MojeID

Autentizační protokoly

Jaromír Talíř • jaromir.talir@nic.cz • 13. 11. 2015

CZ.NIC | SPRÁVCE DOMÉNY CZ

Obsah

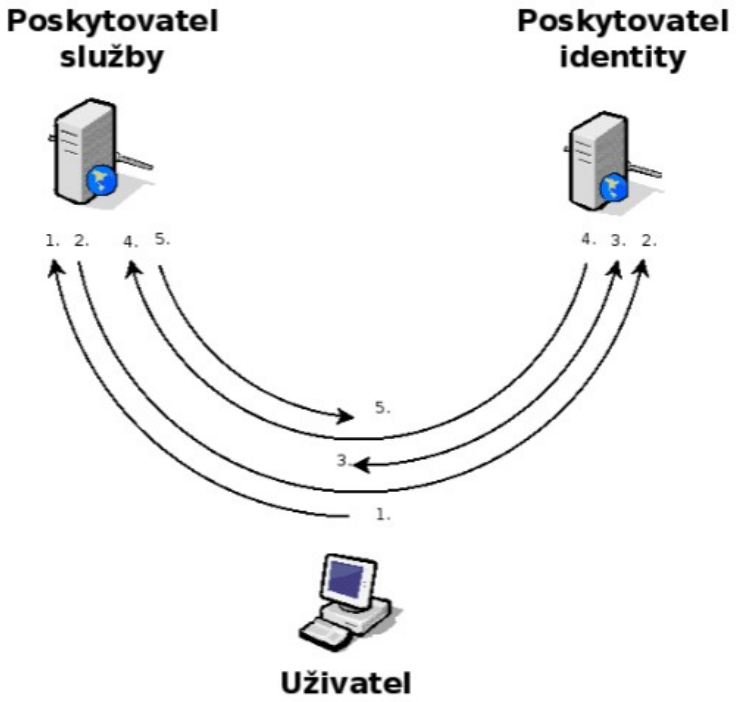
- mojeID a autentizačních protokoly
- Obecné schéma a historie
- OpenID 2.0
- SAML 2.0
- OpenID Connect

mojeID a autentizační protokoly

- Systém elektronické identity (eID) od CZ.NIC – www.mojeid.cz
- Hlavní vlastnosti
  - Jednotné přihlašování (Single Sign On)
  - Centrální správa identity
  - Důvěryhodné předávání atributů
- Implementace standardizovaným způsobem – autentizační protokoly

Obecné schéma

- Počáteční nastavení důvěry
- Identita, zjišťování vlastností
  -„discovery“
- Prohlášení o uživatelově identitě
  - „assertion“
- Předávání dalších údajů
  - „front channel“ vs. „back channel“



Historie

- 1993 - Kerberos 5
- 2002 - SAML 1.0
- 2005 - **SAML 2.0**, OpenID 1.0
- 2007 - **OpenID 2.0**
- 2011 - Mozilla BrowserID/Persona
- 2014 - **OpenID Connect**

SAML 2.0

- Manuální registrace metadat, X.509 certifikáty
- Není formálně definovaná identita, proces zjišťování řeší WAYF/DS
- Assertion ve formátu XML zpráva podepsaných XMLDsig
- Atributy součástí Assertion (front channel) nebo přístupné přes SOAP (back channel)

SAML 2.0 v mojeID

- Implementace PySAML2 od Rolanda Hedberga
- Pouze HTTP POST a HTTP Redirect bindings
- Využití pro integraci se systémy podporující pouze SAML
- Projekt přeshraniční elektronické identifikace STORK
- Akademická federace identit EduID

OpenID 2.0

- Není nutná registrace služeb, vše se řeší dynamicky. Ustanovení asociace s výměnou klíčů pomocí Diffie-Hellman
- Identita jako URL nebo XRI, YADIS protokol pro „discovery“ proces, XRDS dokument obsahující metadata
- Standardizovaný způsob jak serializovat data odpovědi a podepsat přes HMAC
- Atributy jsou součástí odpovědi (pouze „front channel“)

OpenID 2.0 v mojeID

- Implementace python-openid od JanRain
- První a stále hlavní autentizační protokol v mojeID
- Kontrola poskytovatelů přes jejich XRDS dokument – problém pro implementátory
- Knihoven je velké množství, ale obsahují I chyby

