SignaturGruppen

Nets eID BROKER

Sessions

Version 0.9 2021

Table of Contents

Terminology

Term	Description
Nets eID Broker (**NEB**)	Nets eID Broker. Certified MitID Broker and general broker and identity provider for enterprise services.

Changelog

Version 0.9

- Created this document. Moved information away from the “Technical Reference” and consolidated the information in this document.

Introduction

This document describes the technical setup around sessions in Nets eID Broker (NEB), how session are handled by NEB and the various ways to handle sessions as a service provider integrating to NEB.

The intended audiences are IT developers and IT architects.

Business functionality specified in this document may be subject to different commercial agreement requirements.

General information, online demonstration, documentation (including newest version of this document) and example code is found at https://broker.signaturgruppen.dk.

Sessions

NEB automatically issues or updates an end-user session upon all successful authentication flows.

Sessions generally lives for hours (see session_expiry), but various mechanism available to integrating setups allow a fine-grained control and usage of the NEB end-user session.

As default, each integrating client (OIDC client_id), has their own end-user session with the end-user which is not shared across other clients or services. Setting up a SSO allows for sharing sessions between services.

ID token session information

The returned ID token contains the following claims relevant for session handling

Claim	Description
session_expiry	Session expiry. Contains the absolute expiry time of the issued NEB end-user session in Epoch Unix Timestamp format. This time also indicates the period of which other session may be created based on the ID token. If the authentication from NEB is used to create an internal setup with e.g., a SSO setup, then the session expiry indicates when it is no longer allowed to create new logins and session based on the ID token issued by NEB.
neb_sid	Session identifier. Reference to the active NEB session.
auth_time	Authentication time. Time when the end-user authentication occurred in Epoch Unix Timestamp format.

Authentication request control of session usage

Parameter	Description
max_age	Maximum Authentication Age. Specifies the allowable elapsed time in seconds since the last time the end-user was actively authenticated by NEB. If the elapsed time is greater than this value, NEB will ensure to actively re-authenticate the end-user.
prompt	Space delimited, case sensitive list of ASCII string values that specifies whether the Authorization Server prompts the end-user for reauthentication. Supported values are • **none** (no ui for authentication) • **login** (force authentication request) • **select_account** (enable idp selection) If **login** is used, the end-user will be forced to complete the requested authentication flow. This can be used anytime it is required that the end-user completes the requested authentication flow, i.e. when requesting a signature from the end-user. If **none** is used, a request for automatic login based on the end-user session is requested. If the automatic login could not be honored, an error will be returned to the service. If **select_account** is used, the end-user will be allowed to select among the available identity providers for the given flow, even though the end-user has an active session with NEB. It does not trigger a forced reauthentication, so if the end-user selects the same identity provider for which he has an active session, he will be automatically reauthenticated.

Max age and authentication time

The **max_age** authentication parameter can be used to control how old an existing session can be before triggering a new authentication entirely.

The **auth_time** claim in the ID token will always contain the authentication time of the session which the token is issued from. In this way the **auth_time** can be verified to ensure that the authentication was processed within the expected and/or allowed timeframe.

Client specific default max_age via ADM-UI

ADM-UI supports setting a default max_age for a specific client, enabling control of the default maximum time from authentication before a new authentication must be processed for the end-user.

Session management

Session management is supported by the methods described in this section.

OpenID Connect Prompt none

An authentication request with the **prompt=none** will return with a specific error code if the end-user session is no longer valid for the requested authentication or return with updated tokens if the session is still active.

Session state from API endpoint

Under development

An API is under development, which will enable retrieval of session state based on the supplied ID token.

The ID token may be expired and information like that of OIDC session management (iframe) can be expected (unchanged/changed).

Logout

See “Nets eID Broker Technical Reference” for reference to API swagger information.

End session endpoint

The OpenID Connect End Session Endpoint is supported.

A valid ID token sent in the id_token_hint parameter is mandatory when calling the NEB End session endpoint.

Redirecting the end-user to the End Session endpoint with a valid ID token will result in the session identified by the ID token will be terminated and all clients who have actively participated in the session will have their registered Back-Channel endpoint called with a Logout Token notification.

See [OIDC-BACK-CHANNEL] section 2.6 for more information on the Logout Token.

When done, the optional post_logout_redirect_uri parameter is used to redirect the end-user back to the post logout URI if specified. If a valid post_logout_redirect_uri is omitted, the end-user will not be redirected back to the service provider.

NEB will ensure to call required logout endpoints at the external identity provider if required.

Logout API endpoint

The Logout endpoint is a NEB specific endpoint performing the SLO ceremony involved for logging out the end-user session.

Calling the API endpoint with a valid ID token will result in the session identified by the ID token will be terminated and all clients who have actively participated in the session will have their Back-Channel endpoint called with a Logout Token notification. Note, that it is optional to register a Back-Channel endpoint.

See [OIDC-BACK-CHANNEL] section 2.6 for more information on the Logout Token.

After calling the Logout API endpoint the ID token should be discarded.

NEB will ensure to call required logout endpoints at the external identity provider if required.

Single-Sign-On and Single-Log-Out (SSO and SLO)

Neb supports various setups utilizing SSO either directly through NEB or identity providers like MitID.

This section will be updated at a later stage. Contact Signaturgruppen if you plan on utilizing SSO either directly through NEB or via MitID.

References

1. [OIDC-SESSION]: ”OpenID Connect Session Management” - https://openid.net/specs/openid-connect-session-1_0.html
2. [OIDC-FRONT-CHANNEL]: ”OpenID Connect Front-Channel Logout” - https://openid.net/specs/openid-connect-frontchannel-1_0.html
3. [OIDC-BACK-CHANNEL]: ”OpenID Connect Back-Channel Logout” - https://openid.net/specs/openid-connect-backchannel-1_0.html