PER Auskunft

Access concept

Classification	public
Version	1.0
Date	October, 31st 2024

For digital Switzerland. For Sure.

abraxas

Contents

1. Introduction

Because it holds very sensitive personal data, authentication and authorization is a very important subject to PER. The guiding principle is that access control is delegated as much as possible to the specialized Abraxas service SECURE Connect. This immediately excludes a big number of challenges that may occur with a self-implemented solution. PER adheres as far as possible to standard security procedures and relies on the widely used concept of roles and permissions. The permissions for accessing data are very fine-grained to take account of the sensitive nature of the data stored in PER.
Note that PER itself doesn't maintain any user data. Users are solely kept in SECURE Connect.

2. Authentication

All authentication is delegated to the Abraxas SECURE Connect platform. Users of PER Auskunft are redirected to the SECURE Connect application upon login. There they enter their login details and receive a **JWT token**, which the web app can then present to the API Gateway. Users must have the correct application and tenant activated in SECURE Connect.

SECURE Connect Item	Required Value
Application	Auskunft
Tenant	Auskunft
Role (checked during authorization)	ROLE_Auskunft_Auskunft_xy

2.1 Authorize new users

2.1.1 PER Administration

To authorize a new user for PER Auskunft, the following requirements must first be met:

- **Match between role SECURE Connect and role PER**
  - Each role must be defined in two places, first in PER Administration, then in SECURE Connect.
  - The role in PER Administration consists of a title and the attributes that a user is allowed to read.
  - The counterpart in SECURE consists of a title only.
  - The two roles are matched via their title, so both names have to be identical.
  - The reason for this discrepancy is due to the fact that the SECURE Connect roles are assigned to users, but don't contain any further information.
  - If PER only used SECURE Connect roles, PER would know that user A has role X, but PER would not know, what to do with it.
  - But since the role X also exists in PER, PER knows that this role allows the user to read attributes Z.
- **Match between tenant of SECURE Connect and organization PER**

- PER contains information about so called "organizations". An organization can be a municipality, a composite (several municipalities) or the entire canton (a combination of all the municipalities).
- This information is used to restrict which persons a user is allowed to see. For example, a user who is entitled to municipality A will only see persons who are residents in municipality A.
- The SECURE Connect equivalents to PER organizations are the tenants.
- To match the tenant with the organizations, the ID of the tenant (for example 123456789012345678) must be added manually to the PER organization (in the field "Mandant" within SECURE Connect)

If these conditions are met, a user can be authorized in SECURE Connect.

2.1.2 SECURE Connect

A user gets authorized on a Mandant for the application "PER Auskunft" with the role "User" (default role, which is required to open PER Auskunft) and his additional roles (which define which attributes he is allowed to view).
In the following example, the same user is authorized for two different Mandaten. For the first Mandant (PER Test Gossau), the user has two roles: "User", which is required for opening PER Auskunft and "allRights" which is a role in PER Administration (see previous chapter). For the second Mandant (PER Testkanton), the user is also authorized for "User" and "allRights" but has additional four roles (which also exist in PER Administration). The roles allRights, birthDeathData, nameBasicSexData, nameFullData and placeOfOriginData are additive. If the role nameFullData allows the user to view attribute X, it doesn't matter if the other four roles contain the permission for attribute X or not; the user is allowed to view it.

3. Authorization

Authorization in PER Auskunft relies on roles and permissions. A permission represents the right to view some kind of data about persons, for example the names or data about religion. The permissions are grouped according to their meaning in the eCH standards. The following diagram shows the involved domain classes used to model the roles and permissions.

Roles contain several properties that pertain to permissions. This primarily includes the **AttributePermission** property, which regulates access to the data stored in persons. Furthermore there are other properties that guard the scope of data accessible:

Role property	Governs
houseHoldMemberPermission	Whether household members can be viewed
accessToInactiveResidents	Can see persons even if they don't have an active residence
historicValues	Can see past data but only up to a configured time (except if fullHistoricPermission is set)
fullHistoricPermission	No restriction on the amount of historic data

The Personenregister service which serves the requests of the user checks the permissions of the roles the user might have.

Roles are stored in the database of PER but are given to users in SECURE Connect. This is done by giving the users roles in SECURE Connect as shown in the table in section 2. The component responsible for resolving the roles of the users is API Gateway. API Gateway contacts SECURE Connect with the token received and queries the roles of a user. Then the **roles are transmitted to any downstream service using a role header**. This means that the roles are listed in a header and thus made available to downstream servers that need to check the permissions (in particular the Personenregister service). Note that the user token is not used to carry the roles of the user. Instead, the roles are queried from SECURE Connect by the API Gateway using the token.