OpenID Connect

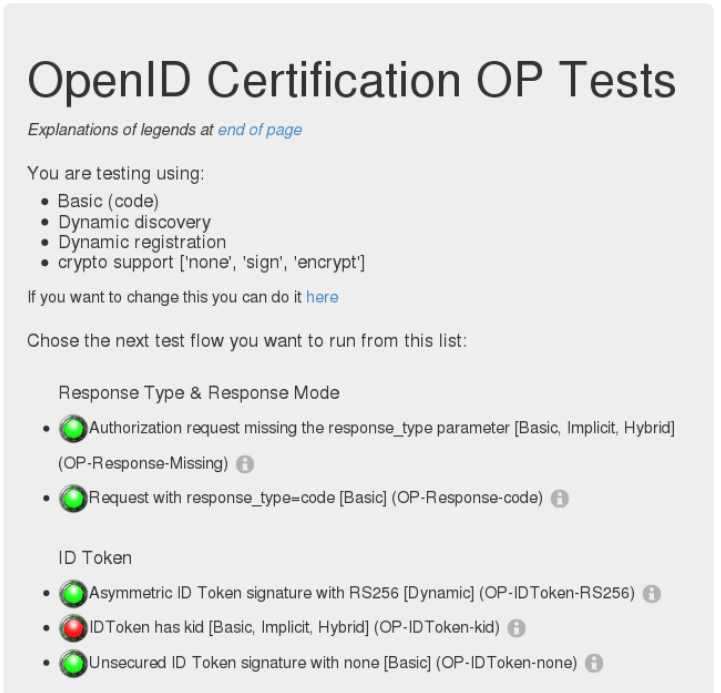
- Manuální nebo dynamická registrace služby u poskytovatele identit
- Identita je URL nebo email, Webfinger protokol pro „discovery“, JRD dokument obsahující informace
- Assertion ve formě JWT (JSON Web Token) podepsané JWS (JSON Web Signature)
- Data mohou být součástí JWT („front channel“) nebo mohou být vyžádána službou napřímo

OpenID Connect v mojeID

- Implementace PyOIDC od Rolanda Hedberga
- Jednoduchá JS knihovna https://www.mojeid.cz/mojeidconnect/
- Podpora dynamické registrace
- Zatím není moc poskytovatelů služeb
- Připravujeme „offline mód“

OpenID Connect - certifikace

- https://openid.net/certification



OpenID Certification OP Tests

Explanations of legends at end of page

You are testing using:

- Basic (code)
- Dynamic discovery
- Dynamic registration
- crypto support ['none', 'sign', 'encrypt']

If you want to change this you can do it here

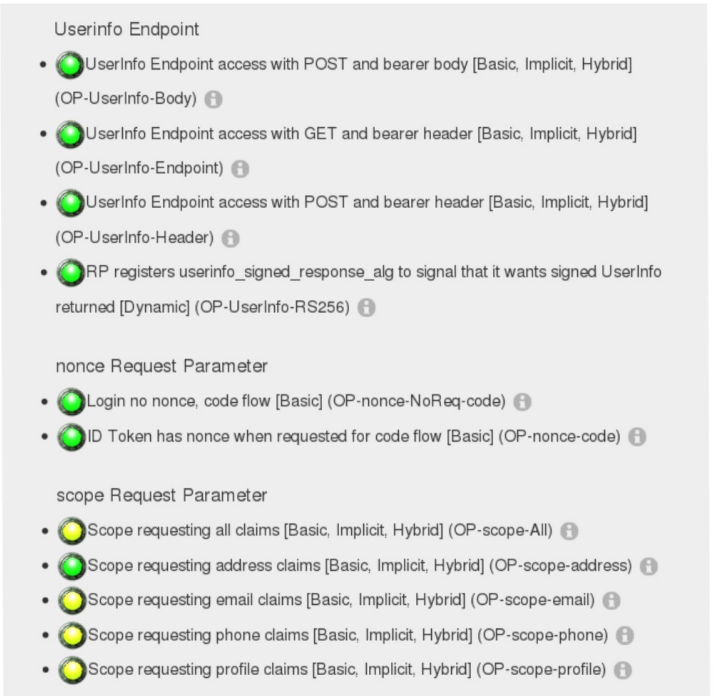
Chose the next test flow you want to run from this list:

Response Type & Response Mode

- Authorization request missing the response_type parameter [Basic, Implicit, Hybrid] (OP-Response-Missing)
- Request with response_type=code [Basic] (OP-Response-code)

