Shibboleth2 DiscoveryService

Shibboleth2 Discovery Service

A Discovery Service ugyanazt a szerepet játssza a Shibboleth2 infrastruktúrában mint a WAYF szolgáltatás a Shibboleth1.x esetén. A WAYF szolgáltatás azonban Shibboleth-specifikus, míg a Discovery Service pontos működését a SAML2.0 szabvány írja le.

Részletes konfigurációs segédlet a Shibboleth2 Wikin

Az IdP Discovery menete

A Discovery Service (DS) feladata tehát, hogy az SP számára kiválasszon egy IdP-t, amit a felhasználó használ. Ezt alapvetően kétféleképpen éri el: cookie-k illetve egy webes IdP kiválasztó felület segítségével.

Amennyiben a DS cookie-ban tárolja a felhasználó által kiválasztott IdP-t, ezt egy _saml_idp nevű cookieban kell tennie, aminek a formátuma kötött: egy darab space-szel elválasztott, base64 kódolt IdP entityID lista (tehát több IdP-t is képes tárolni, és a használati sorrendet is megőrzi - bár utóbbit nem teszi kötelezővé a szabvány).

A Shibboleth2 DS képes arra, hogy a cookie-k használatán kívül a felhasználónak egy webes formot mutasson, amiben a federációk és az egyes federációkban szereplő IdP-k listáját jeleníti meg. Ezt a listát a felhasználó egy szöveges kereső segítségével szűrheti is.

A Discover Service metaadatok konfigurálása

A DS konfigurálása a wayfconfig.xml fájl segítségével történik. Itt kell megadni a használt template-et és a metaadatokat is. A metaadatokat ugyanazon formátumban kell konfigurálni mint az IdP esetén (tehát lehetőség van egy URL-ről automatikusan letöltött metaadat-állomány használatára is).

A DS-nek ismernie kell a kérő SP metaadatát is, alapbeállításként pedig csak azokat az IdP-ket listázza, amelyek egy metaadat-fájlban vannak az aktuális SP-vel.

Discovery Service pluginek

A DS kiterjeszthető olyan pluginekkel, amelyek segítik a felhasználót az IdP választásban. Ilyen plugin például a _saml_idp cookie kezelő, ami SAML2 szabvány-kompatibilissé teszi a DS-t.

Változat #1
document-uploader hozta létre 2025-08-07 12:03:09 CEST
document-uploader frissítette 2025-08-07 12:03:09 CEST