
CATCHPlus

User Profile Repository Functioneel Ontwerp Versie 1.3

User Profile Repository
Functioneel Ontwerp
Versie: 1.3
Publicatiedatum: 18-1-2012

User Profile Repository	Versie: 1.3
Functioneel Ontwerp	Datum: 18-1-2012

Documenthistorie

Datum	Versie	Beschrijving	Auteur
29-08-2011	1.0	Initiële versie	Peter Bloem
12-10-2011	1.1	Bijgewerkte versie	Mart Trautwein
5-1-2012	1.2	User Story bijgewerkt, niet-functionele eisen uitgebreid, architectuur beschreven, toelichting OpenID bijgewerkt	Mart Trautwein
18-1-2012	1.3	Hoofdstuk Gebruikersidentificatie en authenticatie toegevoegd	Mart Trautwein

Distributie

Naam	1.0	1.1	1.2	1.3										
GridLine	X	X	X	X										
CATCHPlus	X	X	X	X										
Beeld & Geluid	X	X	X	X										

User Profile Repository	Versie: 1.3
Functioneel Ontwerp	Datum: 18-1-2012

Inhoudsopgave

Inleiding.....	5
Doel van dit document.....	5
Referenties.....	5
Globale Architectuur.....	6
Verantwoordelijkheden & vertrouwen.....	6
Applicatie landschap	6
Uitgangspunten.....	8
Gebruikers.....	8
Usability tests.....	8
Entiteiten, taken, paden en rollen	10
Entiteiten.....	10
Rollen	11
User stories	12
User Story 1.....	12
User Story 2.....	14
Use-cases en vereiste functies.....	15
Overzicht use-cases.....	15
Vereiste functies	15
Niet-ondersteunde functies	16
Niet-functionele eisen.....	16
Gebruikersidentificatie en authenticatie	18
Gebruikersidentificatie.....	18
Authenticatie.....	19
Autorisatie.....	20
Primaire databronnen.....	21
OpenID Providers	22
Datamodel Profielinformatie	23
Profielinformatie in UPR	23
Gedelegeerde profielinformatie	23
Bijlage 1: Globale workflows.....	24

User Profile Repository	Versie: 1.3
Functioneel Ontwerp	Datum: 18-1-2012

Bijlage 2: Inloggen met OpenID	27
--------------------------------------	----

User Profile Repository	Versie: 1.3
Functioneel Ontwerp	Datum: 18-1-2012

Inleiding

Doel van dit document

Dit document beschrijft het functioneel ontwerp van de *User Profile Repository* en het *ZieOok Recommendation Platform* dat GridLine bouwt voor het CATCHPlus project, in samenwerking met Beeld & Geluid.

Het grafisch ontwerp ([2]) bevat mockups van de widgets en UPR-website.

Referenties

- [1] GridLine; *Voorstellen Toekomstige Functionaliteit*; versie 1.0; 29-8-2011.
- [2] GridLine; *Grafische Ontwerp*; versie 1.1; 12-10-2011
- [3] Hennie Brugman (CATCHPlus); *Visie document : User Profile Repository, Art Recommender*; versie 2.0 ; 1 juli 2011

User Profile Repository	Versie: 1.3
Functioneel Ontwerp	Datum: 18-1-2012

Globale Architectuur

CATCHPlus wil voorzien in meerdere algemene diensten die elkaar onderling versterken. Twee van deze algemene diensten zijn de User Profile Repository en de ZieOok recommendations. In de visie van GridLine biedt het gebruik van open standaarden en een open architectuur de flexibiliteit die nodig is om binnen CATCHPlus nieuwe diensten aan te bieden en bestaande diensten te vervangen.

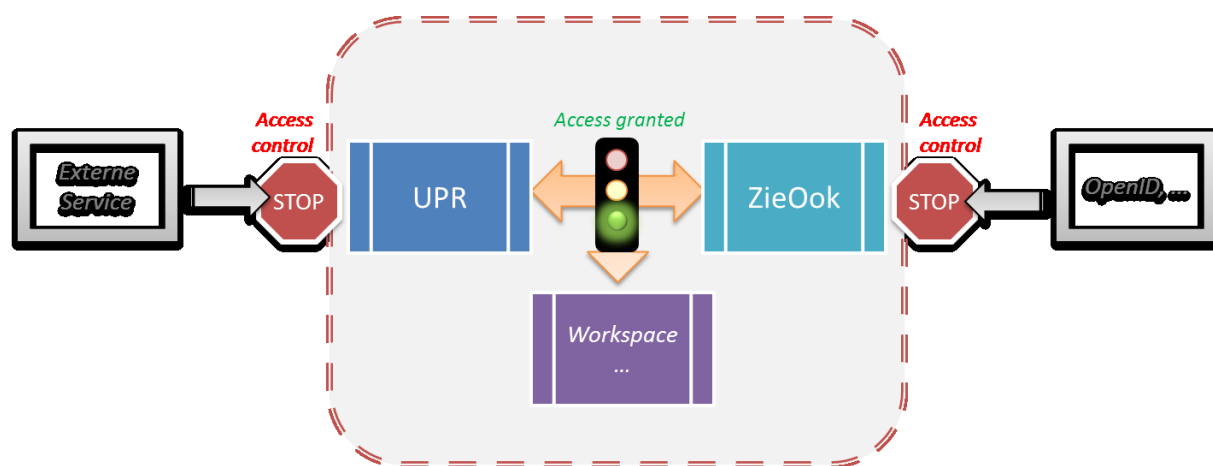
Verantwoordelijkheden & vertrouwen

Een cruciaal onderdeel van onze architectuur-visie is dat van ieder systeem in de architectuur de eigen verantwoordelijk moet zijn beschreven. Gedeelde verantwoordelijkheden zijn uit den boze. Systemen mogen taken delegeren aan andere systemen, maar dat ontslaat het delegerende systeem niet van de eigen verantwoordelijkheid.

Leverende systemen zijn bevoegd zelf te bepalen welke diensten zij beschikbaar stellen en op welke wijze. Afnemende systemen kunnen functionele eisen stellen aan de diensten van een leverend systeem. Indien een leverend systeem vereiste diensten niet kan en niet wil leveren, zal het systeem de taak moeten delegeren aan een ander systeem.

De architectuur van CATCHPlus veronderstelt een gezamenlijk domein waarin de diensten elkaar kennen¹ en vertrouwen en op basis van vertrouwen gegevens uitwisselen. Deze architectuurkeuze maakt het eenvoudig op een gecontroleerde wijze nieuwe diensten toe te voegen.

Indien een service vanuit het CATCHPlus-domein een verzoek stuurt aan een andere service binnen het domein, wordt dit verzoek gehonoreerd. Voor verzoeken van services buiten het domein is expliciete toestemming van die externe service vereist.



Applicatie landschap

Binnen dit project zijn de onderstaande systemen betrokken.

- **User profile repository:** verantwoordelijk voor authenticatie van eindgebruikers, beheert gebruikersprofielen en accounts, en biedt single-sign-on functionaliteit binnen CATCHPlus.
- **ZieOok recommender:** verzorgt aanbevelingen bij collectiestukken op basis van intrinsieke en extrinsieke eigenschappen, biedt collectiebeheerders mogelijkheid aanbevelingen te

¹ Identificatie van services gebeurt op basis van zogenaamde secret-keys.

User Profile Repository	Versie: 1.3
Functioneel Ontwerp	Datum: 18-1-2012

beheren en registreert door gebruikers aangegeven voorkeursobjecten (“ratings”).

