Deelrapportage Ontsluiten Maritieme Informatie

Dit document geeft toelichting op de resultaten voor invulling van requirements:

- PTL01.076.000.D05 URL toegankelijk met iSHARE identiteit en documentatie beschikbaar
- PTL01.076.000.D06 URL's (toegankelijk met iSHARE identiteit), pilotresultaten en documentatie beschikbaar

Achtergrond

In het projectvoorstel Dataontsluiting maritieme lading is beschreven hoe de ontwikkelingen van iSHARE passen binnen de strategie van Portbase: Informatie over lading is vaak (concurrentie-) gevoelig, met als gevolg dat voor het delen hiervan er strenge eisen zijn met betrekking tot security en autorisatie.

Als onderdeel van het project Ontsluiten Maritieme Informatie zijn werkzaamheden uitgevoerd op het vlak van IAM (Identity & Access Management). Hiermee wordt invulling gegeven aan het veilig en gecontroleerd data kunnen delen. De werkzaamheden beschreven in dit project staan niet alleen, Portbase is met een breed IAM-programma bezig om voor nieuwe en bestaande dienstverlening veranderingen door te voeren. Dit programma is niet alleen technisch van aard maar raakt ook een aantal processen binnen Portbase zoals aanmeldprocessen voor nieuwe klanten, self-service mogelijkheden, aansluitprocessen met klantsystemen etc.

Allereerst beschrijven we welke werkzaamheden zijn uitgevoerd om invulling te geven aan de IAM requirements. In het volgende deel wordt de ontwikkeling van de dataservices waarmee de maritieme informatie wordt ontsloten toegelicht. De ontwikkelingen van IAM worden toegepast voor veilige ontsluiting van deze dataservices en zal gelden als norm voor alle Portbase dienstverlening.

De werkzaamheden aan IAM die relevant zijn voor dit project zijn te verdelen in 3 hoofdactiviteiten:

- Het ontwikkelen van het Community Passport, voor veilige (iSHARE) login tot meerdere logistieke systemen. Het ontwikkelen van System Connect, voor beveiligde verbinding tussen systemen conform iSHARE

Het ontwikkelen van een service om toestemmingen vast te leggen van klanten welke data Portbase mag delen met welke (markt)partij. Om veilig data te delen– conform de iSHARE visie – is een goede implementatie vereist van bovenstaande onderdelen. Het Community Passport zorgt ervoor dat van personen op veilige wijze wordt vastgesteld wie ze zijn. Wanneer data tussen systemen uitgewisseld wordt, is het van belang om dit met System Connect te organiseren tussen systemen die betrouwbaar zijn en een verbinding die veilig is. Tot slot is het voor data-eigenaren (iSHARE: "entitled parties") van belang om zelf regie te houden over *wie*, *wat* mag doen met *welke* data. Hiervoor is een machtigingen- of authorisatieregister van belang. Alleen wanneer alle genoemde schakels goed zijn ingericht kan een datadelen keten daadwerkelijk volledig veilig worden ingericht.

Voor het ontsluiten van Maritieme Informatie is de samenhang van bovenstaande onderdelen als volgt:

- Voordat data gedeeld kan worden moet door de data-eigenaar toestemming worden verleend en de toestemming moet worden vastgelegd
- Toestemming kan alleen worden verleend als de data-eigenaar (iSHARE: entitled party) zich kan identificeren, hier speelt het Community Passport een rol
- Via de Portbase data share manager geeft een data-eigenaar toestemming aan Portbase om met bepaalde doelgroepen (later: specifieke bedrijven) data te delen. Dit wordt vastgelegd in een intern autorisatieregister.
- Overal waar systemen data uitwisselen, moet een beveiligde verbinding worden opgezet

Wanneer er data wordt opgevraagd, controleert de dataservice via het interne autorisatieregister of dit is toegestaan.Portbase ontwikkelt functies, services en richt intern processen in om bovenstaande stappen als nieuwe standaard te maken voor diensten die Portbase ontwikkelt en vermarkt.
Portbase ontwikkelt het Community Passport conform iSHARE technische specificaties vanuit de wens een Identity Provider rol in te kunnen vullen in het stelsel. Ook wil Portbase via System Connect het mogelijk maken om conform iSHARE specificaties een beveiligde verbinding opzetten. Hier is vanuit “data delen in de Versketen” Portbase succesvol de iSHARE conformancetest doorgelopen.

Binnen de scope van dit projectvoorstel zijn werkzaamheden uitgevoerd om het Community Passport in productie te kunnen nemen Ook is er gewerkt aan het kunnen gebruiken van het Portbase Community Passport voor applicaties van derden. Hierbij is het portaal van Havenbedrijf Rotterdam de eerste applicatie waarmee een koppeling is opgezet. . De werkzaamheden worden in het volgende hoofdstuk nader toegelicht.

In het laatste hoofdstuk van dit document wordt beschreven hoe de data vanuit het Port Community Systeem (PCS) ontsloten wordt naar het informatieplatform. Het ontsluiten van de data op het informatieplatform naar de buitenwereld op veilige, gecontroleerde wijze wordt gedaan door gebruik te maken van de functies zoals beschreven in H1.

Ontwikkeling Community Passport

In de volgende paragrafen wordt toegelicht welke werkzaamheden zijn verricht om het Community Passport te realiseren. Hierbij wordt de opgeleverde functionaliteit op een nieuw technologieplatform beschreven, de relatie met de eigen services binnen het PCS en tot slot wordt een project genoemd waarbij het Community Passport door een externe service wordt gebruikt.

Nieuw platform

Om aan te kunnen sluiten bij moderne specificaties zoals die in iSHARE zijn voorgeschreven (OpenIDConnect) is het nodig om een nieuw Identity Management platform in gebruik te gebruiken en af te stappen van de huidige tooling (openAM). Door hierbij over te stappen op technologie van Okta heeft Portbase de beschikking over moderne tooling. Deze nieuwe tooling opent enerzijds de mogelijkheid om een rol te spelen als ID providerom inloggen in andere applicaties mogelijk te maken. Daarnaast biedt het juist mogelijkheden om met externe (iSHARE) ID providers toegang tot het PCS te verkrijgen. Naast de technische ontwikkelingen moeten hiervoor andere belangrijke zaken geregeld worden in processen maar ook op juridisch vlak, hier gaan we in dit document niet verder op in.

