MDQ MDQ MDQ!

SWAMID
SWAMID Wiki
SAML IdP Best Current Practice

Konfigurera metadatahämtning i Shibboleth Identity Provider för SAML

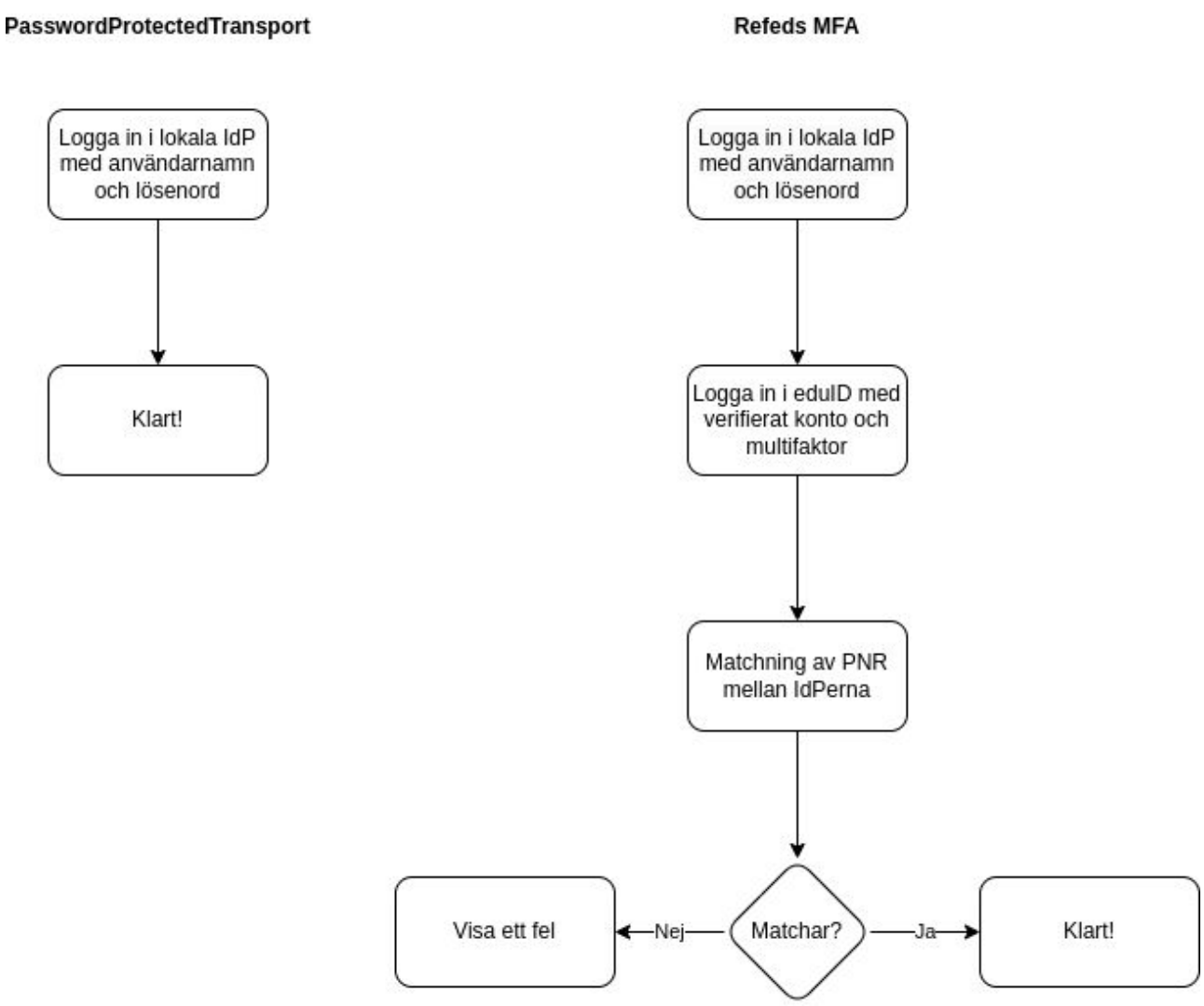
```
<MetadataProvider id="DynamicEntityMetadata"
xsi:type="DynamicHTTPMetadataProvider"
          connectionRequestTimeout="PT2S"
          connectionTimeout="PT2S"
          socketTimeout="PT4S">
      <MetadataFilter xsi:type="SignatureValidation" requireSignedRoot="true"
            certificateFile="%{idp.home}/credentials/md-signer2.crt" />
      <MetadataFilter xsi:type="RequiredValidUntil" maxValidityInterval="P14D"/>
      <MetadataQueryProtocol>https://mds.swamid.se/</MetadataQueryProtocol>
</MetadataProvider>
```

Shibboleth proxied MFA

Sunet Hackathon 23-24 april 2023


BRASKLAPP
imgflip.com

Flödet


PasswordProtectedTransport
Logga in i lokala IdP med användarnamn och lösenord
Klart!
Refeds MFA
Logga in i lokala IdP med användarnamn och lösenord
Logga in i eduID med verifierat konto och multifaktor
Matchning av PNR mellan IdPerna
Matchar?
Nej
Visa ett fel
Ja
Klart!

