student, stagebedrijf, etc.) die te maken heeft met taak en volgorde in het proces. De functionaliteit en user interface van deze rollen komt sterk overeen. Een uitzondering vormt de rol van de 'student'; in specifieke workflows hebben ondertekenaars met deze rol de verantwoordelijkheid voor het verstrekken van het email adres van personen met de rol 'ouders'.

Verder kunnen de methoden van authenticatie en signing verschillend zijn voor rollen per workflow. In het ideale geval krijgen alle gebruikers ongeacht rol of toegepaste methoden eenzelfde gebruikersinterface gepresenteerd, waarbij de workflow engine onzichtbaar ervoor zorgt dat alle gegevens correct bij alle partijen wordt afgeleverd.

In de toepassing voor de MBO stage overeenkomst worden de volgende methoden ondersteund:

- Onderwijsinstellingen: Kennisnet Federatie/SURFconext
- Stagebedrijf MBO: Two-factor authentication (email en sms)
- Ouders: DigiD op termijn, maar dat is nu nog niet mogelijk
- Leerlingen MBO: DigiD

Voor ondertekening door de student moet door de school het emailadres en BSN nummer doorgegeven worden aan Edusign. Met het emailadres kan een link worden verstuurd. Met het BSN nummer kan geverifieerd worden of degene die inlogt met DigiD ook daadwerkelijk moet ondertekenen. De student moet dus alleen een DigiD account hebben.

Bij stagebedrijven moet de school het emailadres en mobiele nummer van het stagebedrijf doorgeven. Edusign kan dan eveneens een link versturen met een login per mail. Naast de login wordt een SMS verstuurd naar het – door de school - doorgegeven mobiele nummer. Het stagebedrijf moet dus de goede gegevens doorgeven aan de school voor ondertekening.

In dat geval ontstaat een generiek userstory patroon:

1. Edusign verstrekt unieke link aan ondertekenaar in gespecificeerde volgorde.
2. Ondertekenaar navigeert naar en logt in op de in de workflow gespecificeerde IdP.(Of geeft aan dit te weigeren (met reden)).
3. Na succesvolle login wordt op basis van toegangscode ondertekenaar naar specifiek document geleid, gereed voor ondertekening.
4. Ondertekenaar start signing
 - a. Indien ondertekenaar signing heeft gestart, initieert Edusign signing op de in workflow gespecificeerde Signing Engine.
 - b. Indien ondertekenaar weigert wordt workflow status op 'Geweigerd' ingesteld.
5. Edusign verstuurt mail naar ondertekenaar (en indien geconfigureerd de administratief medewerker en/of student en/of overige ondertekenaars).

Afwijking voor rol Student

De rol van student kent een specifieke uitbreiding op de generieke userstory in het geval dat een student minderjarig is (aangegeven door medewerker instelling bij initiatie workflow). In dat geval volgt na stap 4 van de generieke workflow de volgende stappen:

7. Student voert naam en emailadres ouder in.
8. Edusign slaat deze gegevens op.

Vervolgens wordt de user story vervolgd met stap 5.

9. Einde workflow

Zodra alle vereiste handtekeningen op het document geplaatst zijn, ontvangt de ondertekenaar het ondertekende document.

Alle nog niet alle handtekening geplaatst zijn, dan ontvangt de ondertekenaar bericht hoeveel handtekeningen er nog gezet dienen te worden.

6.3. M2M koppeling SIS

De M2M koppeling met een SIS is een API zijn die door Edusign wordt aangeboden (K2 in Figuur 3 Componenten Edusign). Deze API volgt de Edukoppeling standaard⁵. Via de API zal de complete set van de 'medewerker' functionaliteit (zie boven) ontsloten worden, zodat vanuit het SIS een workflow gestart,gevolgd en beheerd kan worden.

⁵ <http://www.edustandaard.nl/afspraken-en-architectuur/beheerde-afspraken/edukoppeling/>

1. Aanmelden SIS

Het SIS maakt verbinding met de Edusign api, waarbij de api key wordt gecontroleerd. Na deze verificatie krijgt het SIS toegang tot de gegevens van de desbetreffende instelling.

2. Initiëren workflow

Het SIS verstuurt de gegevens volgens een specificerde api call naar Edusign. Edusign bevestigt ontvangst en correctheid of geeft hier foutmelding over.