- **“OpenID”-providers²**: bieden authenticatie volgens OpenID- en vergelijkbare standaarden (OAuth, Facebook-connect).

² In dit document wordt de term OpenID-provider altijd in deze brede betekenis gebruikt. Waar enkel en alleen OpenID wordt bedoeld wordt dit expliciet vermeld.

User Profile Repository	Versie: 1.3
Functioneel Ontwerp	Datum: 18-1-2012

Uitgangspunten

Gebruikers

Het project kent drie soorten gebruikers:

- **Collectieaanbieder**
 - Een organisatie die een collectie via internet aanbiedt en daarbij gebruik wil maken van de services van CATCHPlus. Een Collectieaanbieder zal doorgaans een collectie in een collectiebeheersysteem hebben en een website waar deze collectie wordt aangeboden.
- **Bezoeker**
 - Een bezoeker van de website van een collectieaanbieder. Als de bezoeker zich aanmeldt bij CATCHPlus via de website dan hebben we het over een **geregistreerde bezoeker**.
- **Beheerder**
 - Een gebruiker met speciale administratieve rechten om de CATCHPlus systemen te beheren.

In de conceptvorming voor het Amsterdam Museum wordt uitgegaan van de rollen: toerist, amsterdammer en onderzoeker voor de bezoekers. Deze rollen zijn meer gericht op het Amsterdam Museum specifiek en spelen in het onderwerp geen rol van betekenis.

Usability tests

Om een eerste indruk te krijgen van het gebruikersgedrag rondom de beoogde functionaliteit is een gebruikerstest uitgevoerd met verschillende medewerkers van het Amsterdam museum. De test bestond uit algemene vragen, een gebruikerstest op een bestaand platform (Youtube, Vimeo of Amazon) en een gebruikerstest op een eerste generatie wireframes.

Het is belangrijk te onthouden dat een gebruikerstest geen wetenschappelijk onderzoek is, maar slechts dient om de ontwerper inzicht te verschaffen in zijn gebruikers en een gesprek tussen de twee tot stand te brengen. Een usability test leidt nooit tot harde conclusies. Evengoed zijn de volgende conclusies gemaakt op basis van indrukken uit deze test en literatuuronderzoek:

- Facebook is verreweg het meest gebruikte sociale netwerk.
- Onder de getestte gebruiker was weinig animo voor het raten van kunststukken (of überhaupt voor het raten van online items). De facebook "like" functie wordt wel veel gebruikt. Ook als de site in kwestie een eigen rating functie biedt, hebben veel gebruikers de voorkeur voor een facebook "like".
 - Gebruikers die graag een rating geven zijn zeldzaam, maar bestaan wel. Deze gebruikers geven de voorkeur aan een gedetailleerde rating (bijvoorbeeld tien halve sterren).
- Het terugzien van gegeven ratings (waardoor ratings een soort favorieten worden) wordt als een nuttige functie beschouwd.
- Als het geven van een rating de enige functie is die mogelijk wordt gemaakt door registratie, zullen weinig gebruikers de moeite nemen om zich te registreren. Mogelijkheden voor andere functies die in vervolgetrajecten geïmplementeerd kunnen worden, worden beschreven in het document *Toekomstige Functionaliteit*. Binnen de scope van dit project is het belangrijk om de registratie zo simpel mogelijk te maken, en te zorgen dat de bestaande functionaliteit voor gebruikers zo nuttig mogelijk is.
- De doelgroep van dit project (kunstcollecties) verandert de betekenis van ratings enigszins

User Profile Repository	Versie: 1.3
Functioneel Ontwerp	Datum: 18-1-2012

ten opzichte van normale sociale sites. Bij een kunstvoorwerp of een ander museumstuk is een negatieve rating minder toepasselijk dan bij een YouTube-video. Een rating op een museumstuk gaat meer uit van een persoonlijke mening. De kans klein dat een museumstuk “objectief” als slecht kan worden gezien, omdat er al een selectie door een curator aan vooraf is gegaan. De rating op een museumsite geeft aan dat het stuk voor de huidige gebruiker positief of nuttig of betekenisvol is. Het is de vraag of een negatieve rating überhaupt toepasselijk is.

- Als symbool voor ratings hebben we een hartje, een duimpje en een sterretje getest. Het duimpje werd gezien als het meest conventioneel, en het hartje als het meest toepasselijk.
 - Omdat het niet ondenkbaar is dat de widgets gebruikt gaan worden in combinatie met facebook knoppen, gaat onze voorkeur uit naar het hartje.
- Als ratingsysteem hebben we een binaire rating (duimpje omhoog/omlaag), een like-knop en een vijfsterrenrating getest.
 - Er was geen duidelijke voorkeur onder de testers. We geven zelf de voorkeur voor de like-knop omdat dit minimaal denkwerk vereist van de gebruiker en omdat het de nadruk legt op de functie van favorieten. Onze verwachting is dat een like-mechanisme tot de meeste ratings zal leiden.³

³ Voor de kwaliteit van de recommendations is de granulariteit van de ratings niet van belang. Alleen het feit dat een gebruiker een rating heeft gegeven is genoeg informatie om tot een goede recommendation te komen.

Entiteiten, taken, paden en rollen

Het systeem kan ruwweg uitgesplitst worden in de entiteiten die de gebruikers kunnen manipuleren, de taken die de gebruikers uit kunnen voeren, de paden die de gebruikers door de applicatie kunnen volgen, en de verschillende gebruikersrollen die aangeven welke operaties door welke gebruiker uitgevoerd mogen worden.

Dit hoofdstuk is bedoeld als illustratie van het systeem en de gebruikte terminologie. De rollen en entiteiten worden hieronder benoemd. Een volledige en leidende lijst van functionaliteiten (taken en paden) is te vinden in het hoofdstuk *Use-cases en vereiste functies*.

Entiteiten

- **Widget⁴**
 - Javascript code die toegevoegd kan worden aan de pagina van een collectiestuk. Dit project biedt vier widgets voor in-/uitloggen, populariteit tonen, ratings geven en recommendations tonen.
- **Collectiebeheerder**
 - Een collectiebeheerder is een instantie die een collectie aanbiedt via internet en daarbij de widget gebruikt.
- **Collectie**
 - Iedere collectiebeheerder biedt één collectie aan, bestaande uit collectiestukken.
- **Collectiestuk**
 - Een collectiestuk bestaat uit een beschrijving in sleutel-waarde paren. Extra structuur in de collectie (thesauri, trefwoorden, categorieën) wordt niet meegenomen.
- **Profiel**
 - **Extern profiel**
 - Dit wordt aangemaakt voor een bezoeker die zich met een externe (OpenID) provider heeft aangemeld.
 - **Lokaal profiel**
 - Dit wordt aangemaakt voor een bezoeker die zich registreert.
- **Rating**
 - Een rating wordt door een bezoeker gegeven aan een collectiestuk. De rating bevat geen extra informatie, d.w.z. de ratings fungeren als een like-knop. (De bezoeker kan alleen aangeven dat ze iets mooi vindt, niet hoe mooi ze iets vindt.)
- **Recommender**
 - Op een collectie kunnen een of meer recommenders worden gedefinieerd. Een recommender levert een (grote) lijst van relevante collectiestukken op. Doorgaans is de aanroeper niet in de volledige lijst van collectiestukken geïnteresseerd. Manieren om de lijst te beperken zijn een top- of randomselectie.
 - **Item-based recommender**
 - De recommender levert collectiestukken die lijken op een gegeven collectiestuk.
 - **User-based recommender**
 - De recommender levert collectiestukken die een rating hebben gekregen

⁴ In normaal taalgebruik is een widget een veel gebruikt UI-element, zoals een knop, een voortgangsbalk of een dialoogvenster. Op het web gaat het vaak om onderdelen van een website die door een externe site gegenereerd worden. Bijvoorbeeld een twitter-, facebook- of flickr-widget.