Om het inloggen op het PCS met een iSHARE ID technisch mogelijk te maken is de volgende fasering van toepassing:

1. Okta inrichten en configureren conform Portbase requirements
2. PCS dienstverlening aanpassen om Okta te kunnen gebruiken als Identity Service
3. Alle gebruikers PCS migreren van oude omgeving naar nieuwe
4. Techniek & processen inrichten om externe ID providers (conform iSHARE) te ondersteunen

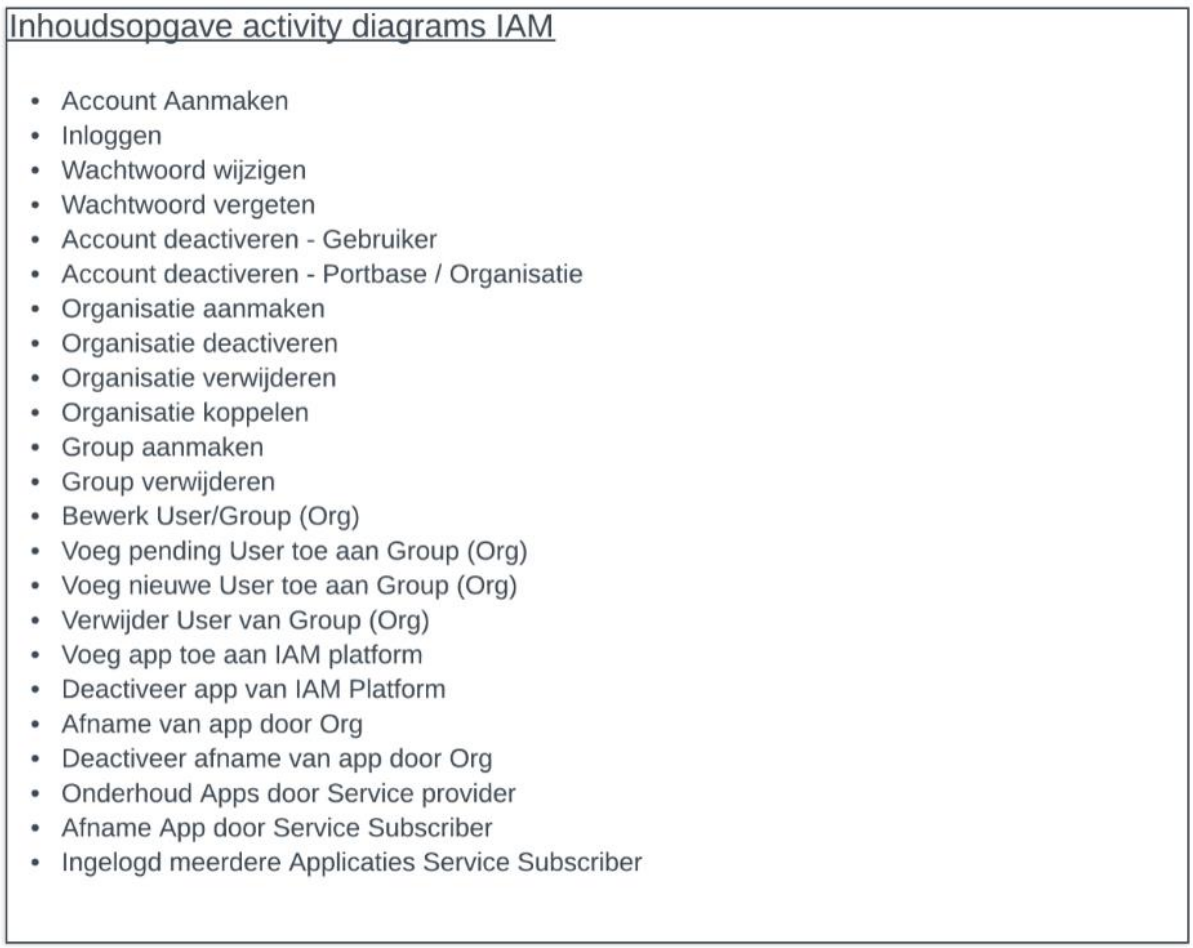
Binnen de scope van dit project is gewerkt aan de stappen 1. en 2, waarbij stap 1 voltooid is. Op dit moment zijn de werkzaamheden om het PCS geschikt te maken voor de nieuwe ID provider nog onderhanden (stap 2). De huidige planning is om eind Q1 te beginnen met de migratie van gebruikers (stap 3). Het realiseren van deze migratie is cruciaal om de stap te kunnen zetten om een externe ID provider toegang te geven tot het PCS. Werkzaamheden hiertoe kunnen in 2020 worden opgepakt.

Beheer van gebruikers, organisaties en services

Het Community Passport vervangt voor Portbase “het Portbase account” waarmee ingelogd wordt in het Port Community Systeem. Om voorbereid te zijn op het gebruik van het Community Passport door applicaties/systemen van derden, moet de beheermodule van Portbase volledig herzien worden. Op hoofdlijnen zijn dit de volgende onderdelen:

- Meer self-service functies voor snellere processen en meer regie klant
- Meer mogelijkheden voor het beheer van gebruikers binnen organisaties
- Beheerfuncties voor het bepalen tot welke services/applicaties een medewerker met het Community Passport toegang kan verkrijgen
- Beheerfuncties voor het verlenen van data-toestemming en zien hoe dit gebruikt wordt (bv audit-log voor toegang)

In figuur 1 is te zien welke beheer- en gebruiksfuncties ontwikkeld worden voor het Community Passport:



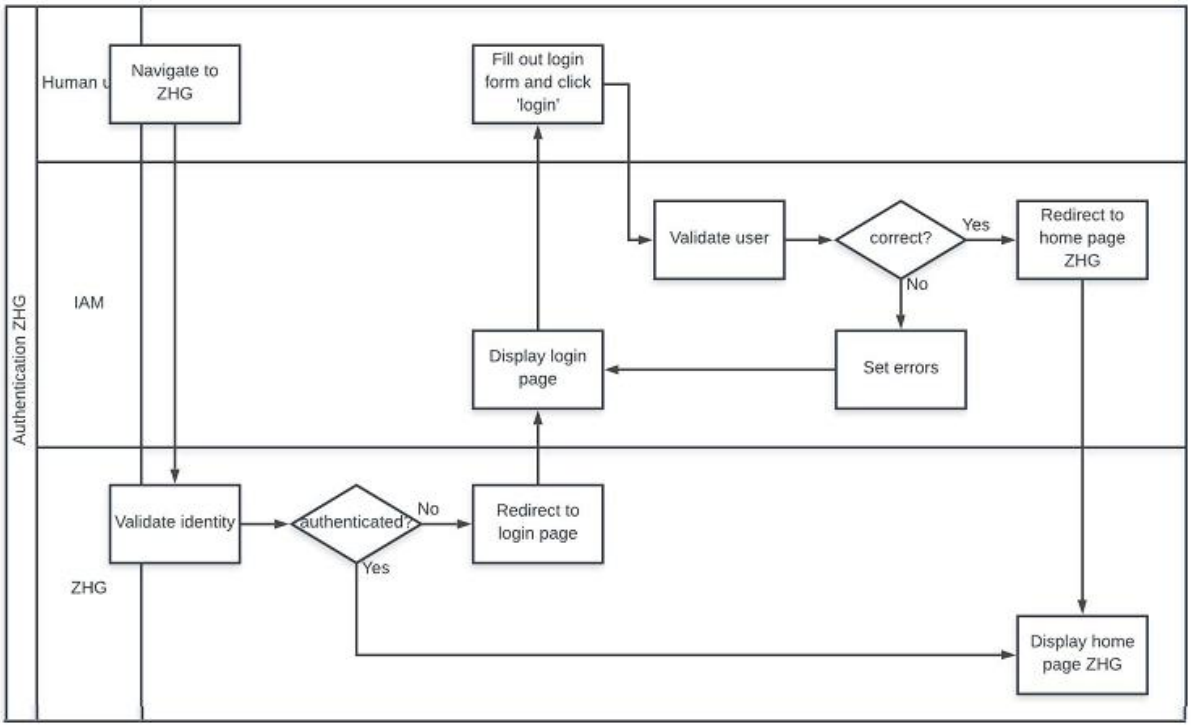
Figuur 1: Overzicht functies voor Community Passport met User, Organisatie en Service Management

Gebruik van Community Passport door services derden

Samen met Havenbedrijven Rotterdam en Amsterdam is een visie uitgesproken om met één digitale identiteit in te kunnen loggen in de Nederlandse havens. Er is gekozen om dit concept in de praktijk

te brengen door een eerste geselecteerde applicatie van het Havenbedrijf Rotterdam aan te sluiten op het Community Passport van Portbase voor een eerste doelgroep.

