VOTING Stimmregister

Authorization Model

Author	Abraxas Informatik AG
Classification	confidential
Version	1.0
Date	20. Nov 2023

Für die digitale Schweiz. Mit Sicherheit.

abraxas

Contents

1. VOTING IAM 3
1.1 Applications 3
1.2 Roles 3
1.2.1 Permission Inheritance 3
1.3 Tenants 4
1.4 Users 6

2. Authorization Table 7
2.1 API Endpoints 7
2.2 User Interactions 9

3. Data Access Authorization 11
3.1 Process Flow 11
3.2 Prerequisites 11
3.3 DOI Synchronization 11
3.3.1 Requirements 11
3.3.2 Data Structure 12
3.3.3 Data Samples 13

1. VOTING IAM

1.1 Applications

The following applications are available for VOTING Stimmregister (VOSR):

Application	Description
VOTING-STIMMREGISTER	Application for managing master data for voting eligibility to be able to obtain information on voting rights on a daily basis, in real time and based on saved filters.

1.2 Roles

The following roles are available for the application VOSR:

Application	Role	Description
VOTING-STIMMREGISTER	Reader	A user with the role *Reader* has read permission for all areas in VOSR and has view permission on persons for the security scope of the assigned tenant.
	Manager	A user with the role *Manager* has full access to all functionalities within VOSR except for export and manual import. These two features are authorized separately.
	Exporter	A user with the role *Exporter* has permission to export CSV or eCH-0045 reports from either the person search or filter management.
	ManualImporter	A user with the *ManualImporter* role has the authorization to manually import registrations that are not delivered via an automatic interface.
	ApiImporter	A service user with the role *ApiImporter* is allowed to import registry data into VOSR through a defined API interface. This role is only intended to be assigned for service users (refer to chapter: Users) and access is restricted according to least privileged principle.
	ApiExporter	A user with the ApiExporter role is authorized to request eCH-0045 exports via a defined API interface.
	ImportObserver	A user with the role *ImportObserver* has permission to view all import statistics history from all ACL scopes.

1.2.1 Permission Inheritance

Roles are not atomic and thus may inherit permissions from other roles. The following table provides an overview of possible inheritance:

✓ Indicates this role applies permissions directly.
x Indicates this role inherits permissions from another role.

	Manager	Reader	Exporter	ManualImporter	ApiImporter	ApiExporter	ImportObserver
Manager	✓	x	-	-	-	-	-
Reader	-	✓	-	-	-	-	-
Exporter	-	-	✓	-	-	-	-
ManualImporter	-	-	-	✓	-	-	-
ApiImporter	-	-	-	-	✓	-	-
ApiExporter	-	-	-	-	-	✓	-
ImportObserver	-	-	-	-	-	-	✓

1.3 Tenants

In the context of VOTING, the tenant is reflected by a political unit such as a canton or municipality. An example configuration is shown below:

Tenant	Application	Available Roles	Unit	Permission	Comment
State Chancellery of Canton A *Staatskanzlei Kanton A*	VOTING-STIMMREGISTER	Reader Manager Exporter ManualImporter	Canton	A canton has access to all its associated municipalities and their associated persons. The access authorization is determined by the hierarchical domain of influence in VOTING Basis.	As the supervisor authority of the Canton A, the State Chancellery manages VOSR on top level with a view point over all persons of the canton and all its municipalities. In addition, the supervisor authority is allowed to manually import the Swiss abroad from the manual import.

Tenant	Application	Available Roles	Unit	Permission	Comment
Municipality of B *Gemeinde B*	VOTING-STIMMREGISTER	Reader Manager Exporter	Municipality	A municipality user has only access to the persons of its own municipality.	The municipality B is able to manage voting filters with a view point over all persons of its municipality or a filtered subset of it. Optionally, result sets can be exported as csv or eCH-0045 for further processing.
Municipality of C *Gemeinde C*	VOTING-STIMMREGISTER	Reader Manager Exporter	Municipality	A municipality user has only access to the persons of its own municipality.	The municipality Cis able to manage voting filters with a view point over all persons of its municipality or a filtered subset of it. Optionally, result sets can be exported as csv or eCH-0045 for further processing.
Abraxas Informatik AG	VOTING-STIMMREGISTER-IMPORTER	ApiImporter	Service User	The service user for the API based import can only use the API, but has no access to personal data from the VOSR.	The tenant Abraxas Informatik AG is the leading resource owner for special importer applications that are used by

Tenant	Application	Available Roles	Unit	Permission	Comment
					subsystems for delivering import data.