3. Status overzicht

Het SIS verstuurt een verzoek volgens een gespecificeerde api call naar Edusign. Edusign verstrekt de actuele statusinformatie van de desbetreffende workflow (zie boven) of geeft een foutmelding.

De interface K2 wordt bij voorkeur in zijn geheel door EduSign aangeboden. Een aangesloten SIS zal als client fungeren en zelf geen koppelvlak aanbieden. Dit heeft als voordelen dat EduSign een grote(re) controle heeft over de beveiliging van de koppeling en dat de benodigde inspanning voor SIS-bouwers verkleind wordt.

In deze versie van het ontwerp is het interactiepatroon voor de koppeling K2 niet verder uitgewerkt. Het is aan de leverancier om dit uit te werken.

6.4. M2M koppeling Edusign – Signing/IdP leverancier

Via de M2M koppeling tussen de signing engine en de workflow/opslag componenten (K1 in Figuur 3 Componenten Edusign) zal minimaal een Signing/IdP leverancier worden gekoppeld met Edusign. Deze interface zal worden aangeboden door de leverancier volgens de Edusign specificaties. Deze API volgt de Edukoppeling standaard⁶.

In de Edusign wordt uitgegaan van een situatie waarbij vanuit de markt combinaties van Signing/IdP 'blokken' worden aangeboden, waarop aangesloten worden. In een workflow kunnen meerdere van deze 'blokken' toegepast worden; de workflow wordt bewaakt door Edusign.

Een SIS kan ook kiezen voor een directe koppeling met een 'blok' van een leverancier zonder gebruik te maken van Edusign. In dat geval koppelt het SIS via deze interface.

De API biedt de volgende functionaliteit:

1. Aanmelden Edusign/SIS

Edusign maakt verbinding met de api, waarbij de api key wordt gecontroleerd. Na deze verificatie kan Edusign een document ter ondertekening aanbieden.

2. Aanbieden document

EduSign verstuurt een document en gegevens van de ondertekenaar(s) volgens een specificerde API call naar de leverancier. Deze bevestigt de ontvangst en correctheid of geeft hier foutmelding over.

3. Opvragen status

Edusign verstuurt een verzoek volgens een gespecificeerde api call naar de Leverancier. De leverancier verstrekt de actuele status van het document (ondertekenend/geweigerd/aangeboden).

4. Opvragen document

Edusign verstuurt een verzoek volgens een gespecificeerde api call naar de Leverancier. De leverancier geeft het ondertekende document terug (en verwijderd dit uit zijn systeem).

⁶ <http://www.edustandaard.nl/afspraken-en-architectuur/beheerde-afspraken/edukoppeling/>

In deze versie van het ontwerp is het interactiepatroon voor de koppeling K1 niet verder uitgewerkt. Het is aan de leverancier om dit uit te werken.

7. Kwaliteitseisen

Onderdeel	Architectuur
Omschrijving	Het onderwijs werkt aan een efficiëntere en uniforme (sectoroverstijgende) informatievoorziening. De ROSA is de referentiearchitectuur van het onderwijs en is een instrument bij informatiegerichte ketensamenwerking. Met het Certificeringsschema kunnen binnen het onderwijsdomein clouddiensten en -leveranciers worden getoetst op basis van een gezamenlijk opgesteld 'normenkader'.
kwaliteitseisen	
	De leverancier en Edusign conformeren zich aan de eisen en voorschriften uit de Referentie Architectuur van het Onderwijs (ROSA) .
	De leverancier is getoetst aan de hand van het Certificeringsschema ROSA
	De leverancier en Edusign conformeren zich aan de eisen en voorschriften uit de Hoger Onderwijs Referentie Architectuur (HORA) .

Onderdeel	Gegevens
Omschrijving	Instellingen zijn en blijven eigenaar van de gegevens in het Edusign. Een instelling moet over deze gegevens kunnen beschikken wanneer dit nodig blijkt.
kwaliteitseisen	
	Instellingen kunnen via de K2 interface of via het portaal zonder tussenkomst van een leverancier op ieder moment hun documenten terug trekken uit de workflow. De documenten worden blijvend en volledig verwijderd uit de EduSign omgeving.
	Documenten en de audit trail(s) worden automatisch na een per workflow afgesproken/ingesteld interval verwijderd of uiterlijk na de wettelijk hiervoor vastgestelde termijn. Door deze instelbaar te maken wordt een bewuste afweging per casus tussen gebruiksgemak en beveiliging mogelijk.
	Het toegepaste PDF formaat voldoet aan een open standaard en ondersteunt digitaal ondertekenen binnen het document (PDF 1.7 - ISO 32000-1:2008 of nieuwere versies).