In dit project wordt het voor het eerst mogelijk om in te loggen in een externe applicatie middels het Portbase Community Passport. Omdat het PCS, de Portbase dienstverlening, het Community Passport nog niet ondersteund is in deze fase nog geen sprake van “Single sign-On”, dit zal uiteraard vanaf het moment van de migratie van gebruikers wél zo zijn. In de tussentijd biedt dit echter een geschikte gelegenheid om de usecase externe login concreet uit te werken, wat parallel kan verlopen aan de andere IAM ontwikkelingen. In Figuur 2 is te zien hoe de flow eruit ziet om met een externe applicatie de authenticatie-functies via Portbase te doorlopen.



Figuur 2: Authenticatie-flow user met externe applicatie

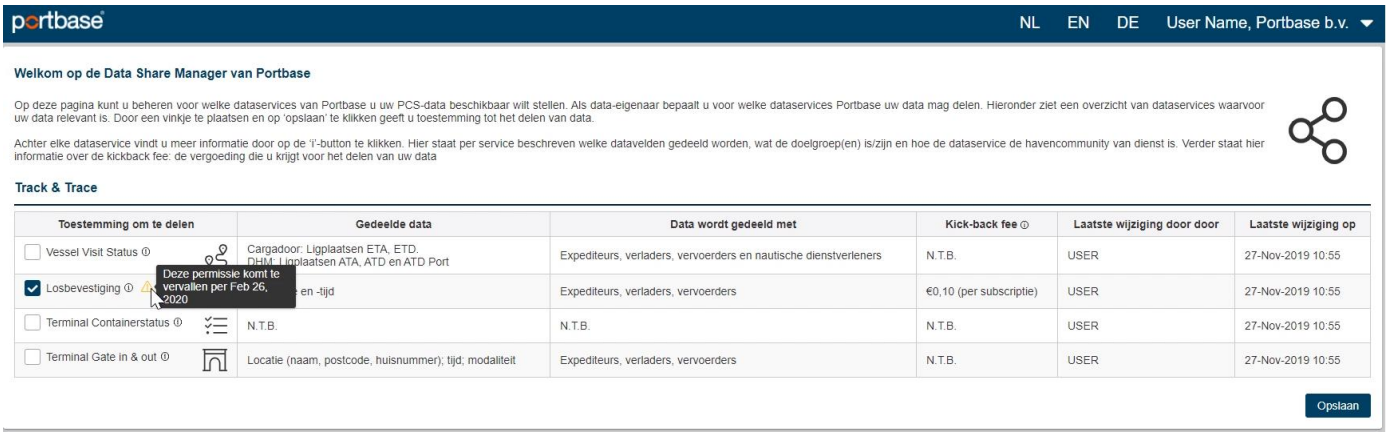
In Bijlage 1 zijn een aantal screenshots te zien die illustreren hoe het beheer van gebruikers binenn organisaties ingericht is. Ook is te zien hoe een gebruiker gebruik maakt van het Portbase Community Passport (hier genoemd IAMConnected) om in te loggen bij de dienst MyPort van Havenbedrijf Rotterdam.

Gebruiken van authorisaties bij datadelen

In het vorige hoofdstuk is toegelicht welke werkzaamheden worden uitgevoerd om het Community Passport te onwikkelen. In onderstaande alineas wordt getoond hoe Portbase voor dataservices de datatoestemming zal vastleggen. Alleen gebruikers met de juiste rechten gekoppeld aan hun Community Passport zullen deze authorsiaties kunnen inzien of muteren.

Vastleggen authorisaties

In project voor het data delen in de vers-keten is reeds gebruik gemaakt van het interne authorisatieregister om per dataverzoek te controleren of de data verzonden mag worden. In dit project was de scope van het data delen nog beperkt; er was sprake van een éénmalige machtiging die aan het begin van het project is vastgelegd. Voor het ontsluiten van de maritieme data is het nodig om voor vele partijen (via self-service) de toestemming te kunnen verlenen maar ook in te kunnen trekken. Om dit mogelijk te maken is de data share manager ontwikkeld. Aan de backend lezen de dataservices bij elke aanroep in het authorisatieregister of data gedeeld mag worden. De Data Share Manager zorgt voor de functies en de schermen om machtigingen te beheren, waaronder het inzien en wijzigen de belangrijkste eerste functie is.
In figuur 3 is een voorbeeld te zien hoe dit voor Portbase datadiensten eruit ziet. Voor het ontsluiten van de maritieme data zal hetzelfde mechanisme worden gebruikt.



Figuur 3: De Data Share Manager

Visie op iSHARE

In dit hoofdstuk is uiteengezet welke werkzaamheden Portbase heeft verricht om de services die ontwikkeld worden volgens iSHARE naar de markt te kunnen brengen. Hieronder vallen niet alleen technische maar ook organisatorische ontwikkelingen. Portbase is in 2019 officieel deelnemer van iSHARE geworden en heeft via een conformance test laten zien dat verbindingen volledig volgens de iSHARE standaard ondersteund worden. Dit betekent echter niet dat alle verbindingen met klantsystemen automatisch aan het iSHARE stelsel zullen voldoen, hiervoor is verdere adoptie van iSHARE binnen de markt uiteraard een belangrijke voorwaarde.

Portbase is vanaf het begin co-creatie partner en staat nog steeds voor het verbeteren van de veiligheid van data delen. iSHARE kan hierin een waardevolle rol spelen. Onder meer via de samenwerking met UCGroup zet Portbase zich actief in om verdere adoptie van iSHARE in de markt te stimuleren. Enerzijds doen we dit door zelf volledig volgens de iSHARE standaard diensten te kunnen leveren. Anderzijds is het cruciaal om in de markt cases te ontwikkelen waar bedrijven door het delen van data nieuwe mogelijkheden krijgen om waarde in de logistieke keten te creëren.

Data ontsluiting lading domein

Dit hoofdstuk beschrijft de werkzaamheden die Portbase heeft uitgevoerd om data uit het lading domein te ontsluiten, zodat deze beschikbaar komt om via datadiensten aan te bieden aan de markt (Deliverable PTL01.076.000.D06). Dit in combinatie met de hierboven beschreven resultaten (community passport, system connect en autorisaties).