1.4 Users

User accounts are managed in VOTING IAM. An example configuration is shown below:

User	Tenant	Application	Role ID
Barbara Burger	State Chancellery of the Canton A	VOTING-STIMMREGISTER	Manager
			ManualImporter
			Exporter
Franz Fürer	Municipality B	VOTING-STIMMREGISTER	Manager
	Municipality C	VOTING-STIMMREGISTER	Reader Exporter
Karin Brandt	Municipality D	VOTING-STIMMREGISTER	Reader Exporter
Erika Moore	Abraxas Informatik AG	VOTING-STIMMREGISTER	ImortObserver
VOTING-STIMMREGISTER-IMPORTER	Abraxas Informatik AG	VOTING-STIMMREGISTER	ApiImporter

In addition, it is possible to have multiple roles with the same combination of application and client. Thus, a user could simultaneously have the roles *Reader* and *Exporter* in the municipality A and B for the application "VOTING-STIMMREGISTER". In practice, however, such combinations rarely occur in the VOTING environment.

2. Authorization Table

This chapter provides an overview of all actions which can be executed on the frontend and API level. The listed actions can only be executed when all conditions are fulfilled. If a condition is empty, it is considered fulfilled.

2.1 API Endpoints

Action	API Namespace, Route	Conditions
PERSON SEARCH		
Search persons by filter criteria	abraxas.voting.stimmregister.v1.services.PersonService.GetAll	Reader
Get person details	abraxas.voting.stimmregister.v1.services.PersonService.GetSingle	Reader
FILTER OVERVIEW		
List all filters	abraxas.voting.stimmregister.v1.services.FilterService.GetAll	Reader
Save a new filter	abraxas.voting.stimmregister.v1.services.FilterService.Save	Manager
FILTER DETAILS		
Get filter details	abraxas.voting.stimmregister.v1.services.FilterService.GetSingle	Reader
Get persons by filter	abraxas.voting.stimmregister.v1.services.PersonService.GetByFilterId	Reader
Save edited filter	abraxas.voting.stimmregister.v1.services.FilterService.Save	Manager
Delete filter	abraxas.voting.stimmregister.v1.services.FilterService.Delete	Manager
Duplicate filter	abraxas.voting.stimmregister.v1.services.FilterService.Duplicate	Manager
FILTER / VERSION EXPORT		

Action	API Namespace, Route	Conditions
Export CSV report	/v1/export/csv	Exporter
Export eCH-0045 report	/v1/export/ech-0045	Exporter
FILTER VERSION		
Save a new version	abraxas.voting.stimmregister.v1.services.FilterService.CreateVersion	Manager
Get persons by filter version	abraxas.voting.stimmregister.v1.services.PersonService.GetByFilterVersionId	Reader
Rename filter version	abraxas.voting.stimmregister.v1.services.FilterService.RenameVersion	Manager
Delete Filter Version	abraxas.voting.stimmregister.v1.services.FilterService.DeleteVersion	Manager
DATA		
Upload data of type 'Persons Cobra'	/v1/import/cobra/persons	ManualImporter || ApiImporter
Upload data of type 'DOI Lognato'	/v1/import/loganto/doi	ApiImporter
Upload data of type 'Persons Loganto'	/v1/import/loganto/persons	ApiImporter

Action	API Namespace, Route	Conditions
Upload data of type 'Persons Innosolv'	/v1/import/innosolv/persons	ApiImporter
Get import statistics	abraxas.voting.stimmregister.v1.services.ImportStatisticService.List	Reader
Get import statistics history	abraxas.voting.stimmregister.v1.services.ImportStatisticService.GetHistory	Reader

2.2 User Interactions

Action	Component Name, Interaction	Conditions
PERSON SEARCH		
Open person search menu	PERSONENSUCHE	Reader
Add or remove filter criteria	FILTER HINZUFÜGEN	Reader
Reset person search filter criteria	ZURÜCKSETZEN	Reader
Create filter from person search filter criteria	FILTER ERSTELLEN	Manager
Show person details	*<person table row selection>*	Reader
FILTER OVERVIEW		
Open filter menu	FILTER	Reader
Create a new filter	FILTER ERSTELLEN	Manager
FILTER DETAILS		
Show filter details	<filter *table row selection*>	Reader
Enter edit filter mask	FILTER BEARBEITEN	Manager
Delete filter	LÖSCHEN	Manager
Duplicate filter	DUPLIZIEREN	Manager

Action	Component Name, Interaction	Conditions
FILTER / VERSION EXPORT		
Open dialog to export data	EXPORTIEREN	Exporter
FILTER VERSION		
Open dialog to select existing version	VERSION LADEN	Reader
Open dialog to save new version	VERSION SPEICHERN	Manager
Select rename filter version	UMBENENNEN	Manager
Select delete filter version	LÖSCHEN	Manager
DATA		
Open menu "DATEN"	DATEN	Reader
Open dialog to upload data	HOCHLADEN	ManualImporter

3. Data Access Authorization

A user within VOSR has access to a defined set of persons. Depending on the assigned user permissions (tenant and role) in VOTING IAM, the subset of accessible persons may vary. The leading system that provides all necessary information for decision making is VOTING Basis. In VOTING Basis the hierarchical domain of influence tree represents the access control list for every authority.