MFA flödet

- Ersätter Password flödet som huvudflöde
- Bygger på två sub-flöden
  - Password
  - SAML
- SAML flödet konfigureras för att
  - stödja Refeds MFA principal
  - peka vilken IdP man ska proxa vidare till (t.ex eduID)

Lokala IdP som en SP

Den lokala IdP måste också agera som en SP

Behöver en SPSSODescriptor med signing- och encryption-certifikat

Dessa certifikat är samma som för IDPSSODescriptor

De två Descriptors ligger i samma metadata-fil

Authentication konfiguration

conf/authn/authn.properties

- Aktivera MFA flöde
- Aktivera Password och SAML som subflöden

conf/authn/mfa-authn-config.xml

- Definiera TransitionMap

Attribute Resolver och Filter

conf/attribute-filter.xml

- IdP måste importera attribut från upstream IdP
- I vår exempel kommer vi att använda norEduPersonNIN

conf/attribute-resolver.xml

- Exponerar norEduPersonNIN från subject till en attribute som kan användas i den lokala IdPn

Subject canonicalization

conf/c14n/subject-c14n.properties
conf/c14n/subject-c14n.xml
conf/ldap.properties

- Sy ihop allting efter inloggning i den upstream IdPn.
- Extrahera norEduPersonNIN från upstream IdP assertion för att använda för attribute resolution i den lokala IdPn.
- Custom javascript för att kontrollera att norEduPersonNIN från lokala IdPn matchar norEduPersonNIN från upstream IdP.
- Resolver search filter ändras till att söka på flera olika principals.
- LDAP måste returnera norEduPersonNIN under autentisering.

Förberedelse inför egen labb

- Vi kommer att arbeta i metadata.**lab**.swamid.se för att inte störa er helpdesk.
  - Logga in och hämta hem er Metadata för IdP:n ni vill labba med.
  - Kopiera IDPSSOSecriptor och lägg in som SPSSODescriptor
  - Ladda upp till Metadata.lab.swamid.se och meddela mig (Björn) vilket ID ni fick :-)
- Kontakta mig (Björn) under nästa paus för att få ut ett testkonto till eduid.dev som vi kommer att användare senare idag.
  - Finns ett fejkat personnummer till varje testkonto som ni behöver lägga in i er lokala LDAP / AD / SQL för att kunna matcha om ni vill göra det via **norEduPersonNIN**
  - Logga in på **https://dev.eduid.se/** och lägg till MFA
  - Notera även vilket personnummer som tillhör “ditt” konto om du vill matcha på norEduPersonNIN.
- All konfiguration finns tillgänglig här: https://tinyurl.com/swamid-hackaton

Lägg till en SPSSODescriptor i er metadata

https://shibboleth.atlassian.net/wiki/spaces/KB/pages/1459979597/Using+SAML+Proxying+to+another+IdP#UsingSAMLProxyingtoanotherIdP-UpdateyourIdP'smetadata

```
--- idp-metadata.xml    2023-05-17 13:16:45
+++ idp-metadata-with-sp.xml    2023-05-17 13:27:17
@@ -12,6 +12,91 @@
       <mdrpi:RegistrationPolicy xml:lang="en">http://swamid.se/policy/mdrps</mdrpi:RegistrationPolicy>
     </mdrpi:RegistrationInfo>
   </md:Extensions>
+  <md:SPSSODescriptor protocolSupportEnumeration="urn:oasis:names:tc:SAML:2.0:protocol">
+    <md:Extensions>
+      <mdui:UIInfo>
[..]
+      </mdui:UIInfo>
+    </md:Extensions>
+    <md:KeyDescriptor use="signing">
[...]
+    </md:KeyDescriptor>
+     <md:KeyDescriptor use="encryption">
[...]
+    </md:KeyDescriptor>
+  <md:AssertionConsumerService Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST"
Location="https://shibmfa.test.swamid.se/idp/profile/Authn/SAML2/POST/SSO" index="0"/>
+  </md:SPSSODescriptor>
```

