Portbase Case Study on Authorisations

Ownership of data has always been a key a foundational topic in the history of Portbase.

The Portbase Community agreed on the separation of data into:

- Kerndata (“core data”) which is used in the Kernprocessen (“core processes”) facilitated by Portbase
- Other data

The core data can freely be shared between the involved participants in the specific logistic flow. The data owner has given upfront permission for sharing this data with the participants that are defined as actors, based on their logistical roles, in the core process the data is shared.

Permission of the Data Owner is required for:

- Sharing core data with other organisations then the involved participants (so outside core processes)
- Sharing other data than the core data

How the permissions are managed is depending on the use case. Below three examples which are running today in production within Portbase.

Portbase has developed and implemented an Authorisation Register which manages the permissions for sharing the data between organisations. This AR is called MyData

Each organisation can view and edit the permissions using the MyData via web screens. A dedicated role “Data Manager” has been defined on a user level and can be assigned to one or more users of the Organisation, to limit managing data sharing permissions to those responsible. These permissions entails release of complete data sets defined by the service that release them.

The permissions are retrieved by Portbase services using a REST API. Portbase target architecture is an event-based mechanism using the Portbase streaming platform based on Pulsar. The local copy is used by the service for authorisation decisions.

Three Use Cases

Use Case 1: Vessel Visit API

The Vessel Visit API is a broad API which is available for all interested organisations. It consists of 40+ data points from 130+ Data Owners.

When a Data Consumer uses the API and requests data, the local, but up-to-date, permissions are checked and only the datapoints are returned for which the data-owner has given the permission to share the data with that the Data Consumer.

Use Case 2: CBS Container Data

Container Terminals are obliged to share container shipment data with CBS. Portbase is offering a service to the Terminals which can be used to fulfil this obligation.

Container Terminals can use MyData to give data sharing permission to CBS.

CBS is requesting once per month the data for all terminals. The Data sharing permissions decide for which terminals the data can be retrieved.

Use Case 3: Terminal Premium Data

A terminal can decide that specific data can only be viewed in a PCS Service if a paid subscription for this data has been procured by the Data Consumer. This subscription data is hosted within the Terminal.

The subscription data is synchronized (by hourly polling) with MyData. MyData transforms the obtained subscription data into permissions, syncs this using the pub-sub pattern with the data services which uses local copies to decide if a customer is allowed to view the data.

Portbase decided not to “poll” external Authorisation Registers runtime. In other words, an external Authorization Register is not queried in the same process while authorizing a Data Consumer request by a data service due to the dependency on performance / delay and availability.