3.1 Process Flow

1. The user logs into VOSR and selects a tenant.
2. The user opens the person search page and loads all person data.
3. The VOSR backend searches for the active tenant within the hierarchical domain of influence tree from VOTING Basis and creates a list of inherited BFS numbers.
    a. Municipality (MU): Has access to its own municipality only (In practice, no hierarchical inheritance of other municipalities exist).
    b. Canton (CT): Has access to many hierarchically inherited municipalities.
    c. Root (CH): Has access to many hierarchically inherited municipalities.
4. Based on the list of accessible BFS numbers, the VOSR backend limits the result list shown in the person search overview.

3.2 Prerequisites

This chapter defines all required data needed to evaluate the data accessibility for a logged in user.
VOTING Stimmregister:

- The VOTING IAM tenant id of the active tenant
- The hierarchical domain of influence (DOI) structures must be up-to-date with VOTING Basis

VOTING Basis:

- Each element of the hierarchical DOI nodes must be correctly assigned:
    - The BFS number must be set
    - The authority (Behörde) must be assigned with a valid VOTING IAM Tenant Id

3.3 DOI Synchronization

3.3.1 Requirements

- Cyclic synchronization of all DOI with VOTING basis (at least once a day)
- DOI data may not be directly queried from VOTING Basis at runtime.
- A synchronization is required to prevent a critical operational dependency between the systems.
- Person data access authorization must be integrated into the repository security layer which is applied to every person query, regardless of the caller.

3.3.2 Data Structure

Attribute	Data Type	Required	Sample Data	Description
Id	Guid	Required	3d337327-a5a1-4604-a553-7e4be0709fca	The identification for the DOI element
ParentId	Guid	Optional	df603a42-6039-4373-920d-16485d7bc946	The parent id of the current DOI element. May be null for root elements (CH).
Children	DOI (Object)	Optional		The DOI tree structure is exported by VOTING Basis as a hierarchical representation of nested objects.
Name	String	Required	Auslandschweizer	Represents the name of the DOI as visualized in VOTING Basis.
Bfs	String	Optional	9170	The BFS number must be set for elements of type MU (municipality) but may be missing for other DOI types.
TenantName	String	Optional		Represents the tenant (authority) name as defined within VOTING IAM. This attribute is used for information purposes only.
TenantId	String	Optional	177778113432781596	Represents the tenant id as defined within VOTING IAM.
DomainOfInfluenceType	Number	Required	4	Represents the type of DOI, one of: DOMAIN_OF_INFLUENCE_TYPE_UNSPECIFIED = 0; DOMAIN_OF_INFLUENCE_TYPE_CH = 1; DOMAIN_OF_INFLUENCE_TYPE_CT = 2; DOMAIN_OF_INFLUENCE_TYPE_BZ = 3; DOMAIN_OF_INFLUENCE_TYPE_MU = 4; DOMAIN_OF_INFLUENCE_TYPE_SK = 5; DOMAIN_OF_INFLUENCE_TYPE_SC = 6; DOMAIN_OF_INFLUENCE_TYPE_KI = 7; DOMAIN_OF_INFLUENCE_TYPE_OG = 8; DOMAIN_OF_INFLUENCE_TYPE_KO

Attribute	Data Type	Required	Sample Data	Description
				= 9; DOMAIN_OF_INFLUENCE_TYPE_AN = 10;
DomainOfInfluenceCanton	Number	Required	1	Represents the responsible canton, one of: DOMAIN_OF_INFLUENCE_CANTON_UNSPECIFIED = 0; DOMAIN_OF_INFLUENCE_CANTON_SG = 1; DOMAIN_OF_INFLUENCE_CANTON_TG = 2; DOMAIN_OF_INFLUENCE_CANTON_ZH = 3; The canton is only set for top level elements of type CH.

3.3.3 Data Samples

Depending on the authorized tenant, a user may have access to different sets of BFS numbers. A tenant may be assigned to multiple DOIs within the hierarchical tree and thus the resulting set of accessible persons may be a composition of many BFS numbers.

Domain of Influence	Tenant	Accessible BFS
▾ Kanton A eidgenössisch (CH) *(zuletzt geändert 2023-11-14 / 12:37)* Auslandschweizer (MU) *(zuletzt geändert 2023-11-14 / 09:08)* ▾ Kanton A kantonal (CT) *(zuletzt geändert 2023-11-15 / 12:08)* Gemeinde A1 (MU) *(zuletzt geändert 2023-11-15 / 12:09)* Gemeinde A2 (MU) *(zuletzt geändert 2023-11-15 / 12:10)* Gemeinde A3 (MU) *(zuletzt geändert 2023-11-15 / 12:11)*	Canton A federal (CH)	9170 (Auslandschweizer) 3203 (Municipality A1) 3238 (Municipality A2) 3340 (Municipality A3)
	Canton A cantonal (CT)	3203 (Municipality A1) 3238 (Municipality A2) 3340 (Municipality A3)
	Municipality A1 (MU	3203 (Municipality A1)