Achtergrond

Als gesteld bij aanvang van het project bestaat vanuit de markt een urgente behoefte aan het kunnen koppelen met data en events ten aanzien van de status van lading. Deze data wordt blijvend uitgewisseld via een veelvoud aan procesdiensten, kent een verhoogde gevoeligheid en is derhalve niet voor alle rollen (bestaand en nieuw) in de keten beschikbaar.

Ketens werken hierdoor suboptimaal en innovatieve oplossingen zijn lastig tot niet schaalbaar. Met deze deliverables wil Portbase dit samen met de community doorbreken door in te zetten op het ontkoppelen van data en proces en toepassen van I-share rollen. Gelet op datapositie icm proceslogica en unieke sleutels, is Portbase de enige partij om dit te bewerkstelligen. Hierdoor zijn derden in staat om geautoriseerd data te gebruiken ten behoeve van bijvoorbeeld control towers, plansystemen en/of dashboards.

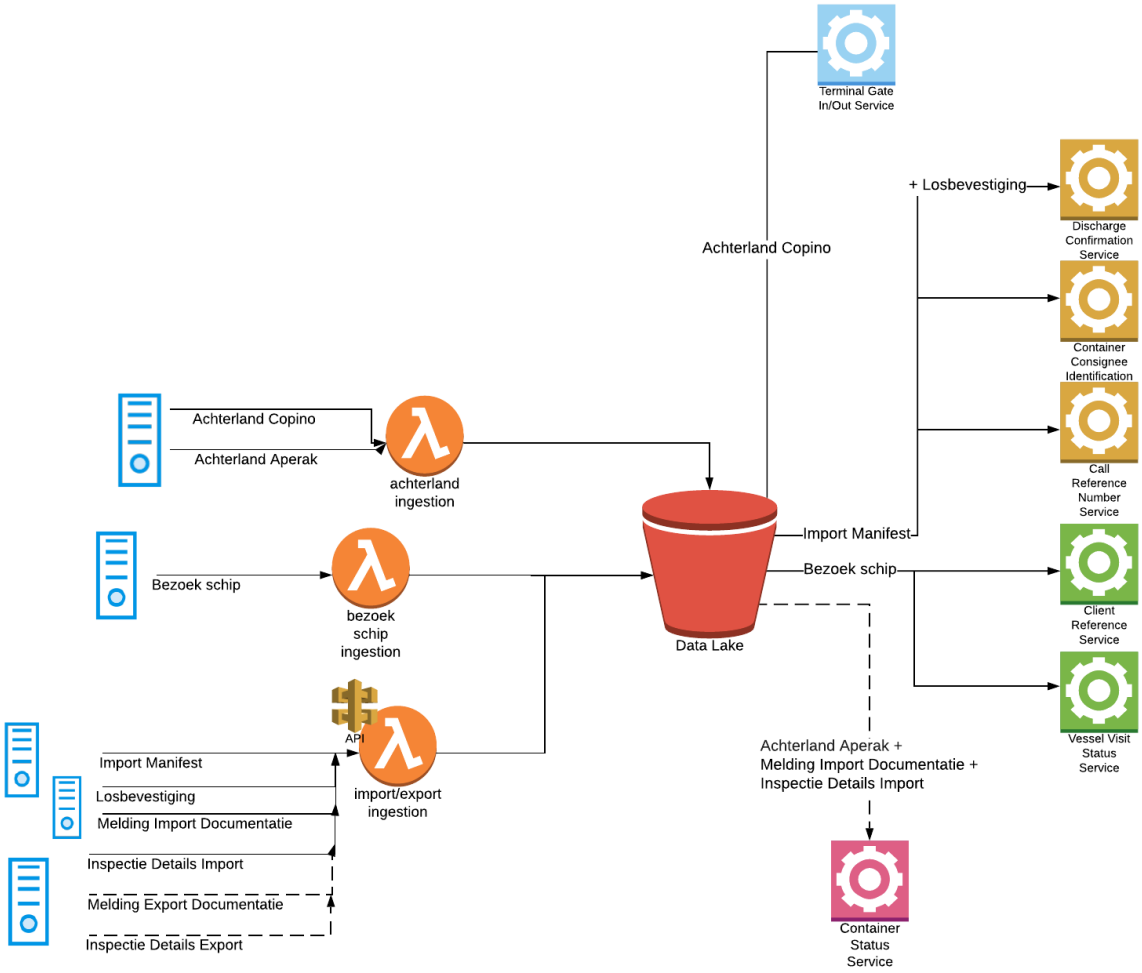
Het lading domein binnen het Port Community Systeem bestaat uit diensten gericht op de kernprocessen van de haven. Hieronder vallen ondermeer meldingen vanuit rederijen/ agenten aan de Douane (onder andere manifest, transit, domproc) en aan de VWA, los- en laadbevestigingen vanuit de deep sea terminals en inspectie statussen vanuit de overheden. Daarbij is tevens een koppeling tussen rederijen en expediteurs gerealiseerd, zodat expediteurs naast inzicht in de status van containers ook zicht hebben op het gemelde manifest.

De dekking is breed – voor alle maritieme import geldt dat de manifesten via het PCS worden verstuurd aan de Douane en statussen van lading worden ontvangen en doorgestuurd over de keten heen.

Architectuur en dataontsluiting

Vanuit het lading domein worden events vastgelegd en ter beschikking gesteld aan het informatieplatform van Portbase. Deze data wordt in een data lake opgeslagen en vanuit daar middels API’s ter beschikking gesteld aan de markt.

Aan onderstaand architectuuroverzicht valt af te lezen dat Portbase dit realiseert voor alle functionele domeinen binnen het Port Community Systeem (schip, achterland en lading).



Figuur 4: Architectuur dataontsluiting PCS

In bijlage 4 is opgenomen welke events met bijbehorende datavelden worden ontsloten vanuit het lading domein. Dit betekent concreet dat deze data via het informatieplatform van Portbase beschikbaar is en dat er derhalve API's opgebouwd kunnen worden. Het gaat om de volgende sets:

1. Summary cargo declaration sent to customs
2. Summary cargo declaration accepted by customs
3. Summary cargo declaration rejected by customs
4. Discharge report received
5. Import document sent
6. Import document accepted
7. Import document rejected
8. Inspection notified
9. Inspection released

Implementaties

Portbase heeft een aantal concrete cases opgepakt betreffende ontsluiting van ladinggegevens binnen het project, in afstemming met data eigenaren en vragende partijen. In het project is eerder al de case van losbevestiging beschreven, evenals de fresh case. Naast deze twee zijn er nog twee interessante cases uitgewerkt, welke hieronder uiteengezet zijn.

1. Dataservice extern terminal transport (ETT)

Containers die aan deepsea-zijde aankomen op een terminal gaan vervolgens, in veel gevallen, via de terminal naar het achterland. In enkele gevallen is vervoer naar een volgende terminal vereist. Dit betekent dat de container vanuit de terminal geïmporteerd wordt in de EU en vervolgens geëxporteerd wordt naar de volgende terminal. Het proces van het vervoeren van containers tussen terminals wordt Extern Terminal Transport (ETT) genoemd. Naast dit ETT proces, bestaan er andere varianten van ETT die afhankelijk zijn van de afkomst en toekomstige bestemming.

