SignaturGruppen

Nets eID BROKER

Privilege Management - Introduction

Version 1.0

SignaturGruppen

Table of Contents

Changes

Version 1.0 26-02-2024

- Updated document to version 1.0

Terminology

Term	Description
Nets eID Broker (**NEB**)	Nets eID Broker. Certified MitID Broker and general broker and identity provider for enterprise services.
OpenID Connect (**OIDC**)	**OpenID Connect** 1.0 is an identity layer on top of the OAuth 2.0 protocol
Nets eID Broker Privilege Management UI web-interface (**PRIV-UI**)	Nets eID Broker Privilege Management web-interface. Interface allowing configuration and administration of the integration
OIO Basic Privilege Profile	Danish Public model-specification for privileges.
Privilege organization administrator	Administrator able to create and administrate privileges for one or more organizations. Operations like defining new privileges, update description and update assignability settings for privileges.
Privilege user administrator / Privilege assigner	Administrator able to assign privileges for organization employees. In the Nets eID Broker Privilege Management, there is administrative scenarios for both organization and user administration, so we will in general refer to the administrative role of assigning privileges to employees as the “privilege assigner” or “privilege user administrator”.

Introduction

This document is an introduction to Nets eID Broker Privilege Management (NeB-PM)

The intended audiences are Privilege administrators, IT developers and IT architects.

Nets eID Broker Privilege Management is a Privilege Management API and web-interface, that allows organizations to create and administrate privileges specific for their own services and allows organizations to assign privileges and roles to the employees of their organizations.

Both the API and the web-interface is tailored towards two overall usages

- Privilege organization administration
- Privilege user assignment

This document focuses on privilege administration and the integration for organizations that creates and administrates their own privileges.

Getting started

Privileges can be created and administrated through the API and/or via the web-interface. Signaturgruppen will help with the initial onboarding of API clients and administrative users for access to the API and web-interface.

As the system matures, processes will be introduced that help automate and control the onboarding of the various types of administrative and supporting roles that need access to the system, but initially it will be kept to a minimum to get the basics up and running.

Privileges

The privileges data model is based on the OIO Basic Privilege Profile [OIO-Priv-Profile], with support for organization scopes and privileges in first versions.

When a user has logged into a service using Nets eID Broker, then the retrieved access token can be used to get the privileges for the user, if the “privileges” scope has been specified for the login.

The returned JSON from the privileges API contains the identity of the end-user, the receiving organization and the list of privileges assigned to the end-user scoped to the receiving organization.

An example of privileges for a specific end-user who has been authenticated towards a service under the “Privileges Demo Organization”, could be like:

```
{
  "identity": {
    "idp": "mitid_demo",
    "idp_identity_id": "tuetest1"
  },
  "client_organization": {
    "id": "afa009de-d523-437c-8cc0-9b4208d7f2c6",
    "name": "Privileges Demo Organization",
    "cvr": "DK00000002"
  },
  "privilege_scopes": [
    {
      "organization_id": "84e11a16-d93b-48a6-8dad-bf5ef26f31be",
      "organization_cvr": "DK29915938",
      "organization_name": "Signaturgruppen A/S",
      "privileges": [
        {
          "id": "db4fbc0e-9d04-4c3c-5bd6-08dad14a0997",
          "name": "Supporter"
        },
        {
          "id": "ec94f8bc-f38d-4abc-76c8-08dad14a2dfc",
          "name": "Revisor"
        }
      ]
    },
    {
      "organization_id": "afa009de-d523-437c-8cc0-9b4208d7f2c6",
      "organization_cvr": "DK00000002",
      "organization_name": "Privileges Demo Organization",
      "privileges": [
        {
          "id": "24c7a2ab-492d-4d4c-76c9-08dad14a2dfc",
          "name": "Administrator"
        },
        {
          "id": "db4fbc0e-9d04-4c3c-5bd6-08dad14a0997",
          "name": "Supporter"
        }
      ]
    }
  ]
}
```

Administration of privileges

It is possible to create and administrate privileges using the API or web-interface.