User Profile Repository	Versie: 1.3
Functioneel Ontwerp	Datum: 18-1-2012

van gebruikers die lijken op de gegeven gebruiker.

- **Aanbeveling**
 - **Persoonlijke aanbeveling**
 - Een aanbevolen collectiestuk gebaseerd op de gelijkenis van de gebruiker met andere gebruikers.
 - **Collectiestuk aanbeveling**
 - Een aanbevolen collectiestuk gebaseerd op de gelijkenis met een gegeven collectiestuk.

Rollen

- **Anonieme bezoeker**
 - De anonieme bezoeker kan zich registreren, krijgt de populariteit te zien, een inactieve “like” knop en recommendations.
- **Geregistreerde bezoeker**
 - De geregistreerde bezoeker kan op de “like” knop klikken, en krijgt een overzicht van de items waarvoor hij op die knop heeft gedrukt.
 - De geregistreerde bezoeker kan zijn profielinformatie beheren op UPR.
- **Collectiebeheerder**
 - De collectiebeheerder kan de recommender tunen via het ZieOok platform.
- **Beheerder**
 - De beheerder heeft specifieke rechten om administratieve taken op de CATCHPLus systemen uit te voeren.

User Profile Repository	Versie: 1.3
Functioneel Ontwerp	Datum: 18-1-2012

User stories

Een user story is een tekstuele beschrijving hoe het systeem gebruikt kan worden.

User Story 1

Sjoerd van Vliet is 23 jaar en woonachtig te Utrecht. Dit jaar gaat hij van start met een studie natuurwetenschap aan de Universiteit van Amsterdam. Hij wil graag meer te weten komen over de stad Amsterdam en haar geschiedenis. Via Google komt hij uit op de website van Amsterdam Museum (<http://www.amsterdammuseum.nl>).

Hij kan duidelijk kiezen tussen de verschillende thema's *evenementen*, *tour*, *tentoonstellingen* en *collectie* die in de hoofd-navigatie van de website zijn opgenomen.

Daaronder ziet Sjoerd informatie met visuals over de lopende tentoonstellingen, nieuws en toekomstige evenementen. Alhoewel Sjoerd overal op de website kan rondsurfen zonder zich aan te melden, logt hij met zijn Twitter account in op de website. Op deze manier kan Sjoerd eventuele vondsten delen met zijn eigen netwerk of kan hij interessante plekjes op de website markeren voor later gebruik. Middels de knop 'inloggen', waar de volgend id-suppliers in op zijn genomen:

- Facebook;
- Twitter;
- Gmail;
- Hyves.

Sjoerd kiest voor Twitter en de na een keuze te hebben gemaakt, vraagt de Twitter applicatie of hij de website van het Amsterdam Museum toegang wilt verlenen tot zijn profiel. Sjoerd geeft hier een akkoord op en is nu met zijn Twitter account aangemeld op de website van het Amsterdam Museum.

Tijdens zijn onderzoek kiest Sjoerd het thema *collectie* en geeft de zoekmachine van de website de opdracht om naar het steekwoord 'Delft' te zoeken. Op basis van de zoekresultaten wordt onder meer een oud stuk krant getoond met de titel 'Tekstfragment over de ontploffing van de kruittoren te Delft, 1698'. Dat is toevallig, want Sjoerd maakt in het kader van zijn studie onder meer gebruik van Vlam Emissie Spectroscopie. Sjoerd geeft aan dat hij het item interessant vindt middels de opgenomen knop 'like'. Sjoerd klikt op nog een aantal items uit de zoek-resultaten en geeft zijn waardering voor de relevante items.

De 'recommendation widget' toont bij ieder bekeken item een lijst met vergelijkbare items die mogelijk van belang kunnen zijn en die Sjoerd niet heeft gewaardeerd. De 'recommendation widget' toont constant 5 items en geeft Sjoerd de mogelijkheid om deze items te benaderen door ze aan te klikken. Als Sjoerd terugkeert bij een eerder bezocht item, ziet Sjoerd andere vergelijkbare items.

Sjoerd is na 90 minuten klaar met zijn onderzoek op de website en wil zien welke items hij nu als relevant had gemarkeerd. Sjoerd gaat naar zijn favorieten naast de knop 'uitloggen'. De items die Sjoerd heeft gemarkeerd middels de like-knop staan hier onder elkaar opgesomd, zodat Sjoerd nu en later een overzicht heeft over de items die relevant zijn.

Sjoerd ziet ook de optie 'bekijk je profiel' en klikt op de button. Hij ziet vervolgens de volgende informatie:

- Profiel;
- Geschiedenis (surfgedrag/historie/);
- Aanbevelingen.
- Favorieten

User Profile Repository	Versie: 1.3
Functioneel Ontwerp	Datum: 18-1-2012

Sjoerd klikt op 'Profiel' en ziet dat hij met zijn Twitter account is aangemeld bij de volgende instellingen, waar hij eerder toestemming voor heeft gegeven om toegang te verlenen tot zijn Twitter profiel:

Profiel

Veld	
Naam instelling	Amsterdam Museum
Locatie instelling	www.amsterdammuseum.nl/upr-id
Meest recente aanmelding	4 september 2011 om 11:43
Toegang verleend met volgende id-supplier	Twitter

Sjoerd klikt op 'Geschiedenis' en ziet de volgende gegevens inzake zijn geschiedenis.

Geschiedenis

Veld	
Naam instelling	Amsterdam Museum
Locatie instelling	www.amsterdammuseum.nl/upr-id
Meest recente aanmelding	4 september 2011 om 11:43
Toegang verleend met volgende id-supplier	Twitter
Bekijk volledig overzicht	[new page overview]

Bij het onderdeel 'Aanbevelingen' ziet Sjoerd de aanbevelingen die het systeem genereerde en die hij heeft gevolgd. De aanbevelingen zijn gekoppeld aan het item waarop zij betrekken hadden.

Aanbevelingen

Bij item	Aanbeveling URI	Aanbeveling Titel	Tijdstip aanbeveling
Tekstfragment over de ontplofing van de kruittoren te Delft, 1698	http://collectie.amsterdammuseum.nl/dispatcher.aspx?action=search&database=ChoiceCollect&search=prirref=20370	Drinkhoorn van het St. Joris- of Voetboogschuttersgilde, 1566	07-10-2011 – 12:34:56
Tekstfragment over de ontplofing van de kruittoren te Delft, 1698	http://collectie.amsterdammuseum.nl/dispatcher.aspx?action=search&database=ChoiceCollect&search=prirref=58195	Oproer te Krakau, soldaten strijden tegen katholieke studenten - 1647, 1698	07-10-2011 – 12:37:30
Tekstfragment over de ontplofing van de kruittoren te Delft, 1698	http://collectie.amsterdammuseum.nl/dispatcher.aspx?action=search&database=ChoiceCollect&search=prirref=58196	Ontploffing van de kruittoren te Delft	07-10-2011 – 12:34:56
[title]	[http://hostname.etc]	[title]	[timestamp]

User Profile Repository	Versie: 1.3
Functioneel Ontwerp	Datum: 18-1-2012

Daaronder ziet Sjoerd zijn favorieten (door hemzelf expliciet afgeven 'likes'). Hij ziet dat hij één aanbeveling ook als favoriet heeft gemarkeerd. Hij kan zijn favorieten aanpassen.

