eduPersonTargetedId

Naziv:	Pseudonim korisnika
LDAP naziv:	eduPersonTargetedId
Opis:	Trajan identifikator korisnika koji razmenjuju davalac servisa i davalac identiteta. Nikada se ne dodeljuje ponovo i ne sadrži nikakve podatke o korisniku. Davalac identiteta koristi odre?enu vrednost atributa kada komunicira sa odre?enim davaocem servisa ili grupom davaoca servisa i ne otkriva ovu vrednost ni jednom drugom davaocu servisa.
Ldap sintaksa:	DirectoryString
Dopuštene vrednosti:	Nema posebnog šifarnika
Status:	Opcionalan
Frekvencija:	N
Poreklo:	eduPerson
Referenca:	eduPerson200806
OID:	1.3.6.1.4.1.5923.1.1.1.10
Primer:	eduPersonTargetedId: kl83HlsnblqYskgh72Kfqkl

Napomene vezane za upotrebu atributa:

Ukoliko je davaocu servisa neophodno da može da prepozna istog korisnika u njegovim razli?itim sesijama, u tu svrhu može da koristi atribut eduPersonTargetedId. Naj?eš?a upotreba je personalizacija servisa odnosno ?uvanje preferenci korisnika kroz njegove sesije. Drugi razlog može biti potreba da se prati aktivnost korisnika radi spre?avanja zloupotrebe servisa.

Atribut omogu?ava instituciji da davaocu servisa pruži trajan, negovore?i (engl. opaque), identifikator korisnika. Svakom davaocu servisa kome se izdaje ovaj atribut, davalac identiteta daje druga?iju vrednost za odre?enog korisnika. Atribut može imati više vrednosti (po jedna vrednost za svakog davaoca servisa kome se atribut izdaje).

eduPerson specifikacija zahteva da jednom dodeljena vrednost atributa eduPersonTargetedId, nikada ne sme biti ponovo dodeljena drugom korisniku. Me?utim treba imati na umu da ne mogu svi davaoci identiteta garantovati da ?e odre?eni korisnik zauvek zadržati neku vrednost. Davaoci identiteta ?ak mogu svojim korisnicima dati opciju da se za njih generiše nova vrednost ako misle da im je privatnost ugrožena.

U zavisnosti od zahteva davaoca pristupa, vrednost može biti izražena u nekom od dva oblika. Format koji se ?esto koristi unutar Shibboleth zajednice ima ime atributa urn:mace:dir:attribute-def:eduPersonTargetedID i njegova sintaksa je @. Noviji format koji u ve?oj meri odgovara komercijalnim SAML implementacijama ima ime atributa urn:oid:1.3.6.1.4.1.5923.1.1.1.10 i on obuhvata ime entiteta davaoca pristupa, ime entiteta davaoca servisa i niz karaktera koji predstavljaju negovore?i indentifikator (pseudonim). Ove vrednosti su odvojene simbolom “!”. Ovaj format je podržan od strane Internet2 zajednice i može preuzeti primat nad prvim formatom.

EduPerson Specifikacija

Iako ovaj atribut ne mora biti sa?uvan u odre?enom direktorijumu, on može biti generisan od njegove strane. U svakom slu?aju, atribut se ovde definiše zbog njegove potencijalne upotrebe u drugim kontekstima servisa kao što su SAML assertions.

Vrednosti eduPersonTargetedId atributa ne treba dodeljivati ponovo.

Trajnost

Dodeljivanje vrednosti atributu eduPersonTargetedId nema definisano trajanje, ali bi ono trebalo da bude duže od jedne korisni?ke interakcije i dovoljno dugo da eduPersonTargetedId bude upotrebljiv kao klju? za odre?eni servis koji ga koristi. Tako?e se mogu koristiti procedure kojima se radi privatnosti korisnika vrednost atributa osvežava. Pritom se davalac servisa obaveštava o ovim promenama, tako da se funkcionalnost servisa ne gubi.

Privatnost

Ovaj atribut je osmišljen da bi se sa?uvala privatnost korisnika i da bi se onemogu?ilo da više nezavisnih servisa mogu da upore?ivanjem vrednosti dovode u uzajamnu vezu aktivnosti korisnika. Iz tog razloga je neophodno da bude negovore?i (engl. opaque) i da nema veze sa ostalim korisnikovim identifikatorima kao što je korisni?ko ime ili eduPersonPrincipalName. Tre?em licu bi trebalo biti teško da rekonstruiše vrednost koju treba vratiti odre?enom davaocu servisa.

Vrednost atributa može biti pseudo-slu?ajna vrednost koju generiše i ?uva davalac identiteta, ili može biti izvedena kao neka funkcija nad identitetom davaoca servisa i drugih podataka koji su jedinstveni za korisnika.

Maksimalna dužina je 256 karaktera.

Jedinstvenost

Odre?ena vrednost atributa namenjena je koriš?enju od strane specifi?nih servisa (obi?no samo jednog). Vrednosti atributa moraju biti jedinstvene unutar opsega davaoca identiteta i opsega davaoca servisa za koga je vrednost kreirana. Logi?ki, vrednost atributa se sastoji od trojke: identifikator, davalac identiteta i davalac servisa.

Ponovno dodeljivanje

Posebna odlika ovog atributa je da je zabranjeno njegovo ponovno dodeljivanje. Obzirom da je vrednost identifikatora negovore?a, ona osim identifikacije korisnika nema nikakvo drugo zna?enje. Zbog toga odre?ena vrednost atributa kreirana od strane davaoca identiteta ne sme biti ponovno dodeljena, tako da se spre?ava da se njime odre?eni davalac servisa referiše na razli?ite korisnike u

razli?itim vremenskim trenucima.

From:
http://www.bpd.amres.ac.rs/ - **AMRES wiki**

Permanent link:
http://www.bpd.amres.ac.rs/doku.php?id=amres_aai_wiki:rseduperson_edupersontargetedid

Last update: **2010/10/05 17:38**