Security

security, authentication, authorization

API authentication

API access requires the user to be authenticated, excluding a few public endpoints. We can divide the sign in into two parts:

- authentication - the user proves his identity
- authorization - the user has access to given resource

Authentication

Authentication is realized through a request filterchain. The filters must always follow specified behavior:

- if credentials are OK, continue to authorization
- if credentials do not match, pass request to another filter in chain

In reality there is only one authentication servlet filter - `AuthenticationFilter`. Others filters are Spring beans implementing `IdmAuthenticationFilter` interface. An exception in filters is the `ExtendExpirationFilter`, which is another servlet filter handling the extension of expiration date of JWT tokens. This filter also controls possible exceptions in authentication flow.

Authorization and JWT token

User authorization is checked on the API endpoint layer and enforced by Spring Security. The content of IdM JWT:

- currentUsername - effective user's login
- originalUsername - logged user's login
- currentIdentityId - effective user's ID
- originalIdentityId - logged user's ID
- exp - token expiration date
- iat - issued at date

All IdM JWT tokens are signed using HMAC256 algorithm. The symmetric encryption key is configuration property of CzechIdM, stored as "idm.sec.security.jwt.secret.token". Default token expiration time is 10 minutes. JWT tokens are persisted in database (`IdmToken` entity) with assigned authorities. When identity is logged out, token is disabled. Disabled and expired tokens are purged periodically by internal scheduled task.

Backend of CzechIdM supports immediate detection of user's authorization change. Each modification type is implemented as application event processor, for further details please check the source code and tests :) When user's authorization changes, then persisted tokens, which user owns, are disabled

⇒ user is logged out. Types of modifications:

- removal of role, which carries application permissions ⇒ user losses some permission.
- disabling the user
- role's permissions change - revokes tokens of all users which have the role assigned

Devel Guide

tsort