

Kako izvršiti zamjenu certifikata za provjeru SSO autentikacije za uslugu Office 365?

VAŽNO - ovaj dio uputa odnosi se samo na ustanove koje su implementirale autentikaciju na Office365 putem sustava AAI@EduHr do 08. 07. 2020. Ustanove koje su (prvi put) registrirale Office 365 za autentikaciju putem sustava AAI@EduHr nakon 08. 07. 2020. već koriste novi certifikat!

Dana 11.07.2020 u 20:00h povlači se (Digicert-ov) root CA kojim je potpisan certifikat koji se koristi za provjeru valjanosti autentikacijskih odgovora koje AAI@EduHr SSO sustav proslijeđuje Office 365 aplikaciji što može utjecati na validaciju autentikacijskih odgovora i posljedično onemogućiti prijavu na sustav Office 365 e-identitetom iz sustava AAI@EduHr zbog čega je na strani Office 365 usluge potrebno evidentirati novi certifikat.

Obzirom da certifikat potrebno istodobno zamijeniti i na strani Office 365 servisa i na strani sustava AAI@EduHr, vrlo je važno administrator Office 365 usluge obaviti sve korake iz ovih uputa. Također, poželjno je da administrator usluge korisnicima najavi kratkotrajni prekid u radu usluge tijekom dogovorenog razdoblja.

Procedura zamjene certifikata sastoji se od sljedećih koraka:

1. Administrator Office 365 usluge treba dohvatiti novi certifikat s adrese:

https://login.aaiedu.hr/office365/module.php/saml/idp/certs.php/new_idp.crt

i pohraniti ga negdje na svom računalu, npr. u direktorij **C:\Users\korisnik\Downloads**

2. Koristeći Windows PowerShell administrator se naredbom:

```
connect-msolservice
```

treba prijaviti u **Windows Azure / Office 365** administrativno sučelje. **VAŽNO:** Za prijavu u PowerShell konzolu **OBAVEZNO** trebate koristiti korisnički račun oblika **proizvoljna_kor_oznaka@nekadomena.onmicrosoft.com**. Ni u kom slučaju korisnički račun oblika jednakog vašem elektroničkom identitetu iz sustava AAI@EduHr!!!

3. Nakon prijave, kroz PowerShell konzolu potrebno je izvršiti sljedeće naredbe (pritom umjesto **domena.hr** treba unijeti LDAP domenu matične ustanove):

```
$dom = "domena.hr"

set-msoldomainauthentication -authentication Managed -domainname $dom

$fedbrandname = "AAI@EduHr"

$url = "https://login.aaiedu.hr/office365/saml2/idp/SSOService.php?entityID=https://login.aaiedu.hr/office365/"
+$dom

$uri = "https://login.aaiedu.hr/office365/" + $dom

$logouturl = "https://login.aaiedu.hr/office365/saml2/idp/SingleLogoutService.php?ReturnTo=https://login.aaiedu.
hr/office365/logout.php"

$cert = New-Object System.Security.Cryptography.X509Certificates.X509Certificate2("C:
\Users\korisnik\Downloads\new_idp.crt")

$certdata = [system.convert]::toBase64string($cert.rawdata)

set-msoldomainauthentication -domainname $dom -federationbrandname $fedbrandname -authentication Federated -
passivelogonuri $url -signingcertificate $certdata -issueruri $uri -logoffuri $logouturl -
preferredauthenticationprotocol SAML
```

4. U sučelju registra resursa na adresi <https://registar.aaiedu.hr> evidentirati da resurs usluge Office365 vaše ustanove koristi novi certifikat.

Administrator resursa Office365 treba u Registru resursa otvoriti karticu "SAML konfiguracija" i potražiti redak **IdpCertFile**. U ovom retku nalazi se naziv datoteke certifikata koji je trenutačno označen kao aktivan. Za promjenu stanja kliknite na poveznicu "**Ažuriraj**":

Microsoft Office365 za korisnike ustanove XY

Opći podaci

SAML konfiguracija

RADIUS konfiguracija

Dodaj modul

1.

SAML konfiguracija

Opće postavke

AuthModule	Univerzalni
AttributeMapping	nijedna
ValidateAuthnRequest	ne
ValidateLogoutRequest	ne
NameIDAttribute	hrEduPersonUniqueID
NameIDFormat	urn:oasis:names:tc:SAML:2.0:nameid-format:transient
NameIDEncryption	ne
EncryptAssertion	ne
RedirectValidate	ne
ForceAuthn	ne
SignAssertion	ne
SignResponse	ne
SignLogout	ne
IdpCertFile	cert_20190810.pem

2.

[Ažuriraj]

Napomena: ovaj redak je vidljiv samo u resursima povezanim s globalnom uslugom Office365 i nad čijim SAML modulom nije trenutačno postavljen nikakav zahtjev za ažuriranjem.

Na stranici za odabir certifikata ispisani su podaci iz resursa usluge i podaci o certifikatu koji je trenutačno označen kao aktivan:

Odabir certifikata SSO servisa (idpCert) za uslugu Microsoft Office 365


Podaci o usluzi	
Opis	Usluga Office 365 za domenu srce.hr
Interna usluga	ne
Status resursa	Uključen
Vrsta resursa	Produkcija
Matična ustanova s kojom je resurs povezan	nijedna
Partner federacije s kojim je resurs povezan	Microsoft Hrvatska d.o.o.
Globalna usluga s kojom je resurs povezan	Microsoft Office 365
URL sjedišta usluge	http://login.microsoftonline.com

Podaci o aktivnom certifikatu	
Datoteka	login_aaiedu_hr_idp_072019.crt
Status	Stari
Opis	Certifikat kojim se potpisuje komunikacija SSO servisa s davateljem usluge. Ovaj certifikat vrijedi do 08. 09. 2021.
Datum isteka	08. 09. 2021.

Promjena certifikata

Odaberite certifikat:

☐ Stari


 Spremi promjene

Da biste stari certifikat zamijenili novim, potrebno je kliknuti gumb "Odaberite certifikat:" tako da prikazuje stanje **"Novi"**, a zatim kliknuti gumb **"Spremi promjene"**:


Promjena certifikata

Odaberite certifikat:

☒ Novi **1.**

 Spremi promjene **2.**

Promjene će se prikazati u tablici "Podaci o aktivnom certifikatu":

Podaci o aktivnom certifikatu	
Datoteka	login_aaiedu_hr_idp_20200708.crt
Status	Novi 
Opis	Certifikat kojim se potpisuje komunikacija SSO servisa s davateljem usluge. Ovaj certifikat vrijedi do 08. 07. 2022.
Datum isteka	08. 07. 2022.

Ako dođe do potrebe za privremeni povratak na stari certifikat, možete ga vratiti preko istog sučelja. Uzmite u obzir da treba pričekati 5-10 minuta da bi SSO servis počeo koristiti novoodabrani certifikat za komunikaciju s uslugom Office365.

U slučaju bilo kakvih problema, dodatnih pitanja ili nejasnoća kontaktirajte nas na adresu aai@srce.hr