Textové poleObsah obrázku logo, Písmo, symbol, Grafika

Popis byl vytvořen automaticky

Vytvořeno: 02. 02. 2024

Verze: 1.0

**© DIA**

Konfigurace Keycloak jako SeP pomocí SAML

Obsah

[1. Konfigurace na straně Keycloak – Instalace a spuštění 3](#_Toc157825967)

[2. Konfigurace na straně Keycloak – AdminConsole 4](#_Toc157825968)

[2.1. Bez rozšiřujících atributů 4](#_Toc157825969)

[2.1.1 General Settings 4](#_Toc157825970)

[2.1.2 SAML settings 4](#_Toc157825971)

[2.1.3 Requested AuthnContext Constraints – nastavení LOA 6](#_Toc157825972)

[2.1.4 Konfigurace certifikátů pro podpis a šifrování 6](#_Toc157825973)

[2.2. Konfigurace rozšířených atributů 7](#_Toc157825974)

[3. Konfigurace na straně CAAIS 9](#_Toc157825975)

[4. Zkratky, pojmy, definice 10](#_Toc157825976)

# Konfigurace na straně Keycloak – Instalace a spuštění

Keycloak byl nainstalován prostřednictvím OpenShift Keycloak Operátora (RedHat build of Keycloak) s následujícími konfiguračními úpravami:

apiVersion: k8s.keycloak.org/v2alpha1

kind: Keycloak

metadata:

  name: keycloak

  namespace: keycloak

spec:

  additionalOptions:

    - name: spi-connections-http-client-default-client-keystore-password

      secret:

        key: password

        name: custom-provider-keystore

    - name: spi-connections-http-client-default-client-key-password

      secret:

        key: password

        name: custom-provider-keystore

    - name: spi-connections-http-client-default-client-keystore-type

      value: PKCS12

    - name: spi-connections-http-client-default-client-keystore

      value: /mnt/custom-provider-keystore/keystore

  db:

    host: ...

    passwordSecret:

      key: ...

      name: ...

    usernameSecret:

      key: ...

      name: ...

    vendor: postgres

  hostname:

    hostname: ...

  http:

    tlsSecret: ...

  instances: 1

  unsupported:

    podTemplate:

      spec:

        containers:

          - volumeMounts:

              - mountPath: /mnt/custom-provider-keystore

                name: custom-provider-keystore

        volumes:

          - name: custom-provider-keystore

            secret:

              secretName: custom-provider-keystore

Vzhledem k množství způsobů instalace a konfigurace systému Keycloak považujeme pokusy o zobecnění výše uvedeného manifestu do jiných forem za kontraproduktivní a necháváme případnou transformaci na čtenáři. Manifest je tedy uveden především pro inspiraci.

Pro úplnost k výše uvedené konfiguraci je vhodné doplnit, že odkazovaný Kubernetes secret obsahuje dva klíče:

1. keystore: binární PKCS12 soubor
2. password: heslo k keystore i privátnímu klíči v něm (tj. obě hesla jsou stejná)

# Konfigurace na straně Keycloak – AdminConsole

## Bez rozšiřujících atributů

### General Settings

* Obsah obrázku text, Písmo, řada/pruh, snímek obrazovky

  Popis byl vytvořen automatickyMůže být nastaveno libovolně – důležitá je zde Redirect URI – tento parametr je potřeba pro správné nastavení AIS v CAAIS

### SAML settings

* Service provider entity ID – libovolné – zadává se jako zkratka AIS do CAAIS
* Identity provider entity ID – Entity id CAAIS – z metadat vystavených systémem CAAIS
* SSO url – URL CAAIS – z metadat vystavených systémem CAAIS
* Logout url – URL CAAIS – url pro odhlášení
* Další nastavení vychází z obecného nastavení CAAIS (je vyžadováno podepisování a šifrování, nameId je typu persistent, podporované a používané algoritmy CAAIS (systémová nastavení v CAAIS))
* Validating X509 certificate – Veřejná část certifikátu, kterým podepisuje CAAIS odpověď – z metadat CAAIS

Obsah obrázku text, snímek obrazovky, číslo, Paralelní

Popis byl vytvořen automaticky

### Requested AuthnContext Constraints – nastavení LOA

Obsah obrázku text, řada/pruh, Písmo, číslo

Popis byl vytvořen automaticky

### Konfigurace certifikátů pro podpis a šifrování

* Obsah obrázku text, řada/pruh, číslo, Písmo

  Popis byl vytvořen automatickyJe potřeba správně nastavit providery certifikátů: rsa a rsa-enc
* Následně tyto mít mezi klíči správně přiřazené pro použití SIG a ENC

Obsah obrázku text, snímek obrazovky, Písmo, číslo

Popis byl vytvořen automaticky

* Veřejné části těchto certifikátů se zadávají do AIS v CAAIS.
* Se základní konfigurací se lze do keycloak přihlásit a CAAIS posílá pouze atribut nameId.

## Konfigurace rozšířených atributů

* Keycloak v základní instalaci nemá podporu rozšiřujících požadavků pro SAML AuthnRequest.
* Pro přidání této možnosti je potřeba použít keycloak extension (<https://www.keycloak.org/extensions.html>).
* Pro ukázku byla upravena extension Eidas Keycloak Extension (<https://github.com/grnet/eidas-keycloak-extension>) (Upravena, aby nevyžadovala zemi…).
* Je použit json požadující všechny atributy, které CAAIS nabízí.