De betrokken terminal in deze case verzorgt dit ETT-proces in samenwerking met een softwarebedrijf. Onderdeel van dit ETT-proces is dat zij voor deze containers een MED-melding moeten doen (Melding export documentatie). Om deze MED-melding te kunnen doen hebben ze het Call Reference Number (CRN) nodig van het schip waarmee de betreffende containers de haven binnenkomt. Waar zij dit CRN nu nog handmatig opzoeken voor elke MED-melding, gaat de dataservice ETT erin voorzien dat dit proces geautomatiseerd kan worden door aanlevering van specifieke informatie.

De datadienst werkt als volgt:

- Om een CRN aan te vragen, dient de klant twee velden aan te leveren op het aanvraagmoment: het containernummer en de IMO-code van een schip (een uniek scheepsidentificatienummer). Deze velden vormen samen de sleutel.
- Vanaf het aanvraagmoment zoeken we 14 dagen terug in de tijd in de importmanifesten om met de sleutel het Call Reference Nummer (CRN) te vinden. Indien er geen CRN beschikbaar is op het moment van aanvragen, sturen wij die later zodra we de sleutel kunnen koppelen aan een CRN. Zodra de data verstuurd wordt, sluiten we de subscriptie (eenmalig antwoord). Indien er binnen 14 dagen na de aanvraag geen CRN gevonden wordt voor een aanvraag, verloopt de subscriptie en sturen we een sluitingsbericht.
- Het antwoord dat we versturen bestaat uit het CRN en een Portbase subscription ID. We sturen de locatie (terminal) niet mee.
- Terminal stuurt het aanvraagbericht in de vorm van een URL. Wij antwoorden op deze URL. Doordat de terminal zelf het boekingsnummer verwerkt in deze URL is het voor hun mogelijk om een mapping te maken voor het achterhalen van de loodscode voor de MED melding.
- Portbase maakt gebruik van het Import Manifest om het antwoord te genereren. Eigenaarschap van de data ligt bij Portbase (CRN wordt aangemaakt door Portbase bij een Melding Bezoek Schip).
- De terminal geeft de voorkeur aan een Pub/Sub-mechanisme, waarmee het zich abonneert per sleutel en Portbase een antwoord pusht zodra beschikbaar.

In bijlage 3 is de technische beschrijving opgenomen van de dienst.

2. Dataservice Container release (TradeLens)

In vergevorderd stadium is de koppeling met TradeLens, een global platform waarbinnen grote containerederijen actief zijn. Doel is om de container release notificatie te koppelen. Technisch zal deze conform de overige datadiensten zijn, echter zijn er enkele opmerkingen te plaatsen:

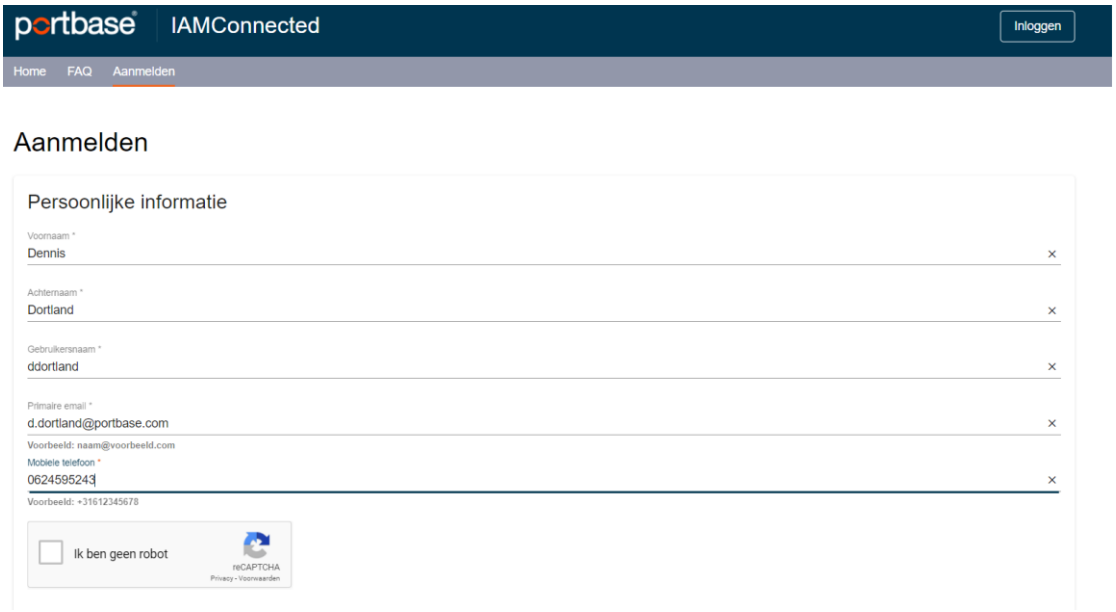
- Toestemming datadelen: er is toestemming nodig zowel vanuit de agenten/rederijen als de Douane. Om het proces hiervoor schaalbaar in te richten zal mogelijk de Data Share Manager worden benut.
- Businessmodel: TradeLens hanteert een data voor data model (ondanks dat het zelf betaalde diensten levert aan verladers). Op dit moment loopt een onderzoek of er waardevolle data terug kan komen vanuit TradeLens richting de Portbase community. Met de dataeigenaren is een gesprek opgestart om gezamenlijk vast te stellen wat de waarde van de data kan zijn.

Vooruitblik

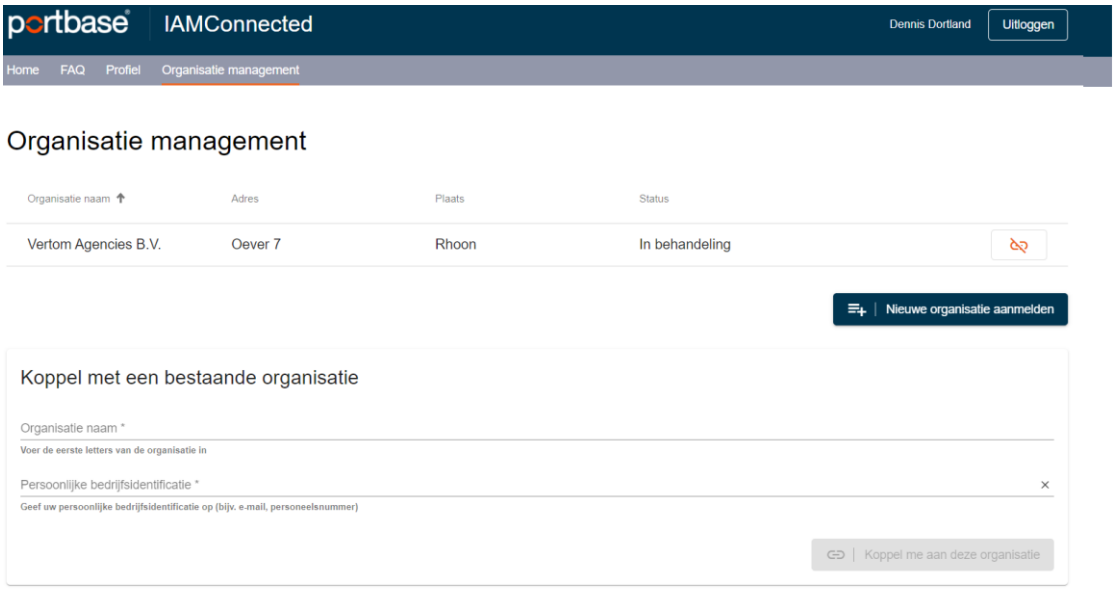
Doordat Portbase heeft ingezet op de IAM-bouwstenen met hierbij de visie op iSHARE in combinatie met datadiensten, zal het in de nabije toekomst een grote rol spelen in de schaling van enerzijds iSHARE zelf, anderzijds van het delen van de data zelf.

