IsPassive

Az **isPassive** SAML2-ben bevezetett lehetőség, mellyel azt szabhatjuk meg, hogy az azonosításnak úgy kell megtörténnie, hogy közben semmiféle látható felhasználói interakciónak nem szabad történnie. Ha az azonosítás így nem hajtható végre, akkor hibát kell visszaadni az SP-nek.

Miért jó?

Az isPassive használatával elérhetjük, hogy Lazy Session-nel védett oldalunkra a felhasználó bejelentkezése automatikusan - azaz "Bejelentkezés" gombra kattintás nélkül - megtörténjen. Ehhez három feltétel együttes teljesülése szükséges:

- a felhasználó már rendelkezik az IdP-je által hitelesített munkamenettel
- az IdP által használt autentikációs mechanizmus támogatja az isPassive-ot
  - erre kizárólag SAML2 IdP esetén van lehetőség
- ha használunk Discovery Service-t, akkor az a felhasználó IdP-jét képes megállapítani interakció nélkül
  - ez általában azt jelenti, hogy a felhasználónak van olyan cookie-ja, amely alapján a DS meg tudja határozni az IdP-t. Érdemes megjegyezni, hogy a SWITCH Discovery Service IP cím alapján is képes meghatározni IdP-t.

Amennyiben ezen feltételek közül valamelyik nem teljesül, úgy az SP hibát fog dobni. Ezt `redirectErrors` attribútum segítségével átirányíthatjuk a saját alkalmazásunkra.

Hátrányok

Lehetséges olyan helyzet, hogy a hiba nem jut vissza az SP-hez:

- az IdP nem SAML2-t használ
- az IdP azonosítási mechanizmusa nem támogatja a passzív azonosítást (pl. azért, mert webszerver-alapú azonosítást használ)
- a Discovery Service vagy a WAYF nem támogatja a passzív választást

Ebben az esetben a felhasználó olyan üzenetet kap, amit valószínűleg nem tud értelmezni. Pl.:

- hibaüzenet az IdP vagy a DS részéről
- IdP azonosítási felület (ami esetleg nem is a felhasználó IdP-je)

Ezért isPassive-ot csak abban az esetben szabad használni, ha garantálni tudjuk, hogy az IdP-k mind támogatják a passzív autentikációt!

M?ködése a gyakorlatban

- Az alábbi szkriptet szúrjuk be az oldalunk főlapjára / fejlécébe.
- A Shibboleth SP konfigurációjában (`shibboleth2.xml`) az adott alkalmazásra vonatkozó beállításoknál új attribútumként adjuk meg a `redirectErrors="SAJÁT KEZDŐLAPOM"` direktívát.
- Bizonyosodjunk meg róla, hogy az oldalt lazy session-nel védjük

Kód

```
<!-- START: isPassive script-->
<script type="text/javascript" language="javascript">
<!--
// Written by Lukas Haemmerle <lukas.haemmerle@switch.ch>, SWITCH

// Check for session cookie that contains the initial location
if(document.cookie && document.cookie.search(/_check_is_passive=/) >= 0){
	// If we have the opensaml::FatalProfileException GET arguments
	// redirect to initial location because isPassive failed
	if (
		window.location.search.search(/errorType/) >= 0
		&& window.location.search.search(/RelayState/) >= 0
		&& window.location.search.search(/requestURL/) >= 0
	) {
		var startpos = (document.cookie.indexOf('_check_is_passive=')+18);
		var endpos = document.cookie.indexOf(';', startpos);
		window.location = document.cookie.substring(startpos,endpos);
	}
} else {
	// Mark browser as being isPassive checked
	document.cookie = "_check_is_passive=" + window.location;

	// Redirect to Shibboleth handler
	window.location = "/Shibboleth.sso/DS?isPassive=true&target=" +
encodeURIComponent(window.location);
}
```

```
</script>
<!-- END: isPassive script-->
```

Változat #1
document-uploader hozta létre 2025-08-07 12:06:39 CEST
document-uploader frissítette 2025-08-07 12:06:39 CEST