Ladda upp metadatan

- Lägg på entitetskategori CoCo v1/v2
- Begär norEduPersonNIN

/opt/shibboleth-idp/conf/attribute-resolver.xml

```
<AttributeDefinition xsi:type="SubjectDerivedAttribute"
    forCanonicalization="true"
    principalAttributeName="norEduPersonNIN"
    id="proxied-nin"
/>
```

/opt/shibboleth-idp/conf/attribute-filter.xml

```
   <AttributeFilterPolicy id="saml-proxy-pass-through">
    <PolicyRequirementRule xsi:type="Issuer"
value="https://idp.dev.eduid.se/idp.xml" />
    <AttributeRule attributeID="norEduPersonNIN" permitAny="true" />
   </AttributeFilterPolicy>
```

/opt/shibboleth-idp/conf/authn/authn.properties

```
: 11:44 root@shibmfa: /opt/shibboleth-idp # diff -u dist/conf/authn/authn.properties conf/authn/authn.properties
--- dist/conf/authn/authn.properties   2023-03-30 13:29:46.000000000 +0000
+++ conf/authn/authn.properties        2023-05-17 11:37:54.319811928 +0000
@@ -2,7 +2,7 @@
 # specific methods.

 # Regular expression matching login flows to enable, e.g. IPAddress|Password
-#idp.authn.flows = Password
+idp.authn.flows = MFA

 # Default settings for most authentication methods.
 #idp.authn.defaultLifetime = PT1H
@@ -206,16 +206,17 @@
 #   Define shibboleth.authn.SAML.discoveryFunction bean
 #   Set proxyEntityID property
 #   Fall through to discovery via discoveryRequired property
-#idp.authn.SAML.proxyEntityID = https://idp.example.org/idp/shibboleth
+idp.authn.SAML.proxyEntityID = https://idp.dev.eduid.se/idp.xml
 #idp.authn.SAML.discoveryRequired = true
 # Generally left false with bidirectional mappings in
 # conf/authn/authn-comparison.xml across the proxy boundary.
 # Adjust as needed to reflect IdP's capabilities/support.
 #idp.authn.SAML.addDefaultPrincipals = false
-#idp.authn.SAML.supportedPrincipals = \
-#    saml2/urn:oasis:names:tc:SAML:2.0:ac:classes:PasswordProtectedTransport, \
-#    saml2/urn:oasis:names:tc:SAML:2.0:ac:classes:Password, \
-#    saml1/urn:oasis:names:tc:SAML:1.0:am:password
+idp.authn.SAML.supportedPrincipals = \
+    saml2/https://refeds.org/profile/mfa, \
+    saml1/https://refeds.org/profile/mfa

 #### MFA ####

@@ -228,8 +229,11 @@
 # rules. The example corresponds to the example in mfa-authn-config.xml that
 # combines IPAddress with Password.
 idp.authn.MFA.supportedPrincipals = \
     saml2/urn:oasis:names:tc:SAML:2.0:ac:classes:InternetProtocol, \
     saml2/urn:oasis:names:tc:SAML:2.0:ac:classes:PasswordProtectedTransport, \
     saml2/urn:oasis:names:tc:SAML:2.0:ac:classes:Password, \
-    saml1/urn:oasis:names:tc:SAML:1.0:am:password
+    saml1/urn:oasis:names:tc:SAML:1.0:am:password, \
+    saml2/https://refeds.org/profile/mfa, \
+    saml1/https://refeds.org/profile/mfa
 # Most actual setup via mfa-authn-config.xml
```