De techniek en standaarden staan, de data is beschikbaar. Belangrijk is het doorgaan met opzetten van nieuwe cases en het bewijzen van de waarde. Daarnaast het inrichten van businessmodellen en de organisatie. Portbase is gecommitteerd om dit blijvend te doen.

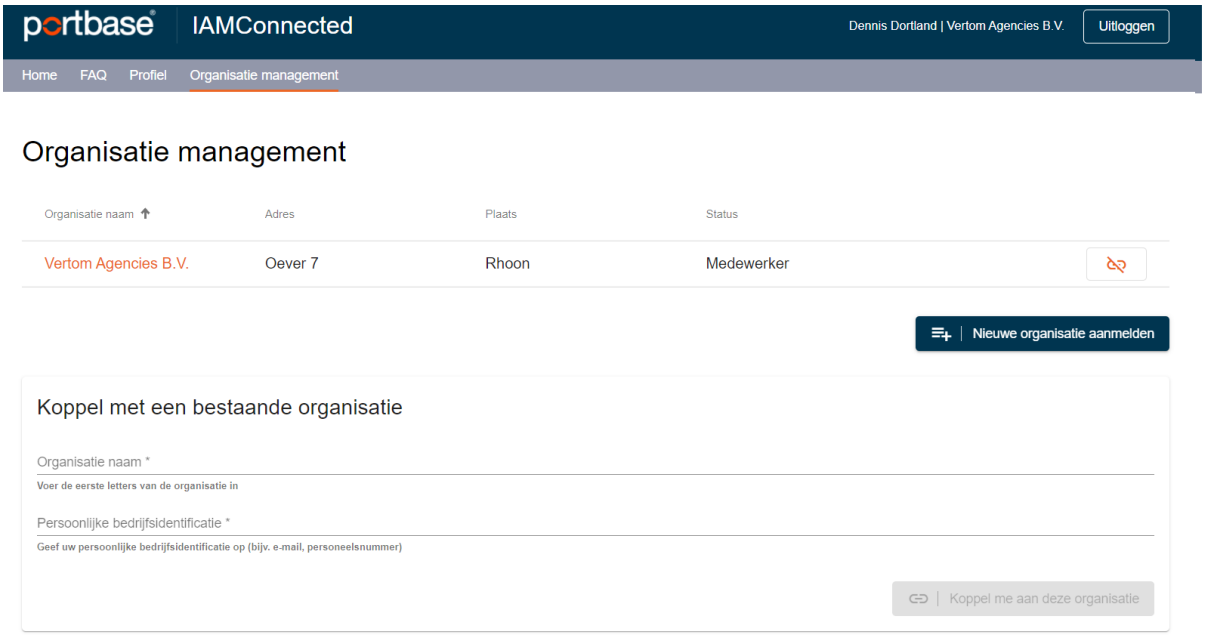
Bijlage 1: Screenshots Community Passport



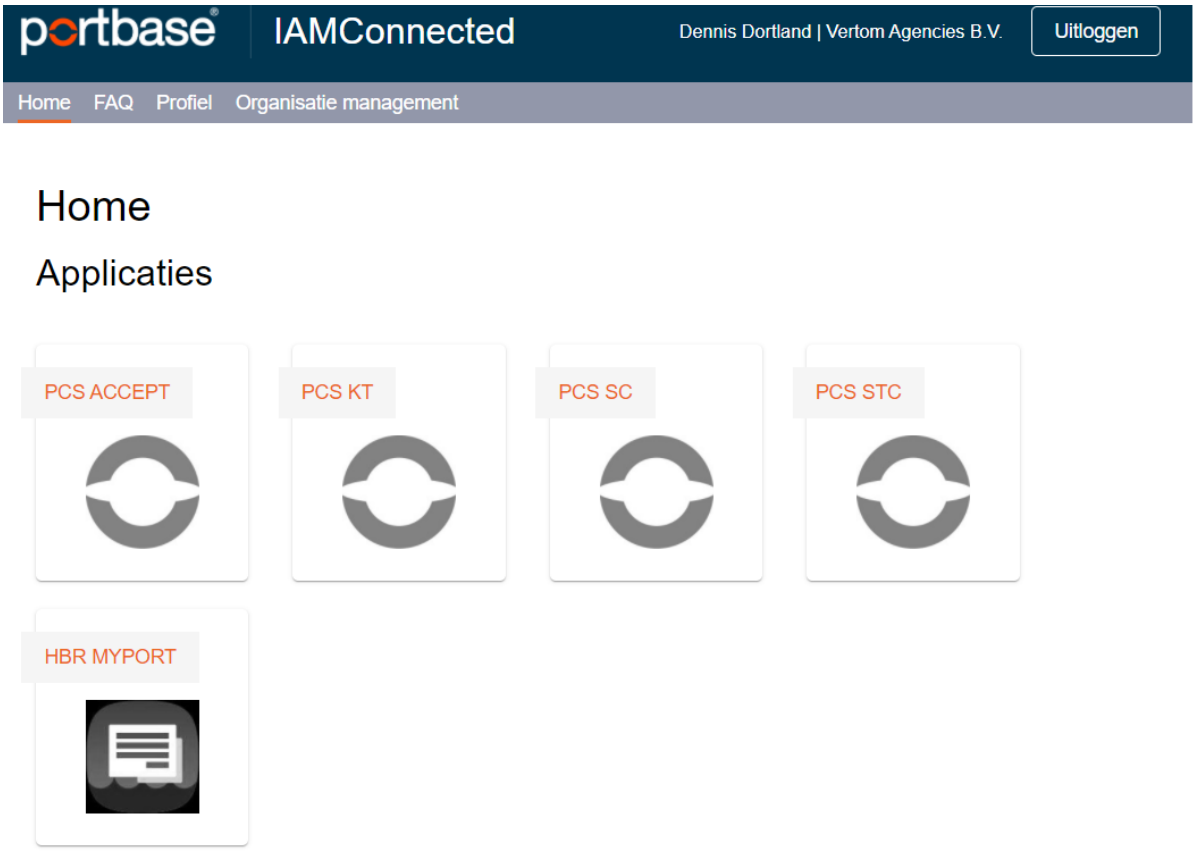
Figuur B1: het aanmaken van een nieuw account