Favorieten

Locatie/URI	Titel	Tijdstip rating	Verwijder
http://collectie.amsterdammuseum.nl/dispatcher.aspx?action=search&database=ChoiceCollect&search=preref=58197	Tekstfragment over de ontplofing van de kruittoren te Delft, 1698	07-10-2011 – 12:34:56	Ja/nee
http://collectie.amsterdammuseum.nl/dispatcher.aspx?action=search&database=ChoiceCollect&search=preref=58195	Oproer te Krakau, soldaten strijden tegen katholieke studenten - 1647, 1698	07-10-2011 – 12:37:30	Ja/nee
http://collectie.amsterdammuseum.nl/dispatcher.aspx?action=search&database=ChoiceCollect&search=preref=79581	Handschoen	07-10-2011 – 12:40:03	Ja/nee
[http://hostname.etc]	[title]	[timestamp]	Ja/nee

Sjoerd is erg tevreden over wat hij op de website van het Amsterdam Museum heeft gezien en neemt zich voor de website vaker te bezoeken.

User Story 2

Sjoerd van Vliet (23 jaar, woonachtig te Utrecht) kent de website van het Amsterdam Museum (<http://www.amsterdammuseum.nl>) omdat hij er eerder is geweest. Sjoerd heeft bij die eerdere bezoeken collectiestukken die hij interessant vond positief beoordeeld. Hij gaat naar de startpagina van de website en logt in met zijn Twitter-account. Sjoerd is direct vanaf de startpagina van het Amsterdam Museum ingelogd.

Omdat Sjoerd een bekende gebruiker is biedt de startpagina naast de standaard indeling van thema's (evenementen, tour, tentoonstellingen en collectie) en de hoofd-navigatie ook persoonlijke aanbevelingen voor Sjoerd. Sjoerd heeft deze functionaliteit niet eerder gezien, maar herkent het principe van aanbevelingen van eerdere bezoeken toen hij door de collectie van het Amsterdam Museum grasduinde. De '*recommendation widget*' voor persoonlijke aanbevelingen toont 5 items en geeft Sjoerd de mogelijkheid om deze items te benaderen door ze aan te klikken.

Zijn oog valt direct op een leuke aanbeveling van de prent *Romeinsche poort aldaar, 1679*. Sjoerd klikt op de aanbeveling en komt op de prent uit de collectie van Jan Luyken terecht. De '*recommendation widget*' toont bij deze prent een lijst met vergelijkbare items en die niet tot Sjoerds favorieten behoren, waaronder *Glasplaten van een transparant (afb. gebouw (Binnenhof Den Haag?))*. Sjoerd markeert de prent *Romeinsche poort aldaar, 1679* als favoriet omdat hij de prent interessant vindt en neemt zich voor om de volledige prentencollectie van Jan Luyken later verder te bekijken. Sjoerd besluit nu eerst de aanbeveling *Glasplaten van een transparant (afb. gebouw (Binnenhof Den Haag?))* te volgen.

Sjoerd blijft zo een half uur rondneuzen op de website. Sjoerd is erg tevreden over wat hij op de website van het Amsterdam Museum heeft gezien en vraagt zich af of andere musea vergelijkbare mogelijkheden bieden. Hij besluit eens een snelle blik te werpen op de website van het Rijksmuseum en ziet daar op de startpagina de inlog-widget die hij van het Amsterdam Museum kent. Sjoerd heeft nu een afspraak met vrienden, maar neemt zich voor de volgende keer eens in te loggen op de website van het Rijksmuseum.

User Profile Repository	Versie: 1.3
Functioneel Ontwerp	Datum: 18-1-2012

Use-cases en vereiste functies

Use-cases zijn korte scenarioschetsen rond de te bouwen applicatie. De applicatie wordt zo ingericht dat aan de belangrijkste use-cases het makkelijkst te voldoen is. De minder belangrijke use-cases krijgen een minder prominente plaats. Aan sommige use-cases wordt bewust geen invulling gegeven. De use-cases zijn geschreven vanuit de gebruiker, en doen zo min mogelijk aannames over hoe het systeem wordt ingevuld.

De **vereiste functies** zijn een fijnere opsomming van de functies die het systeem moet kunnen verrichten of die een gebruiker met het systeem moet kunnen verrichten.

Vanuit de functionaliteiten wordt later de eerste generatie tickets (opdrachten aan de programmeurs) opgesteld. Vanuit de use-cases wordt de eerste generatie testscenario's (opdrachten voor de testers) geschreven.

Overzicht use-cases

De use-cases gaan uit van de entiteiten en gebruikersrollen zoals hierboven beschreven.

Vereiste functies

1. Een anonieme bezoeker kan zich registreren via de site van een collectiebeheerder op de User Profile Repository
2. Een anonieme bezoeker kan zich registreren met verschillende bestaande profielen
 - a. Facebook
 - b. Google
 - c. Hyves
 - d. Twitter
3. Een geregistreerde bezoeker kan inloggen en uitloggen op de site van een collectiebeheerder
4. Een geregistreerde bezoeker kan inloggen en uitloggen op de site van de User Profile Repository om zijn geregistreerde gegevens in te zien.
5. Een collectiebeheerder kan inloggen en uitloggen op het dashboard van ZieOok.
6. Een collectiebeheerder kan op ZieOok een recommender aan maken voor zijn collectie.
7. Een collectiebeheerder kan op ZieOok javascript-code voor de widgets van zijn site ophalen:
 - a. Een widget waarmee een bezoeker zich kan registreren (evt met een bestaand profiel), in kan loggen en uit kan loggen
 - b. Een widget waarmee een bezoeker de populariteit van een collectiestuk kan zien (op basis van ratings en views, gewogen over de tijd)
 - c. Een widget dat voor een collectiestuk soortgelijke (onbekende) collectiestukken laat zien (op basis van een recommender, d.w.z. gelijkenis van collectiestukken of gelijkenis van gebruikers).
 - d. Een widget waarmee de gebruiker een rating kan geven aan het getoonde collectiestuk
8. Een website-beheerder kan javascript-code voor de widgets op zijn site plaatsen.
9. Een collectiebeheerder kan ZieOok statistieken over het gebruik van zijn collecties en recommenders inzien.
10. Een beheerder kan inloggen en uitloggen op de site van de User Profile Repository om administratieve taken uit te voeren.

User Profile Repository	Versie: 1.3
Functioneel Ontwerp	Datum: 18-1-2012

Niet-ondersteunde functies

Sommige use-cases worden expliciet **niet** ondersteund. Ze worden hier beschreven om misverstanden te voorkomen. Voor deze functionaliteit is een vervolgproject noodzakelijk.

Zie ook het document *Toekomstige Functionaliteit* ([1]) voor voorgestelde vervolgtrajecten.

1. Reacties
2. Avatars
3. Metadatacorrecties
4. Zoekfunctionaliteit
5. Social sharing
6. Automatische collectie import

Niet-functionele eisen

Sommige eisen aan het systeem zijn niet in use-cases uit te drukken. Deze niet-functionele eisen worden hier apart genoemd.

Standaarden, interfaces en gebruik

- Een website-beheerder kan middels CSS-aanpassingen de widgets voor de eigen website stylen.
- Gebruiksvriendelijk en eenvoudig te bedienen dashboard voor beheer en monitoring.
- Gebruik van open source en open standaarden is een vereiste.
- Maatwerk componenten worden met de doelstelling van open source gemaakt.