/opt/shibboleth-idp/conf/c14n/subject-c14n.xml

```
--- dist/conf/c14n/subject-c14n.xml   2023-03-30 13:29:46.000000000 +0000
+++ conf/c14n/subject-c14n.xml        2023-05-16 11:53:04.522101535 +0000
@@ -36,7 +36,7 @@
        from an attribute value. To enable universally, just uncomment, but if you want it to run under more
        specific conditions, set an activationCondition property to a condition to apply.
        -->
-       <!-- <bean id="c14n/attribute" parent="shibboleth.PostLoginSubjectCanonicalizationFlow" /> -->
+       <bean id="c14n/attribute" parent="shibboleth.PostLoginSubjectCanonicalizationFlow" />

        <!--
        This is an advanced option for use with SAML 2 proxy authentication to a second IdP that
@@ -147,5 +147,48 @@
        <bean parent="shibboleth.Pair" p:first="^(.+)@example\.org$" p:second="$1" />
        -->
    </util:list>
-
+
+    <util:map id="umich.shibboleth.authn.MFA.customMap">
+        <entry key="AttributeResolver" value-ref="shibboleth.AttributeResolverService" />
+        <entry key="request" value-ref="shibboleth.HttpServletRequest" />
+    </util:map>
+
+                    <bean id="shibboleth.c14n.attribute.PrincipalNameLookupStrategy"
+                                                        parent="shibboleth.ContextFunctions.Scripted"
+          factory-method="inlineScript" p:customObject-ref="umich.shibboleth.authn.MFA.customMap">
+        <constructor-arg>
+          <value>
+          <![CDATA[
+          logger = Java.type("org.slf4j.LoggerFactory").getLogger("net.shibboleth.idp.attribute.resolver.eppnbuilder");
+
+          var principalName = null;
+          var subject = profileContext.getSubcontext("net.shibboleth.idp.authn.context.SubjectCanonicalizationContext").getSubject();
+          var princs = subject.getPrincipals(Java.type("net.shibboleth.idp.authn.principal.UsernamePrincipal").class);
+          var princs2 = subject.getPrincipals(Java.type("net.shibboleth.idp.authn.principal.IdPAttributePrincipal").class);
+
+
+          if (princs.size() == 1) {
+              principalName = princs.iterator().next().getName();
+
+              if (princs2.size() == 1) {
+                  resCtx = input.getSubcontext("net.shibboleth.idp.attribute.resolver.context.AttributeResolutionContext", true);
+
+                  resCtx.setPrincipal(principalName);
+                  resCtx.getRequestedIdPAttributeNames().add("norEduPersonNIN");
+                  resCtx.resolveAttributes(custom["AttributeResolver"]);
+
+                  orig_nin = resCtx.getResolvedIdPAttributes().get("norEduPersonNIN").getValues().get(0).getValue();
+                  eduid_nin = resCtx.getResolvedIdPAttributes().get("proxied-nin").getValues().get(0).getValue();
+                  logger.info("SWAMID-origin-nin: " + orig_nin);
+                  logger.info("SWAMID-eduid-nin: " + eduid_nin);
+                  if (orig_nin != eduid_nin) {
+                      throw new Error("'Identification attribute recived from eduID didn't match the local catalog'");
+                  }
+              }
+          }
+          principalName;
+          ]]>
+          </value>
+        </constructor-arg>
+    </bean>
```

/opt/shibboleth-idp/conf/c14n/subject-c14.properties

```
 #idp.c14n.attribute.uppercase = false
 #idp.c14n.attribute.trim = true
 # Lists of attributes to resolve...
+idp.c14n.attribute.attributesToResolve = proxied-nin
-#idp.c14n.attribute.attributesToResolve =
 #  and then select a principal name from
+idp.c14n.attribute.attributeSourceIds = proxied-nin
-#idp.c14n.attribute.attributeSourceIds =
 # Allows direct use of attributes via SAML proxy authn, bypasses resolver
 #idp.c14n.attribute.resolveFromSubject = false
 #idp.c14n.attribute.resolutionCondition = shibboleth.Conditions.TRUE
```

/opt/shibboleth-idp/bin/module.sh -e idp.authn.MFA

```
--- /tmp/mfa-authn-config.xml.idpnew    2023-05-17 11:50:11.406497913 +0000
+++ /tmp/mfa-authn-config.xml      2023-05-17 11:51:26.749225639 +0000
@@ -60,7 +60,7 @@
         <constructor-arg>
             <value>
             <![CDATA[
+                 nextFlow = "authn/Password";
-                nextFlow = "authn/SAML";

                 // Check if second factor is necessary for request to be satisfied.
                 authCtx =
input.getSubcontext("net.shibboleth.idp.authn.context.AuthenticationContext");
```

/opt/shibboleth-idp/conf/ldap.properties

```
--- dist/conf/ldap.properties        2023-05-11 12:09:52.116733811 +0000
+++ conf/ldap.properties    2023-05-11 06:38:12.085000000 +0000
@@ -52,7 +52,7 @@
 idp.attribute.resolver.LDAP.bindDN              = %{idp.authn.LDAP.bindDN:undefined}
 idp.attribute.resolver.LDAP.useStartTLS         = %{idp.authn.LDAP.useStartTLS:true}
 idp.attribute.resolver.LDAP.trustCertificates   = %{idp.authn.LDAP.trustCertificates:undefined}
-idp.attribute.resolver.LDAP.searchFilter        =
(|(uid=$resolutionContext.principal)(norEduPersonNIN=$resolutionContext.principal))
+idp.attribute.resolver.LDAP.searchFilter        = (uid=$resolutionContext.principal)

 # LDAP pool configuration, used for both authn and DN resolution
 #idp.pool.LDAP.minSize
```


THE END
memegenerator.es