Figuur B2: Het koppelen van een gebruikers aan een organisatie

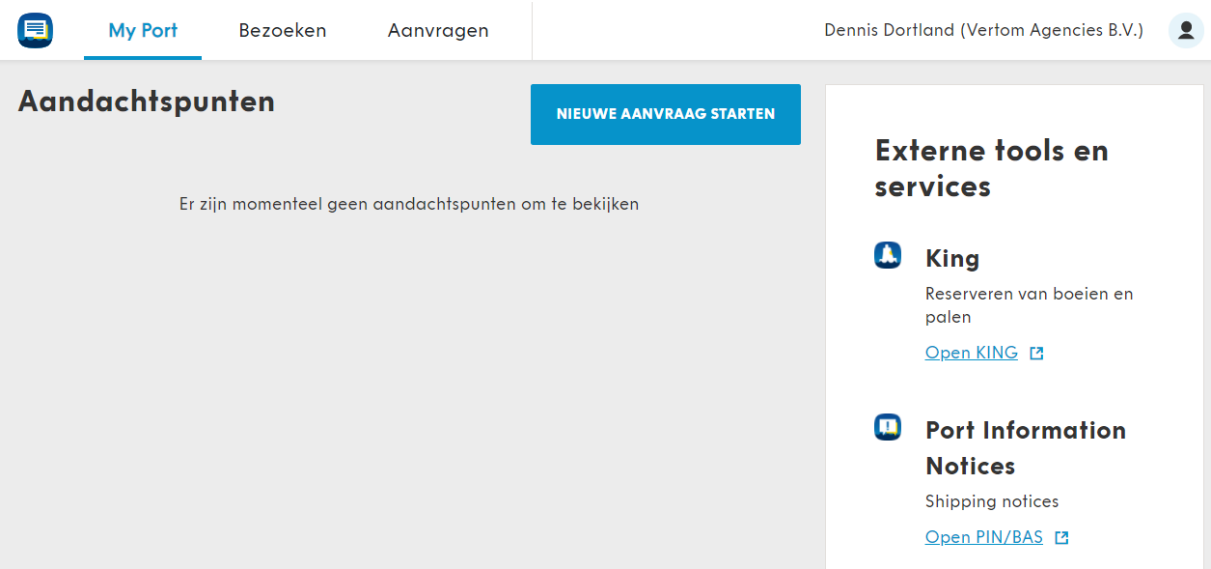


Figuur B3: De gebruiker is geaccepteerd binnen de organisatie



Figuur B4: Het homescherm van het Community Passport: Overzicht aangesloten services (Ontwikkelversie)

Figuur B5: Landingsscherm voor inloggen My Port (applicatie Havenbedrijf Rotterdam)



Figuur B6: De gebruiker is ingelogd door gebruik maken van Community Passport. Gebruiker en organisatie worden door de applicatie geaccepteerd.

Bijlage 2 – ETT service

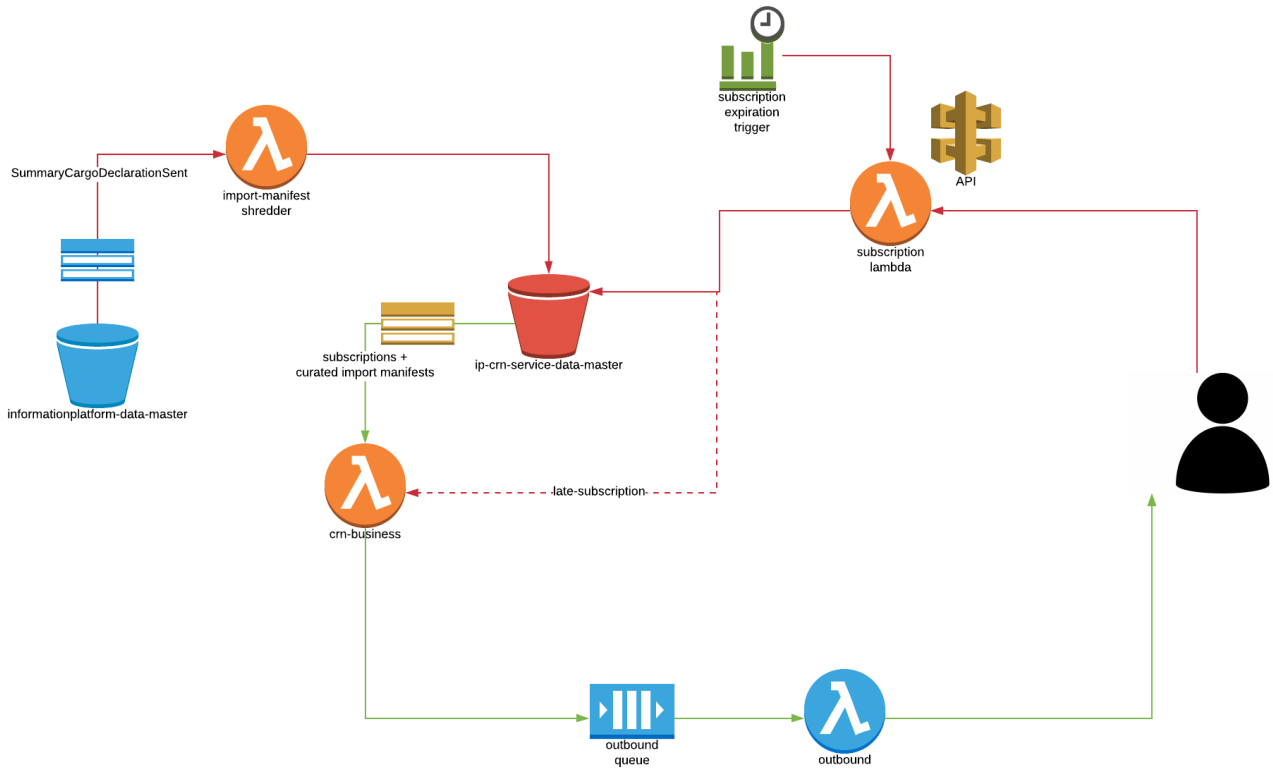
Repository for all the business logic on the crn service as part of the Information Platform.

Introduction

This document is meant for anyone who wants to know the technical story behind the crn service of the Information Platform. It describes a high-level overview of the main components of the service and its relationship to others. Before reading this, we advise you to first read into the *infrastructure* repo.

The diagram below shows an overview of the service implementation in AWS. Components are mainly S3 buckets, SNS topics and Lambdas. Red arrows describe incoming data streams to the service, green arrows are outgoing data streams to the outside world. Furthermore, blue components are defined in the *infrastructure* repo. This means that the discharge confirmation service is a consumer of these components.

Recall that the *infrastructure* repo is the foundation for the Information Platform. This means that its primary objective is to provide data/information services of (1) raw data streams and (2) generic functionality. We decided this to be a proper set-up for the platform, since (1) data should be re-used whenever multiple consumers are interested in this data and (2) functions which are useful for many reasons should be re-used and not re-implemented.



Terminology

Before doing a deep dive into the different components of the service, you should become familiar with the following terminology:

- **raw data**: this type of data is created by real-life events (also called raw event). For instance, the discharge of a container is a real-life event and results in a raw data set of this event.
- **curated data**: this type of data is the result of *curating* a raw event. The process of curating mainly consists of removing unused fields from the raw data set. After this step, you have the curated version of the raw event.
- **business data**: this type of data is a data set which is really to send to a customer. It is the final data set and is generally made when the corresponding curated data sets are present in the service.
- **subscriptions**: this type of data represents the subscription of a customer to the service.