Onderdeel	Aanpasbaarheid
Omschrijving	EduSign moet in staat zijn het ondertekenproces bij meerdere instellingen te ondersteunen. Hiervoor is het nodig dat er meerdere workflows geconfigureerd kunnen worden.
kwaliteitseisen	

	De workflow engine moet aansluiten en te configureren zijn in lijn met de procedures voor de organisatie. Via de K2 interface of in het protaal moet een stappenplan voor ondertekening van een document door meerdere personen via meerdere IdP's en/of signing engine(s) instelbaar zijn.
--	---

Onderdeel	Koppelingen
Omschrijving	Voor het effectief en efficiënt uitwisselen van informatie in het onderwijs is het aansluiten op en aanbieden van standaard interfaces een 'must'.
kwaliteitseisen	
	Edusign volgt waar mogelijk de EduKoppeling standaard (met name de EduKoppeling Transactie standaard is hier van belang) bij het aanbieden van de K1 en K2 interfaces.
	Edusign houdt een log bij van binnengekomen documenten, de voortgang binnen de workflow en de toegepaste signing- en identiteit - leverende partijen.

Onderdeel	Privacy
Omschrijving	
kwaliteitseisen	
	De Wet bescherming persoonsgegevens (Wbp) is uitgangspunt voor elke vorm van gegevensregistratie, -verwerking en -uitwisseling.
	Leveranciers conformeren zich aan het Juridische normenkader cloudservices hoger onderwijs .
	Leveranciers maken (indien van toepassing) zoveel mogelijk gebruik van in Europa ((Europese Economische Ruimte) gevestigde cloud leveranciers.

Onderdeel	Beveiliging
Omschrijving	De onderstaande lijst geeft een aantal punten die in deze context extra aandacht verdienen, maar is geen complete lijst.
kwaliteitseisen	
	Edusign heeft een audittrail waar wijzigingen op gegevens worden gelogd (cf wetgeving).
	Omdat deze bestanden vanuit instellingen worden aangeleverd en het niet uit te sluiten is dat het hierbij om gevoelige informatie gaat, is het veilig, betrouwbaar en tijdelijk opslaan van deze bestanden in wezenlijk onderdeel van EduSign. Het inrichten hiervan is dan ook een belangrijke verantwoordelijkheid van de leverancier (en eventuele hosting partij(en)). Documenten die aangeboden worden ter ondertekening, worden beschermd binnen de EduSign omgeving (in 'de kluis') worden beschermd op een niveau in relatie tot de gevoeligheid deze gegevens.

Bijlage A: Toelichting begrippen en afkortingen

(Digitale) handtekening

Het equivalent verstaan van de zogenaamde “natte” handtekening op een papieren document

IdP

Identiteitsprovider

SIS

Student Informatie Systeem

OOK

Onderwijsovereenkomst

BPVO

Beroepspraktijkvorming Overeenkomst

API

Application Programming Interface

Een application programming interface (API) is een verzameling definities op basis waarvan een computerprogramma kan communiceren met een ander programma of onderdeel (Bron: Wikipedia)

M2M

Machine-to-Machine

BSN

Burger Service Nummer

DigiD

Digitale sleutel voor toegang tot overheidsdiensten (op basis van BSN)