The core functionality contains possibility to create privileges consisting of

- Name
- Description and information
- Assignability
- ID (automatically created, GUID)
- Owning organization id (automatically set, GUID)

After creation, a privilege description and assignability can be modified using API or the web-interface, but the owning organization, id and name is not changeable.

Assignability

The assignability of a privilege refers to the audience of privilege user administrators able to see and assign these privileges when using the API or web-interface as a privilege assigner.

Assignability variants:

- Private: Only assignable by owning organization
- Public: Any privilege user administrator may see and assign the privilege to own employees
- Whitelist: Only owning organization and privilege user administrator specifically whitelisted can see and assign this privilege.

If the assigning organization is no longer whitelisted, the assignment is no longer active. The assignment is still visible for the organization who made the assignment so that this can still be deleted, and it may become active again later, if the assigning organization is again whitelisted.

If an assignment is not active, it will not be returned when listing “runtime” privileges for a specific end-user and thus is not listed for an authenticated user.

Assigning privileges

A privilege administrator can assign privileges to the employees of one or more organizations.

A privilege administrator for “test-org” can list and assign privileges conforming to:

- Privileges created by test-org
- Privileges with public assignability
- Privileges with test-org whitelisted assignability

A privilege administrator is always able to lookup and see all assigned privileges made by the respective organization, unless the privilege has been deleted, for which all assignments for this privilege will be deleted as well.

The available privileges will be listed under the owning organizations and will include the description field for each privilege.

At runtime, a change in privilege state or assignability will dynamically affect the output of assigned privileges to end-users, when checking their assigned privileges, such that these returned assignments always conforms to the current state of the assignments and takes assignability into account.

Privileges API

The privileges API implements the full functionality of the Nets eID Broker Privilege Management ecosystem and can be used by all roles of the integration as a compliment or replacement for using the web-interface.

Getting runtime privileges for end-users can only be achieved using the API.

The API is documented using Swagger, which can be found (when ready), at:

Environment	Swagger URL
Pre-Production (PP)	https://pp.netseidbroker.dk/privileges-api/swagger/index.html
Production	https://netseidbroker.dk/privileges-api/swagger/index.html

Service integration

The API integration (system to system) is done using the OAuth Client Credentials flow using a secure client with a client ID and a client secret (shared secret or asymmetric keys) to retrieve a bearer token (service token), then enabling calling the privileges API.

Onboarding of the API clients will be facilitated by Signaturgruppen or by the integrating organizations in the Nets eID Broker Administrative web-interface when access to this interface has been granted.

To retrieve a valid service token (bearer token) for the privileges API, invoke the Client Credentials flow with standard Token endpoint (Client Credentials) parameters and setting the scope parameter to include “privileges_api”.

Technical documentation for the integration to Nets eID Broker Privilege Management is found at

https://signaturgruppen-a-s.github.io/privilege-management-docs/

Privileges management web-interface

The privileges management web-interface contains the functionality needed by both privileges administrators and privilege assigners and will in time offer functionality to help onboard both small and large organizations into the Nets eID Broker Privilege Management eco-system.

All core functionalities can also be accessed via API directly, but some workflows and onboarding processes will require the use of the web-interface.

The privileges management web-interface will automatically adapt to the privileges of the user logging in and thus allow tailored usage of the different work-roles for the privilege setup.

The web-interface can be found (when ready), at:

Environment	URL
Pre-Production (PP)	https://pp.netseidbroker.dk/privileges
Production	https://netseidbroker.dk/privileges

It will be possible to login with NemID and MitID Erhverv employee identities, as well as a special “MitID Demo” login available in the test environment.

References

1. [OIO-Priv-Profile]: “OIO Basic Privilege Profile”: https://digst.dk/media/20999/oiosaml-basic-privilege-profile-1_2.pdf