Step-by-step description

The diagram shows a blue S3 bucket on the left. This bucket is part of the infrastructure repo and it consists of all raw event data. One of these events is called **SummaryCargoDeclarationSent** (*import manifest* for short). As you can read in the functional documentation of the crn service, the service is dependent on this event stream. Through SNS topics, lambdas are triggered whenever a new raw event is created. Lambdas that process raw events are called *shredders*. Their goal is to grab a raw event file and filter out any unnecessary fields, leaving a curated version of the raw event. These curated versions are saved in the red S3 bucket, which is used to store data that is needed for the crn service specifically and solely. Another term for this type of S3 buckets is service-specific buckets.

Another incoming data stream comes from the subscription API which is the main gate for customers. They use this API and give us the following fields: *container_number*, *imo* (unique id of a ship), *client_url* (customer API endpoint). With these fields, we set up a new subscription for this client, stating that he/she wants to get notified of the corresponding *call_reference_number*.

The **business lambda** tries to match active subscriptions with curated data. The lambda also creates a transaction for this event.

Sending an outbound message to a customer is done by sending this message to an **SQS queue** that is part of **infrastructure**. This queue is implemented to make sure that outbound messages are passed properly by the system to the **outbound lambda**. This lambda sends an outbound message to a customer.

Service Workflows

The **happy workflow** goes as follows:

```
1.  customer creates subscription S for (container_number, imo) X.
2.  The service retrieves import manifest data with container data X and obtains
call_reference_number Y.
3.  The business lambda detects that the X,Y combination is now obtained for subscription S
and creates a business data set ready to send to the customer.
4.  Through the outbound lambda in infrastructure, the customer gets notified.
```

Another possible route is that the call reference number is already known within the platform at the moment of subscription. In this case, the business lambda directly connects the call reference number with this subscription and the customer gets a reponse immediately. **Important**: the service only tracks back call reference numbers for the period up to 14 days ago.

A subscription can only stay active for 14 days after which its status is set to expired. To make sure that these expired subscriptions are cleaned up, the **subscription lambda** scans through all subscriptions and checks if they're overdue their expiration date. This action is being executed once a day by a Cloudwatch Event Rule. So the lambda behavious differently based on the type of trigger:

```
1. API call: create new subscription.
2. Cloudwatch Event Rule: search for expired subscriptions.
```

Subscribing to the CRN Service

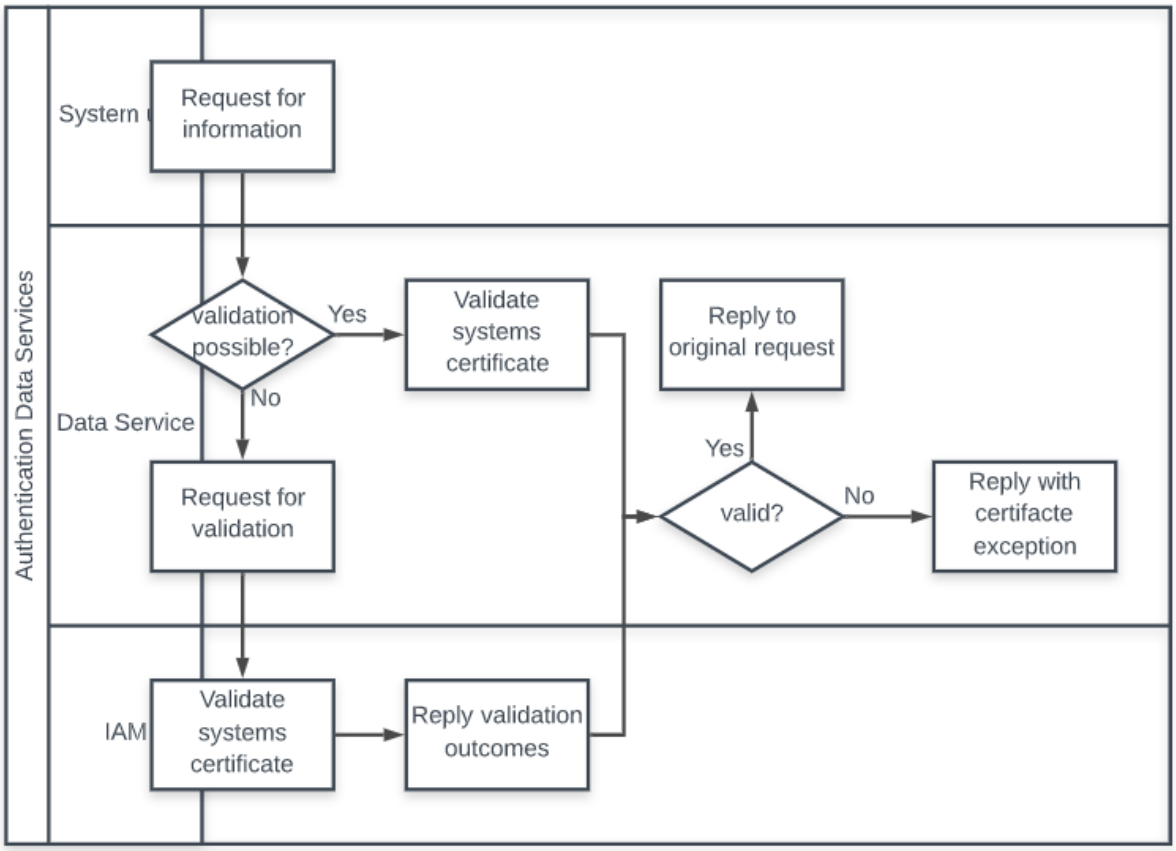
When a valid customer adds a subscription through the subscription API, we first check the following:

```
1. If its message is well-formed,
2. If its message contains the fields necessary and their values have a correct format.
```

If its request does not meet these two requirements, we return a message like "Sorry, but your subscription seems to be invalid, please check and try again". This subscription is not part of the invoicing for the customer, since processing such ill-formed requests is very trivial and practically does not cost us anything.

Another side-track is that the customer sends a well-formed request, but it points to a non-existing container or the container does get processed within the limit of 14 days. In this case, the customer receives a closing message when the subscription time limit is over due. These subscription are part of the corresponding invoice, because the service tried to process these subscriptions for 14 days (which results in some AWS costs). You should see this as "We tried, but couldn't help you because we could not find this container on ship with given imo".

Bijlage 3 – Authentication flow system 2 system



Authentication flow for secure system 2 system connections. For iSHARE compliancy, PKI Overheid certificates are required

Bijlage 4 – Ontsloten datasets ladingdomein PCS


E11-02 Summary cargo declaration sen


E11-03 Summary cargo declaration acc


E11-04 Summary cargo declaration reje


E11-05 Discharge report received v2019


E1700 InspectionNotified.xlsx


E1701 InspectionReleased.xlsx


E2401 ImportDocumentSent.


E2402 ImportDocumentAcce


E2403 ImportDocumentRejec