Omvang en schaalbaarheid

- UPR gaat uit van de volgende capaciteit bij ZieOok recommendation engine:
 - 20 REST-calls gelijktijdig
 - 200 sessies parallel
 - response op REST calls: maximaal 250ms (read)
 - response op REST calls: minimaal 2000ms (create, update, delete)
- De UPR en ZieOok dienen schaalbaar te zijn op basis van algemeen gebruik.
 Bij forse groei zal de capaciteit uitbreidbaar moeten zijn zonder dat UPR of ZieOok moet worden aangepast. De schaalbaarheid wordt gegarandeerd door uitbreiding van HW/CPU processing.
- UPR en ZieOok moeten modulair ontworpen worden om redenen van hergebruik en mogelijk toekomstige uitbreidingen.
- UPR en ZieOok zijn dusdanig ontworpen dat het voorspelbaar blijft functioneren en reageren ondanks veranderende en/of onvoorziene interne of externe omstandigheden.

Logging en documentatie

- UPR en ZieOok zijn voorzien van duidelijke en complete logging / foutafhandeling.
- Gegenereerde data moet dusdanig zijn opgeslagen dat het maken van back-ups mogelijk is.
- Beschikbaarheid van documentatie voor functioneel en technisch beheer door derden.
- Beschikbaarheid van documentatie inzake de architectuur en service interfaces.
- Beschikbaarheid van release notes bij opleveren van een release.
- Beschikbaarheid van installatie documentatie.

User Profile Repository	Versie: 1.3
Functioneel Ontwerp	Datum: 18-1-2012

Beveiliging

- Web-based toegang tot beheer en monitoring functionaliteit ten behoeve van beheerders geschiedt na authenticatie en via beveiligde verbindingen.
- De eindgebruikers zijn eigenaar van hun profielgegevens.
- Toegang tot profielgegevens van eindgebruikers is beperkt op basis van *need-to-know*. (Alleen de beheerder van CATCHPlus heeft toegang tot profielgegevens van eindgebruikers.)

User Profile Repository	Versie: 1.3
Functioneel Ontwerp	Datum: 18-1-2012

Gebruikersidentificatie en authenticatie

Voor identificatie, authenticatie en autorisatie van gebruikers moet altijd een balans gezocht worden tussen gebruiksgemak en veiligheid. In dit hoofdstuk komen met name de (acceptabele) beveiligingsrisico's aan bod die aan de gevolgdde gebruikersidentificatie en authenticatie te grondslag liggen.

Gebruikersidentificatie

Het e-mailadres dient als identificatie van gebruikers. Verschillende accounts met hetzelfde e-mailadres zijn niet toegestaan⁵. E-mailadressen zijn immers naar uniek personen of organisaties te herleiden.

De UPR biedt twee mogelijkheden voor registratie en toegang:

- Lokale UPR-account
- OpenID-provider of vergelijkbaar, te weten Facebook, Google, Hyves, Twitter

Beide vormen van registratie en toegang zijn gelijkwaardig en zelfs inwisselbaar, omdat UPR e-mailadressen als identificatie van gebruikers neemt.

Ergo, een gebruiker kan via verschillende OpenID-providers zijn UPR-account benaderen, als die OpenID-providers hetzelfde e-mailadres⁶ publiceren. Indien een gebruiker een lokaal wachtwoord instelt op een UPR-account, kan de gebruiker ook zonder OpenID het UPR-account benaderen.

Beveiligingsrisico's

Het gebruik van e-mailadressen als identificatie brengt enkele beveiligingsrisico's met zich mee:

- Kan het e-mailadres van het lokale account worden vertrouwd?
- Kan het e-mailadres van de OpenID-provider worden vertrouwd?

Het eerste punt wordt bij registratie van een lokaal account afgevangen. Een anonieme gebruiker kan zich registreren met een willekeurig e-mailadres. Naar dit e-mailadres wordt een activeringsemail verzonden. Het account kan pas worden gebruikt nadat het is geactiveerd door de instructies uit de activeringsemail te volgen. Deze controle garandeert dat de eigenaar van het e-mailadres inderdaad het account heeft aangevraagd en de betrouwbaarheid van het e-mailadres als identificatie van de gebruiker.

Het tweede punt veronderstelt een betrouwbare OpenID-provider. Veel OpenID-providers⁷ controleren het e-mailadres van hun gebruikers om zelf het e-mailadres als identificatie van de gebruiker te kunnen beschouwen.

Het is van cruciaal belang dat UPR de OpenID-provider kan vertrouwen. *UPR mag daarom nooit willekeurig OpenID-providers accepteren als authenticatiepartij.*

Een kwaadwillende OpenID-provider kan namelijk eenvoudig toegang tot een willekeurig UPR-account krijgen door het OpenID-protocol te implementeren, en vervolgens het betreffende e-mailadres te publiceren bij die inlogpoging.

Om deze reden is het invoerveld waarin een willekeurige profiel-URL kan worden opgegeven, zoals

⁵ Dientengevolge faalt iedere poging tot registratie indien een account met het opgegeven e-mailadres reeds in UPR bestaat.

⁶ Omdat Twitter geen e-mailadres publiceert, zal Twitter als OpenID-login altijd tot een apart UPR-account leiden. (UPR genereert voor Twitter een dummy e-mailadres in het domein "twitter.upr.nl".)

⁷ Waaronder in ieder geval Facebook, Hyves en Google.

getoond in onderstaand wireframe-fragment dat in eerdere versies van UPR is gerealiseerd, in de definitieve versie verwijderd.



Figuur 1: Beveiligingsrisico "Andere site/profiel-url"

Authenticatie

De OpenID-provider is verantwoordelijk voor de authenticatie van inlogpogingen middels OpenID. Voor lokale toegang is UPR zelf verantwoordelijk voor authenticatie op basis van e-mailadres en lokaal wachtwoord.

Een UPR-account waarvoor een lokaal wachtwoord is ingesteld, accepteert altijd ook een login middels OpenID met hetzelfde e-mailadres. Een UPR-account waarvoor geen lokaal wachtwoord is ingesteld, kan daarentegen alleen middels een OpenID-provider worden benaderd. De ingelogde gebruiker kan evenwel door een lokaal wachtwoord op het UPR-account in te stellen, het account ook lokaal toegankelijk maken.

Beveiligingsrisico's

De koppeling van een lokaal account en een account op basis van OpenID brengt een beveiligingsrisico mee als het e-mailadres voor het lokale account niet gevalideerd is. Dit punt is ondervangen door de activeringsemail waarmee de juistheid van het lokale e-mailadres is gegarandeerd.

Een tweede risico betreft instellen/wijzigen van een lokaal wachtwoord van een account op basis van OpenID. Het wijzigen van een bestaand lokaal wachtwoord vergt het invoeren van dat actuele lokale wachtwoord als extra beveiligingscontrole⁸. Een account op basis van OpenID heeft initieel echter geen lokaal wachtwoord. De gebruiker kan het nieuwe lokale wachtwoord diensgevolge instellen zonder deze extra beveiligingscontrole.

⁸ Stel de gebruiker is weggelopen en heeft zijn computer in onbeveiligde status achtergelaten. Een kwaadwillende neemt achter de computer plaats en probeert het wachtwoord te wijzigen. Omdat ook het actuele wachtwoord moet worden gegeven, zal de kwaadwillende geen wachtwoordwijziging kunnen doorvoeren.

