ShibIdPX509LdapAuthentication

Shibboleth 2.x IdP X.509/LDAP autentikációs modul

Ezen az oldalon az NIIF által fejlesztett X.509 klienstanúsítvány alapú Shibboleth autentikációs modul leírása szerepel.

In English

Motivations

- The use of hardware tokens as authentication source. However, X.509 certificate authentication is not generally considered secure by nature, hardware tokens are designed to be safer than passwords. Local policy can decide whether they accept software tokens or not.
- Give the choice to our SPs. Some SPs can decide if they wanted to force the X.509 authentication (or force password authentication).

PKIful versus PKIless

- If one has built their full-fledged PKI infrastructure, one could use it for client certificate authentication.
- But it is hard to do PKI right, CRLs and/or OCSP are crucial in PKI.
- If only authentication is needed, storing the (self-signed) certificate is enough.

Shibboleth X.509 authentication

- With PKI, you would use simple RemoteUser authentication with container support.
- Without PKI, the container can not authenticate the user, it can only check if the user has the corresponding private key.
- You will also need some custom workflow to validate the presented client certificates. Eg. checking them against the directory attribute 'userCertificate'. This is step is a must to have control over certificate revocation.

X.509 + LDAP certificate authentication (implementation details)

- The web container does client certificate checking, but does not validate. Instead, it handles the certificate to the Shibboleth authentication module which will validate it.
- Shibboleth is configured with RemoteUser login handler pointing to our X.509 authentication servlet.
- The certificate must contain some identification data (eg the X.500 'UID' RDN). Our authentication servlet takes the presented certificate and compares it to the stored certificate(s) for the user. If a matching certificate is found in the directory, then the user is authenticated.
- The certificate authentication is implemented as a standard JAAS module, and can be reused elsewhere.

Combining X.509 and username/password authentication

- When SP does not specifically request authentication methods, the user should have the choice between supported authentication modes. Otherwise, the IdP must conform with the authentication context class the SP sent. The IdP must refuse to authenticate the user with authentication methods unacceptable to the SP. There is a support ticket named SIDP-258 about this flaw in Shibboleth IdP.
- We want to support two authentication methods: username/password (PasswordProtectedTransport) and X.509 authentication.
- Unfortunately this is not enough, we need a default authentication method which offers the choice of these two methods to our users. This can be done by placing a link to the X.509 authentication servlet in login.jsp. However when the SP requests PasswordProtectedTransport, this link must not be visible, so we decided to configure a new UserPassword login handler which maps to the unspecified authentication class and uses this tweaked login.jsp.
- We also want to send the actual authentication method to the SP (instead of saying 'unspecified'), so both login handlers must set their corresponding authentication class in the Shibboleth request. As the internal UsernamePassword login servlet does not do this, we subclassed it.
- Playing with Shibboleth login handlers and authentication contexts revealed that Shibboleth IdP can not properly support default authentication methods, and our hybrid handler with its 'unspecified' authentication method is invoked on every authentication request (because both actual methods it uses override this unspecified method in the request and IdP can not decide whether the unspecified class is requested by the SP or it is simply the default method configured in relying-party.xml). Fixing SIDP-265 with our proposed patch corrected this behavior.

Követelmények

Az X.509/LDAP autentikációs modul a következő követelmények alapján került kifejlesztésre:

- a felhasználók saját maguk által aláírt tanúsítványokat is használhassanak autentikációra
- ne kelljen PKI infrastruktúrát üzemeltetni a klienstanúsítványok használatához
- a tanúsítványok központilag menedzseltek, egyszerűen visszavonhatók legyenek

Ezen követelmények kielégíthetők a címtárban tárolt klienstanúsítványokkal, ugyanis a címtárba csak egy felettes szerv képes beírni a tanúsítványt, ott minden bejelentkezéskor ellenőrzésre is kerül, ezért könnyen visszavonható.

> **Info**
>
> A felhasználó tanúsítvány alapú azonosításához (identification) szükséges, hogy a tanúsítvány tartalmazza a felhasználónevet, mégpedig az `UID` (subject) mezőben.

Telepítés

Az autentikációs modul letölthető a http://software.niif.hu oldalról. A Shibboleth2 IdP autentikációs motorjának konfigurációját részetesen a Shibboleth2 User Authentication wikioldal írja le.

Apache beállítása

Amennyiben az alapértelmezett szervlet elérési utat választjuk (`/Authn/X509`), a következő opciókat kell megadni az Apache webszerver konfigurációjában:

```
<Location /idp/Authn/X509>
   SSLVerifyClient optional_no_ca  #nincs CA ellenorzes
   SSLOptions +ExportCertData      #tanusitvany exportalasa
</Location>
```

IdP webalkalmazás beállítása

A letöltött modulban található `shibboleth-x509auth-verzio.jar` java osztálykönyvtárat be kell másolni a Shibboleth webalkalmazás `WEB-INF/lib` könyvtárába, valamint a `WEB-INF/web.xml` fájlban meg kell adni az autentikációs szervlet paramétereit:

```
<servlet>
  <servlet-name>X509LdapAuthHandler</servlet-name>
  <servlet-class>hu.niif.middleware.shibboleth.auth.X509LdapLoginServlet</servlet-class>
  <init-param>
    <param-name>jaasConfigName</param-name>
    <param-value>X509LdapAuth</param-value>
  </init-param>
  <load-on-startup>4</load-on-startup>
</servlet>

<servlet-mapping>
  <servlet-name>X509LdapAuthHandler</servlet-name>
  <url-pattern>/Authn/X509</url-pattern>
</servlet-mapping>
```

Info

Az IdP webalkalmazás az `${SHIB_HOME}/war/idp.war` fájlban található, ebben kell elvégezni a módosításokat, majd újratelepíteni az alkalmazást a webkonténerbe.