ID Token

- Asymmetric ID Token signature with RS256 [Dynamic] (OP-IDToken-RS256)
- IDToken has kid [Basic, Implicit, Hybrid] (OP-IDToken-kid)
- Unsecured ID Token signature with none [Basic] (OP-IDToken-none)



Userinfo Endpoint

- UserInfo Endpoint access with POST and bearer body [Basic, Implicit, Hybrid] (OP-UserInfo-Body)
- UserInfo Endpoint access with GET and bearer header [Basic, Implicit, Hybrid] (OP-UserInfo-Endpoint)
- UserInfo Endpoint access with POST and bearer header [Basic, Implicit, Hybrid] (OP-UserInfo-Header)
- RP registers userinfo_signed_response_alg to signal that it wants signed UserInfo returned [Dynamic] (OP-UserInfo-RS256)

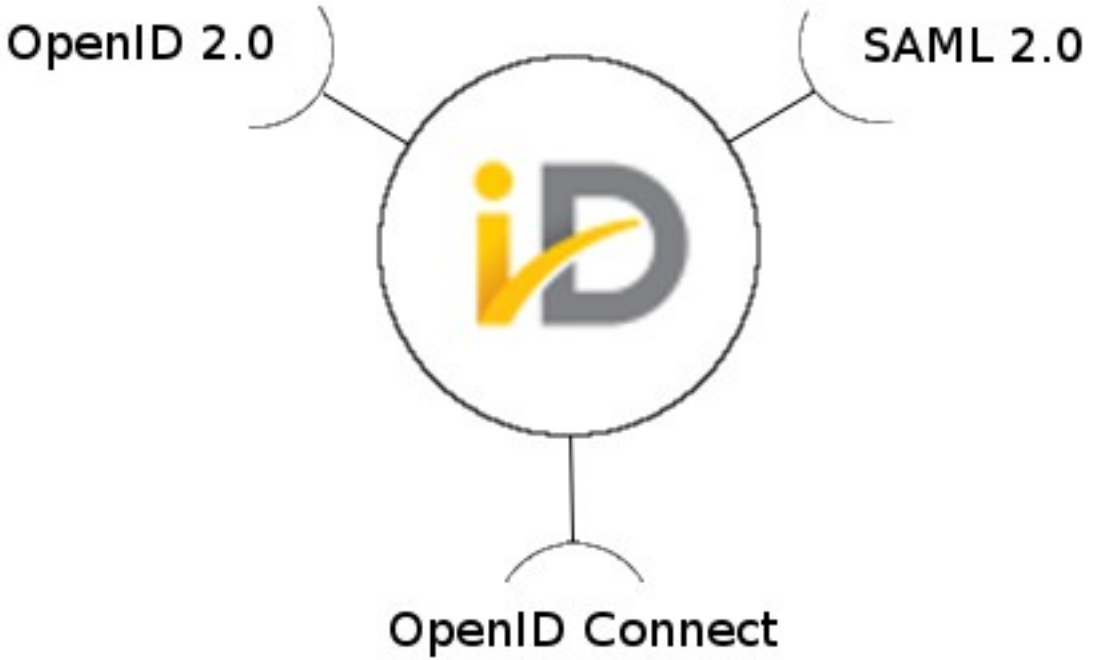
nonce Request Parameter

- Login no nonce, code flow [Basic] (OP-nonce-NoReq-code)
- ID Token has nonce when requested for code flow [Basic] (OP-nonce-code)

scope Request Parameter

- Scope requesting all claims [Basic, Implicit, Hybrid] (OP-scope-All)
- Scope requesting address claims [Basic, Implicit, Hybrid] (OP-scope-address)
- Scope requesting email claims [Basic, Implicit, Hybrid] (OP-scope-email)
- Scope requesting phone claims [Basic, Implicit, Hybrid] (OP-scope-phone)
- Scope requesting profile claims [Basic, Implicit, Hybrid] (OP-scope-profile)

mojeID a autentizační protokoly



Máte chuť spolupracovat?

- Na vývoji mojeID a dalších našich webových službách
  - **Webový vývojář pro Python/Django**
- Na provozu mojeID, doménové registru, DNS Anycastu,...
  - **Systémový administrátor**

- http://www.nic.cz/kariera/

Děkuji za pozornost

Jaromír Talíř • jaromir.talir@nic.cz