User Profile Repository	Versie: 1.3
Functioneel Ontwerp	Datum: 18-1-2012

Een derde risico betreft de reset van een lokaal wachtwoord. Vanwege veiligheid zijn lokale wachtwoorden versleuteld in de database opgeslagen. Niemand kan uit de versleuteling het oorspronkelijke wachtwoord herleiden. Een gebruiker die zijn lokale wachtwoord vergeet, moet een reset van het wachtwoord aanvragen. Een e-mail met een geheime code wordt naar het betreffende e-mailadres gestuurd. Door de instructies van de e-mail op te volgen logt de gebruiker automatisch eenmalige in op UPR. Omdat de gebruiker het actuele lokale wachtwoord niet weet, kan ook nu het nieuwe lokale wachtwoord zonder de extra beveiligingscontrole worden ingesteld.

Een vierde risico betreft “gecorrumpeerde” lokale wachtwoorden. Aan de versleuteling van een lokaal wachtwoord is zichtbaar of de versleuteling is gecorrumpeerd⁹. Een wachtwoord waarvan de versleuteling is gecorrumpeerd is in principe niet te herstellen. Pogingen om het wachtwoord te wijzigen zullen falen omdat het actuele lokale wachtwoord niet gevalideerd kan worden. Indien de versleuteling is gecorrumpeerd kan de gebruiker het nieuwe lokale wachtwoord dientengevolge instellen zonder de extra beveiligingscontrole.

Laatstgenoemde drie risico’s spelen met name een rol indien gebruikers slecht omgaan met hun accounts. D.w.z. accounts open laten staan op publieke computers en computers in onbeveiligde status onbeheerd achterlaten. De consequenties van deze menselijke fouten zijn vele malen groter wanneer de accounts beheerdersrechten hebben.

Autorisatie

UPR onderkent twee rechtenniveaus voor geïdentificeerde gebruikers: beheerders en overigen (normale gebruikers).

Normale gebruikers kunnen hun profielgegevens (niet zijnde e-mailadres) beheren en hun account in zijn geheel verwijderen¹⁰.

Beheerders hebben daarenboven inzicht in de geregistreerde accounts (maar geen wijzigingsrechten) met de gebruikersstatistieken en de mogelijkheid “rechten” van accounts aan te passen.

- Een beheerder kan een willekeurig account beheerdersrechten geven of onttrekken (ook het eigen account).
- Een beheerder kan een willekeurig account blokkeren of deblokkeren (ook het eigen account).

Op een geblokkeerd account kan niet worden ingelogd.

Beveiligingsrisico's

Omdat een beheerder het eigen account kan blokkeren en de beheerrechten op het eigen account kan intrekken, bestaat het risico dat op UPR geen enkel account beheerrechten kan uitvoeren. (Alleen een systeembeheerder kan deze situatie herstellen via een aanpassing in de database.)

Het blokkeren van een account heeft enkel invloed op het inloggen. Een kwaadwillende gebruiker die nooit uitlogt, ondervindt geen hinder van het blokkeren. (Een herstart van het de applicatie door de systeembeheerder logt evenwel alle gebruikers uit.)

⁹ Mogelijk ten gevolge van een schrijffout naar de database, hardwarefout of moedwillige actie van buitenaf.

¹⁰ Beheerders hebben niet de mogelijkheid accounts van andere gebruikers te verwijderen.

User Profile Repository	Versie: 1.3
Functioneel Ontwerp	Datum: 18-1-2012

Primaire databronnen

Bij een applicatie als deze is datareplicatie onvermijdelijk. Om snel genoeg operaties uit te kunnen voeren moet ieder systeem de data lokaal opgeslagen hebben, een zogeheten *redundante kopie*. Daarom is het van belang om te specificeren welke systemen de primaire databron hebben en welke systemen redundante kopieën hebben.

Als een conflict optreedt—de data in systeem A wijkt af van die in systeem B—dan is het de taak van het systeem met de redundante kopie om dit te rectificeren. Daarnaast is het van belang om te specificeren hoe lang de redundante kopie achter mag lopen op de primaire bron. In dit document wordt een indicatie van de orde van grootte van deze tijdsspanne gegeven.

Een laatste punt dat van belang is, is hoe elementen in de data geïdentificeerd worden. Als de redundante kopie verversd wordt, worden dan de bestaande koppelingen in stand gehouden als nieuwe elementen hetzelfde ID hebben, of als ze dezelfde naam hebben? Dit hangt af van de soort data.

Collectie

Voor de collectie heeft de collectiebeheerder de primaire databron. Deze data wordt periodiek geïmporteerd door het ZieOok-platform.

Gebruikersprofielen

De gebruikersprofielen worden opgeslagen in het UPR-systeem. Voor profielen van OpenID providers is de betreffende OpenID provider de primaire databron.

Voor informatie met betrekking tot het gebruik van een andere CATCHPlus-dienst (zoals ZieOok) is de betreffende dienst de primaire bron.

Ratings

De gegeven ratings worden opgeslagen in het ZieOok platform.

Populariteit

De populariteit van een collectiestuk wordt on-the-fly berekend door het web frontend. Dit gebeurt op basis van informatie uit het ZieOok platform: ratings en views gewogen over tijd.

OpenID Providers

Om het inloggen voor gebruikers te vergemakkelijken zal de UPR als OpenID “relying party” fungeren. Dit betekent dat mensen met een account van een met kleur gemarkeerde “OpenID”-provider (Facebook, Twitter, Google of Hyves) in kunnen loggen. De overige providers zijn in een later stadium wellicht relevant om te ondersteunen. Sommigen ondersteunen geen OpenID, maar wel andere services.

Provider		Opmerkingen
Facebook	Sociaal netwerk	Facebook ondersteunt geen OpenID als provider ¹¹ , wel Facebook Connect, een formaat dat concurreert met OpenID.
Twitter	Microblogging/sociaal netwerk	Ondersteunt geen OpenID, wel OAuth.
LinkedIn	Sociaal netwerk	Ondersteunt geen OpenID, wel OAuth.
AOL	Verschillende services	
Yahoo!	Sociaal netwerk	
LiveJournal	Sociaal netwerk	
MySpace	Sociaal netwerk	
WordPress	Blog site	
Blogger	Blog site	
Google	Verschillende services	
Steam	Games platform	
Hyves	Sociaal netwerk	

¹¹ Wel als *relying party*, maar dat betekent alleen dat mensen zich bij Facebook kunnen registreren met bijv. hun Google account.

User Profile Repository	Versie: 1.3
Functioneel Ontwerp	Datum: 18-1-2012

Datamodel Profielinformatie

Profielinformatie in UPR

De UPR is verantwoordelijk voor het beheer van profielinformatie van gebruikers. Gebruikers zijn vrij deze profielinformatie aan te leveren.