SAML

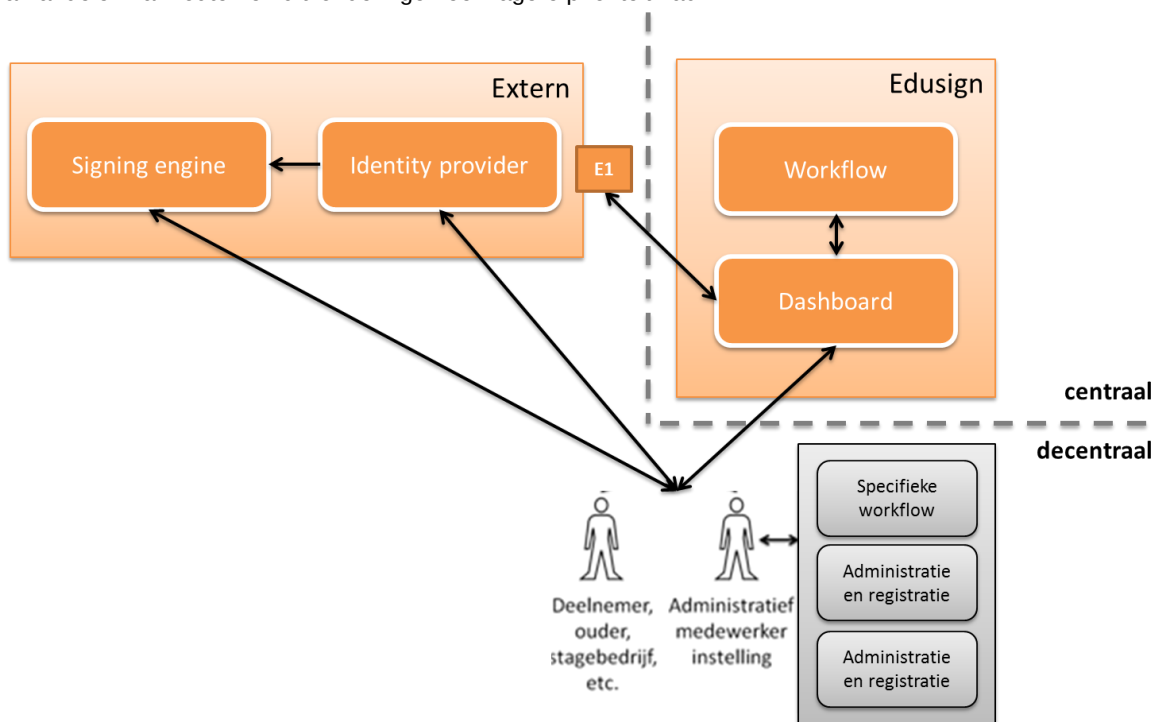
Security Assertion Markup Language

SAML is een op XML gebaseerde standaard voor het uitwisselen van authenticatie- en autorisatiegegevens tussen domeinen. (Bron: Wikipedia)

Bijlage B: Ontwikkeling van Proof of Concept (PoC)

Ervaringen PoC 1 en 2

In de Proof of Concepts 1 en 2 zijn delen van de functionaliteit geïmplementeerd, waarbij de aandacht vooral heeft gelegen op het vaststellen van technische (on)mogelijkheden. Uitgangspunt was de 'happy flow', waarbij het afhandelen van fouten en uitzonderingen een lagere prioriteit had.



Figuur 4 Logisch ontwerp PoC 1 en 2

Het logisch ontwerp van de PoC's is vereenvoudigd ten opzichte van het ontwerp uit hoofdstuk Ontwerp. De voornaamste wijzigingen zijn:

- Gebruik interfaces IdP en Signing Partijen. In het oorspronkelijke ontwerp wordt uitgegaan van een eigen interface waarop IdP's en Signing partijen koppelen. In de praktijk blijkt dat deze partijen interfaces aanbieden waarop gekoppeld is (E1 in figuur 3).
- Geen koppeling met SIS. Er is in PoC 1 en 2 gekozen om de medewerkers van instellingen te laten werken via het portaal van Edusign.
- Gebruikers werken in IdP en Signing Engine omgevingen. Bij het koppelen met IdP en Signing voorzieningen bleek dat het technisch nog niet mogelijk was om een geïntegreerde gebruikers interface te implementeren.

Uitgangspunten PoC 3

Bij het ontwerp van PoC 3 is uitgegaan van de volgende uitgangspunten:

- Verhogen van de robuustheid:
 - o Afvangen van 'unhappy flows'
 - o Bewaken workflow
- Uitbreidbaarheid:
 - o Ondersteunen van en koppelen met meerdere IdP's en authenticatie methoden
 - o Ondersteunen van en koppelen met meerdere Signing engines en methoden