[{"Name":"http://eidas.europa.eu/attributes/naturalperson/PersonIdentifier",  
 "NameFormat": "urn:oasis:names:tc:SAML:2.0:attrname-format:uri", "isRequired":false  
 },  
 {"Name":"http://eidas.europa.eu/attributes/naturalperson/CurrentFamilyName",  
 "NameFormat": "urn:oasis:names:tc:SAML:2.0:attrname-format:uri", "isRequired":false},  
 {"Name":"http://eidas.europa.eu/attributes/naturalperson/CurrentGivenName",  
 "NameFormat": "urn:oasis:names:tc:SAML:2.0:attrname-format:uri", "isRequired":false},  
 {"Name":"http://eidas.europa.eu/attributes/naturalperson/DateOfBirth",  
 "NameFormat": "urn:oasis:names:tc:SAML:2.0:attrname-format:uri", "isRequired":false},  
 {"Name":"http://eidas.europa.eu/attributes/naturalperson/PlaceOfBirth",  
 "NameFormat": "urn:oasis:names:tc:SAML:2.0:attrname-format:uri", "isRequired":false},   
 {"Name":"http://www.stork.gov.eu/1.0/countryCodeOfBirth",  
 "NameFormat": "urn:oasis:names:tc:SAML:2.0:attrname-format:uri", "isRequired":false},   
 {"Name":"http://www.stork.gov.eu/1.0/eMail",  
 "NameFormat": "urn:oasis:names:tc:SAML:2.0:attrname-format:uri", "isRequired":false},   
 {"Name":"http://eidas.europa.eu/attributes/legalperson/LEI",  
 "NameFormat": "urn:oasis:names:tc:SAML:2.0:attrname-format:uri", "isRequired":false},   
 {"Name":"http://eidas.europa.eu/attributes/naturalperson/PlaceOfBirth",  
 "NameFormat": "urn:oasis:names:tc:SAML:2.0:attrname-format:unspecified", "isRequired":false},  
 {"Name":"LegalEntityShortcut",  
 "NameFormat": "urn:oasis:names:tc:SAML:2.0:attrname-format:unspecified", "isRequired":false},  
 {"Name":"Username",  
 "NameFormat": "urn:oasis:names:tc:SAML:2.0:attrname-format:unspecified", "isRequired":false},  
 {"Name":"DegreeBefore",  
 "NameFormat": "urn:oasis:names:tc:SAML:2.0:attrname-format:unspecified", "isRequired":false},  
 {"Name":"DegreeAfter",  
 "NameFormat": "urn:oasis:names:tc:SAML:2.0:attrname-format:unspecified", "isRequired":false},  
 {"Name":"AccessRoles",  
 "NameFormat": "urn:oasis:names:tc:SAML:2.0:attrname-format:unspecified", "isRequired":false},  
 {"Name":"ActivityRoles",  
 "NameFormat": "urn:oasis:names:tc:SAML:2.0:attrname-format:unspecified", "isRequired":false},  
 {"Name":"LegalEntityName",  
 "NameFormat": "urn:oasis:names:tc:SAML:2.0:attrname-format:unspecified", "isRequired":false},  
 {"Name":"LegalEntityEmail",  
 "NameFormat": "urn:oasis:names:tc:SAML:2.0:attrname-format:unspecified", "isRequired":false},  
 {"Name":"InstitutionType",  
 "NameFormat": "urn:oasis:names:tc:SAML:2.0:attrname-format:unspecified", "isRequired":false},  
 {"Name":"PersonIdentified",  
 "NameFormat": "urn:oasis:names:tc:SAML:2.0:attrname-format:unspecified", "isRequired":false},  
 {"Name":"DateOfDeath",  
 "NameFormat": "urn:oasis:names:tc:SAML:2.0:attrname-format:unspecified", "isRequired":false},  
 {"Name":"DocumentIds",  
 "NameFormat": "urn:oasis:names:tc:SAML:2.0:attrname-format:unspecified", "isRequired":false},  
 {"Name":"PublicOrganizationIdentifier",  
 "NameFormat": "urn:oasis:names:tc:SAML:2.0:attrname-format:unspecified", "isRequired":false},   
 {"Name":"AuthorizedPrivateEntityPersonalDataUserIdentifier",  
 "NameFormat": "urn:oasis:names:tc:SAML:2.0:attrname-format:unspecified", "isRequired":false},   
 {"Name":"TimeLimitedId",  
 "NameFormat": "urn:oasis:names:tc:SAML:2.0:attrname-format:unspecified", "isRequired":false}   
]

* Dále je potřeba pro požadované atributy nadefinovat mapování:

Obsah obrázku text, snímek obrazovky, číslo, Písmo

Popis byl vytvořen automaticky

# Konfigurace na straně CAAIS

* Na straně CAAIS je potřeba, aby byl založený AIS,
* zkratka AIS musí odpovídat service provider entity Id v Keycloak,
* v návratových url pro SAML na AIS musí být uvedena Redirect URI z Keycloak,
* v certifikátech na AIS musí být vloženy veřejné části certifikátů z Keycloak (SIG-podepisovací, ENC-šifrovací)
* AIS musí být správně povolen pro domény, mít povolené vyžadované identity providery a mít nastavené minimální LOA

# Zkratky, pojmy, definice

|  |  |
| --- | --- |
| **Zkratka/pojem** | **Vysvětlení** |
| AIS | Agendový informační systém |
| CAAIS | Centrální autorizační a autentizační informační systém, náhrada JIP/KAAS |