Een profiel bestaat uit de volgende informatie:

- E-mailadres (verplicht)
- Schermnaam (verplicht)
- Persoonsnaam
- Geboortejaar
- Geslacht
- Woonplaats & Land

Gedelegeerde profielinformatie

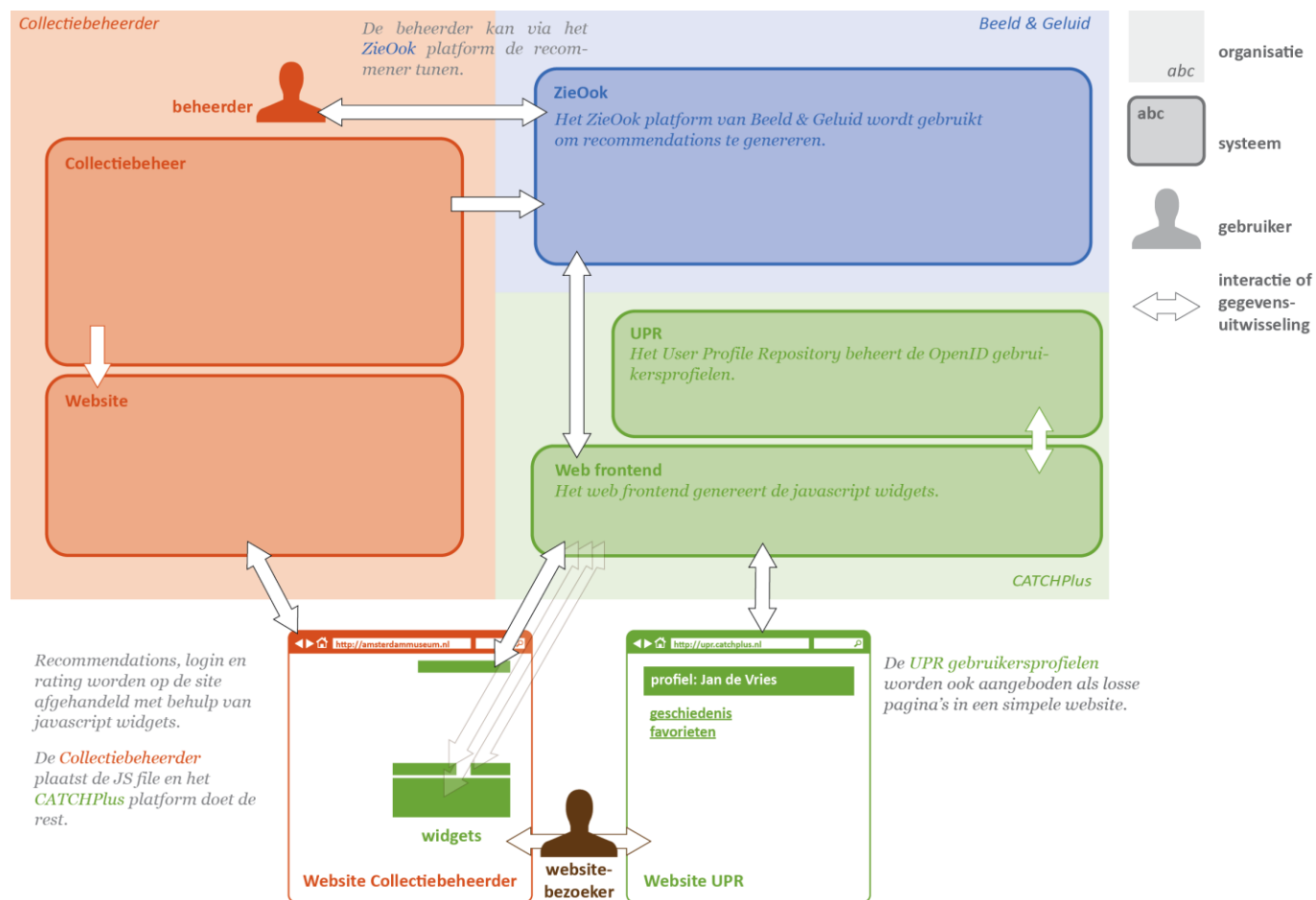
Informatie met betrekking tot het gebruik van een andere CATCHPlus-dienst is opgeslagen bij de betreffende primaire bron. De betreffende dienst dient een eigen identificatie voor de gebruiker te ondersteunen. UPR registreert onder welke identificatie de gebruiker bij de dienst bekend is. Alleen UPR kan het geregistreerde gedrag herleiden naar een specifieke UPR-gebruiker.

Als eis stelt de UPR dat het eigendom van de profielinformatie bij de gebruiker ligt. De betreffende CATCHPlus-dienst dient minimaal de mogelijkheid te bieden de informatie te verwijderen.

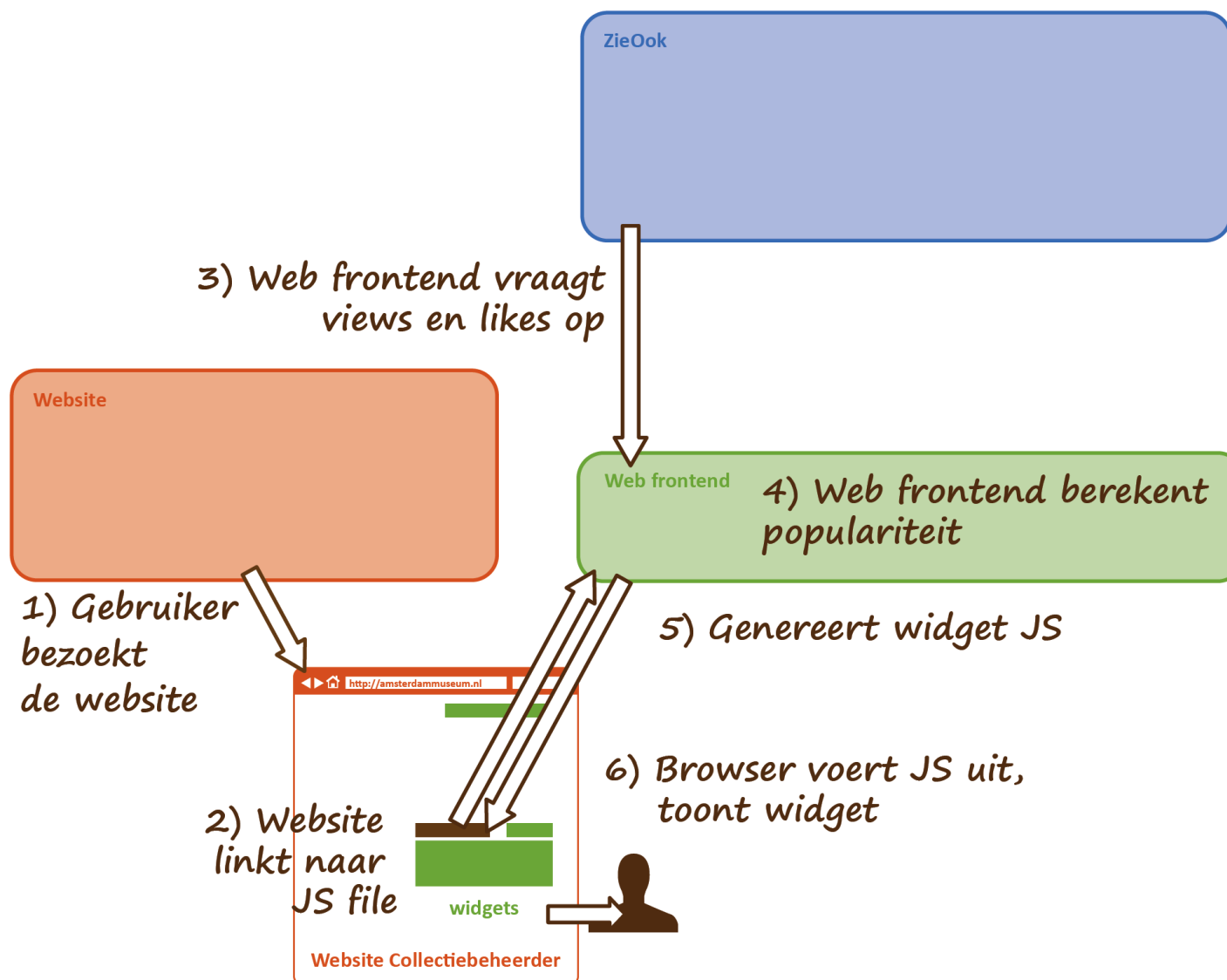
ZieOok gebruikersdata

ZieOok verzamelt gebruikersdata (zijnde de beoordelingen van objecten door gebruikers en opgevolgde aanbevelingen) om gerichte aanbevelingen te produceren. Deze gebruikersdata is feitelijk onderdeel van het profiel van de eindgebruiker. UPR stelt als nadrukkelijke eis aan ZieOok dat deze gebruikersdata verwijderd kan worden.