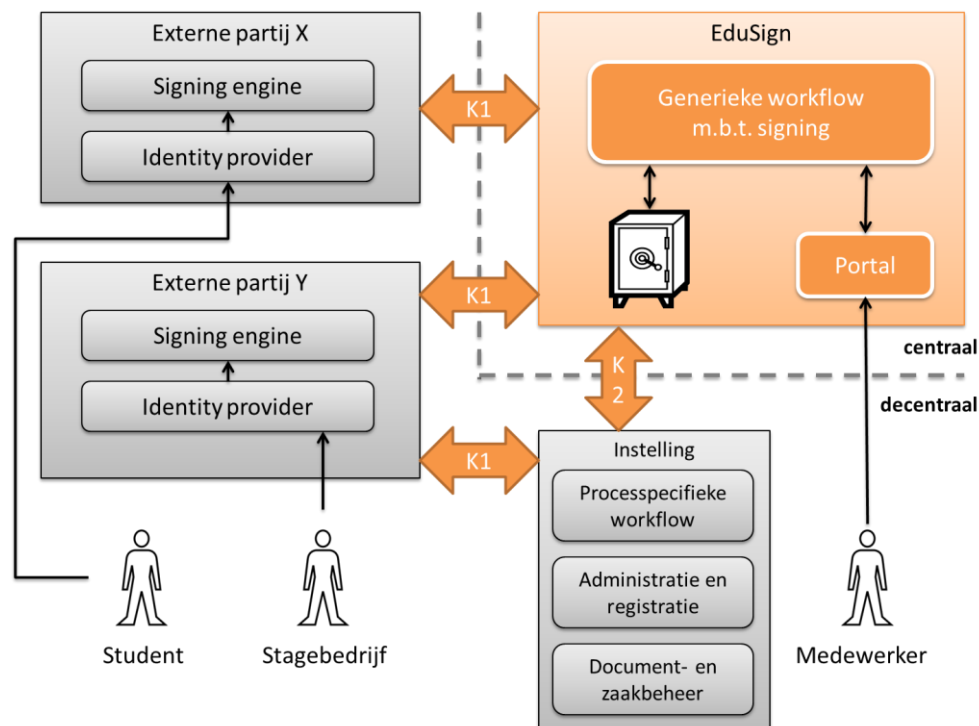
- Integreerbaarheid
 - o Implementatie van een API voor SIS conform EduStandaard
 - o Implementatie van een API voor Signing Engine's en IdP's conform EduStandaard
- Beveiliging
 - o Netwerk configuratie aanpassen aan risico's van PoC toepassing(en)
 - o Beheer koppeltabel voldoende veilig ingericht
 - o Traceerbaarheid verhogen van stappen in workflow
 - o Pseudo identiteiten als basis voor ontwerp workflow toepassen
- Schaalbaarheid
 - o Configuratie in lijn brengen met omvang en belang van PoC toepassing(en)
- Standarisatie
 - o Interfaces volgen de Edukoppeling en VCard standaarden

De workflow van de PoC applicatie is document gericht:

- 'Ondertekenaars' komen via de link in de (externe) omgeving van een leverancier. De gebruiker komt binnen bij het specifieke document. (Er zijn geen 'overzichtschermpjes' voor gebruikers die bij meerdere documenten betrokken zijn een overzicht geven van documenten.)
- Documenten worden niet gearhiveerd. Na het voltooien van een workflow blijven documenten een gelimiteerde tijd opvraagbaar (voor de administratief medewerker en via de M2M koppeling). Daarna wordt het document verwijderd uit de opslag. Ook bij onderbroken workflows wordt het document na het verstrijken van een ingestelde periode verwijderd.

Logisch ontwerp PoC 3

Op basis van de uitgangspunten voor PoC 3 en de ervaringen uit de eerdere PoC's, is het logisch ontwerp aangepast.



Figuur 5 Logisch ontwerp PoC 3

In PoC 3 moeten meerdere Signing Engine's en/of IdP's ondersteund kunnen worden via de Edusign workflow, waarbij er wordt uitgegaan dat deze externe voorzieningen via hun eigen interfaces worden aangesproken (E1 t/m En). Op termijn zal gestreefd worden naar een standaard interface (API) voor deze koppeling.

Daarnaast zal in PoC 2 een API worden aan geboden aan decentrale instellingssystemen (K3 en API), om op dat vlak een grotere integratie te bereiken.

Tenslotte zal er geen sprake meer zijn van volledig integratie van de gebruikersinterface in de Edusign workflow. Gebruikers worden rechtstreeks naar de IdP en Signing engine geleid.