ADFS

Niklas Leide - 2021-11-04 - Innlogging (IdP)

För att konfigurera ADFS som inloggning till Skolon behöver du som kund ladda upp Skolons metadata, och sedan skicka metadata tillbaka till Skolon. Det är också viktigt att det *claim* ni sätter upp i SAML svaret skapas utan **NameID**.

Skolons parametrar och metadata:
Sign on URL: https://ext-idp.skolon.com/a/
App identifier URL:
https://ext-idp.skolon.com/simplesaml/module.php/saml/sp/metadata.php/skolon
Reply URL:
https://ext-idp.skolon.com/simplesaml/module.php/saml/sp/metadata.php/skolon
Skolon metadata:
https://ext-idp.skolon.com/simplesaml/module.php/saml/sp/metadata.php/skolon

E-post ska ligga som ett extra attribut/claim i SAML-svaret. Förslagsvis döps det till "mail", oavsett namn på attributet.

Tänk på att attributet/claim **måste** skickas i transient-format.
Exempel på claim attribut efter att det är satt i transient-format:
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/emailaddress

Länkar till guider
Exakt hur konfigureringen görs varierar från AD version till AD version men nedan finns länkar till dokumentation från Microsoft som oftast används och exempel på hur man konfiguerar om ett claim till Transient nameID.

Guide för att sätta upp en Relying Party i ADFS:

https://docs.microsoft.com/en-us/windows-server/identity/ad-fs/operations/create-a-relying-party-trust

Sätt upp regler att skickas om LDAP attribut som claims:

https://docs.microsoft.com/en-us/windows-server/identity/ad-fs/operations/create-a-rule-to-send-ldap-attributes-as-claims

Guide för att sätta upp regler för transform claims:

https://docs.microsoft.com/en-us/windows-server/identity/ad-fs/operations/create-a-rule-to-transform-an-incoming-claim

Regler för att göra ett claim till Transient:

NameID-opaque

c1:[Type ==
"http://schemas.microsoft.com/ws/2008/06/identity/claims/windowsaccountname"]

&& c2:[Type ==
"http://schemas.microsoft.com/ws/2008/06/identity/claims/authenticationinstant"]

=> add(store = "_OpaqueIdStore", types = ("http://adfs.adfs.net/internal/sessionid"), query = "{0};{1};{2};{3};{4}", param = "useEntropy", param = c1.Value, param = c1.OriginalIssuer, param = "", param = c2.Value);

Create transient name identifier

c:[Type == "http://adfs.adfs.net/internal/sessionid"]

=> issue(Type = "http://schemas.xmlsoap.org/ws/2005/05/identity/claims/nameidentifier", Issuer = c.Issuer, OriginalIssuer = c.OriginalIssuer, Value = c.Value, ValueType = c.ValueType,
Properties["http://schemas.xmlsoap.org/ws/2005/05/identity/claimproperties/format"] = "urn:oasis:names:tc:SAML:2.0:nameid-format:transient")