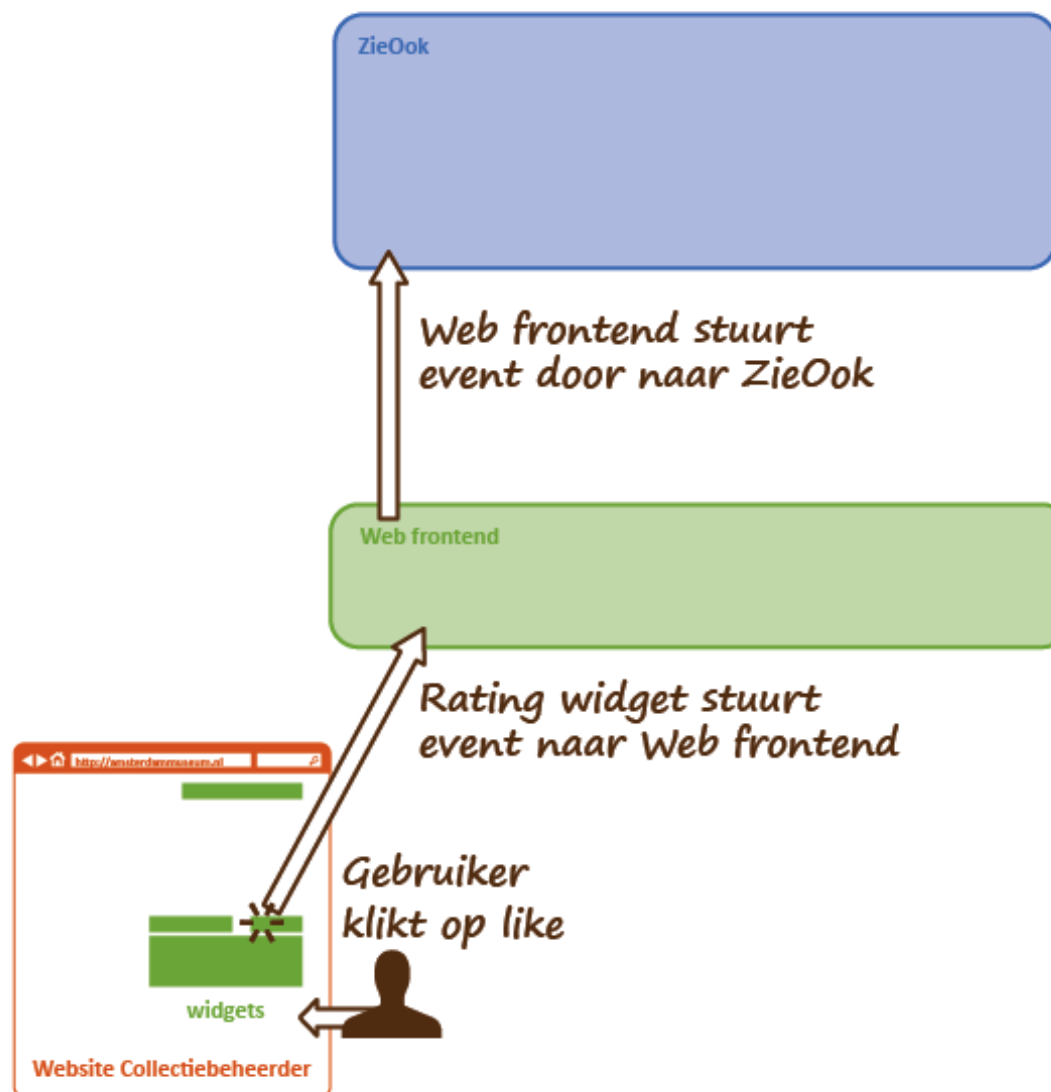
Bijlage 1: Globale workflows



EEN BEZOEKER LAADT DE PAGINA



EEN BEZOEKER GEEFT EEN RATING



Bijlage 2: Inloggen met OpenID

Wanneer een gebruiker met een OpenID-account (of middels vergelijkbare standaard) inlogt, zal de OpenID-provider de gebruiker toestemming vragen gegevens met UPR / CATCHPlus uit te wisselen.

The screenshot shows a web interface for Hyves. At the top, there's an orange header with the Hyves logo and a user profile icon. Below the header, the main content area has a title "Wil je http://upr.gridline.nl/users toestemming geven?" (Do you want to give http://upr.gridline.nl/users permission?). Below the title, there's a paragraph explaining the purpose: "Wil je http://upr.gridline.nl/users toestemming geven om jouw persoonlijke gegevens uit te wisselen met Hyves? Je kunt deze toestemming altijd weer intrekken via mijn account/privacy." (Do you want to give http://upr.gridline.nl/users permission to exchange your personal data with Hyves? You can always revoke this permission via my account/privacy). Below this, there's a diagram showing a box labeled "http://upr.gridline.nl/users" and a Hyves logo (an orange square with a white 'H'). Two blue arrows connect them, with the text "Uitwisselen gegevens" (Exchange data) in the middle. Below the diagram, there's a section titled "Let op! Je gaat gegevens via Hyves uitwisselen (aanpassen)" (Attention! You are going to exchange data via Hyves (adjust)). It says "Je kunt natuurlijk zelf aangeven welke gegevens je wel en niet wilt delen." (You can of course specify which data you do and do not want to share). Below this, there's a list item: "• Overnemen van e-mailadres" (• Take over email address). At the bottom, there's a checkbox labeled "Onthoud mijn instellingen voor deze toepassing" (Remember my settings for this application) which is checked. Below the checkbox, there are two buttons: "Toestemming weigeren" (Deny permission) and "Toestemming geven" (Give permission). A mouse cursor is pointing at the "Toestemming geven" button.

Figuur 2: Voorbeeld - Toestemming Hyves

The screenshot shows a Facebook login page. At the top, there's a title "Aanmelden bij Facebook" (Log in to Facebook). Below the title, there's a paragraph: "Meld je aan om CatchPlus in je Facebook-account te gebruiken" (Log in to use CatchPlus in your Facebook account). Below this, there are two input fields: "E-mailadres:" (Email address) with the value "donald@duckstad.org" and "Wachtwoord:" (Password) with a masked password "••••••••". Below the password field, there's a checkbox labeled "Laat mij aangemeld blijven" (Keep me logged in). Below the checkbox, there's a blue button labeled "Aanmelden" (Log in) and a link "of Registreer je bij Facebook" (or Register on Facebook). Below the button and link, there's a link "Je wachtwoord vergeten?" (Forgot your password?).

Nederlands Frysk English (US) Español Português (Brasil) Français (France) Deutsch Italiano العربية हिन्दी ...

Figuur 3: Voorbeeld - Toestemming Facebook

Na deze toestemming stuurt de OpenID-provider de authenticatiegegevens door en wordt de gebruiker teruggestuurd naar de pagina waar hij vandaan kwam.

User Profile Repository	Versie: 1.3
Functioneel Ontwerp	Datum: 18-1-2012

Wil je <http://upr.gridline.nl/users> toestemming geven?

✓ Gelukt!

Je wordt nu teruggestuurd naar de website waar je gaat inloggen, een ogenblik geduld a.u.b.



[Klik hier](#) als er niks gebeurt.

Figuur 4: Voorbeeld - Doorzetten OpenID-Authenticatie Hyves