IdP konfiguráció

Az IdP konfigurációjában két dolgot kell módosítani: a JAAS autentikációs modul `login.config` konfigurációját, valamint a `handler.xml`-ben az autentikációs módokat.

Az X.509/LDAP JAAS modul beállításához a `${SHIB_HOME}/conf/login.config` fájl tartalmához a következő sorokat adjuk hozzá (az LDAP elérési paramétereket értelem szerint kitöltve; az értékek általában a `ShibUserPassAuth` JAAS konfigurációból átmásolhatóak):

```
X509LdapAuth {
  hu.niif.middleware.jaas.X509LdapLoginModule required
     host=""
     port=""
     base=""
     ssl=""
     userField=""
     serviceUser=""
     serviceCredential="";
};
```

> **Info**
>
> Figyelni kell arra, hogy az itt megadott `serviceUser` olvasási joggal rendelkezzen a `userCertificate` LDAP attribútumra.

A JAAS modul beállítása után a `${SHIB_HOME}/conf/handler.xml` fájlban meg kell adnunk az új autentikációs modulunkat, a következőképpen:

```
<LoginHandler xsi:type="RemoteUser" protectedServletPath="/Authn/X509" >
   <AuthenticationMethod>urn:oasis:names:tc:SAML:2.0:ac:classes:X509</AuthenticationMethod>
</LoginHandler>
```

Ha továbbra is alapértelmezetten felhasználónév/jelszó autentikációt szeretnénk használni, akkor a Shibboleth IdP-ben be kell állítani az alapértelmezett hitelesítési módot, a `${SHIB_HOME}/conf/relying_party.xml` fájlban:

```
...
<DefaultRelyingParty provider="..."
  defaultSigningCredentialRef="..."

defaultAuthenticationMethod="urn:oasis:names:tc:SAML:2.0:ac:classes:PasswordProtectedTransport
">
...
```

Shibboleth SP beállítása

Az egyes SP-k eldönthetik hogy ők kérik-e az X.509 autentikációt, ezt az `authnContextClassRef` SP opcióval lehet jelezni a Shibboleth SP felé.

Ez a kérés azonban nem teljesen megbízható, ezért érdemes az IdP oldalon konfigurálni hogy egy adott SP kérése alapján az X.509 autentikációs módot használjuk (a `${SHIB_HOME}/conf/relying-party.xml` fájlban):

```
...
<RelyingParty id="x509-protected-sp-entityid"
  provider="our-idp-entityid"
  defaultAuthenticationMethod="urn:oasis:names:tc:SAML:2.0:ac:classes:X509" />
...
```

Integráció a felhasználónév / jelszó bejelentkezéssel

A fent leírt telepítési módszer nem biztosítja azt a lehetőséget, hogy egy felhasználó eldönthesse hogy ő jelszóval vagy klienstanúsítvánnyal autentikál. Amennyiben szeretnénk ezt a választási lehetőséget megadni abban az esetben, amikor az SP nem jelez általa preferált autentikációs módot, az alábbi plusz konfiguráció segítségével ezt megtehetjük.

> **Info**
>
> A klienstanúsítvány segítségével történő autentikáció **nem feltétlenül biztonságosabb** mint a jelszavas bejelentkezés, ezért jól fontoljuk meg, hogy minden felhasználónak felkínáljuk-e ezt a lehetőséget.

Shibboleth IdP webalkalmazás módosítása

Az X.509/LDAP autentikációs modul tartalmaz egy olyan szervletet, ami képes a felhasználónév/jelszó és az X.509 autentikáció együtt történő futtatására. Első lépésként ezt a szervletet kell beállítani a `WEB-INF/web.xml` webalkalmazás konfigurációban:

```
<servlet>
  <servlet-name>UsernamePasswordX509LoginServlet</servlet-name>
  <servlet-class>hu.niif.middleware.shibboleth.auth.UsernamePasswordX509LoginServlet</servlet-
class>
  <init-param>
    <param-name>loginPage</param-name>
    <param-value>login_.jsp</param-value>
  </init-param>
  <load-on-startup>4</load-on-startup>
</servlet>

<servlet-mapping>
  <servlet-name>UsernamePasswordX509LoginServlet</servlet-name>
  <url-pattern>/Authn/UserPasswordX509</url-pattern>
</servlet-mapping>
```

Ez a konfiguráció hivatkozik a `login_.jsp` fájlra, ez egy módosított Shibboleth bejelentkeztető form, amiben két plusz gomb kapott helyet. Ezekkel a gombokkal a felhasználó kérheti, hogy erre az egy autentikációra szeretne klienstanúsítványt használni, vagy a munkamenetben mindig. Utóbbi esetben a bejelentkezést lekezelő szervlet létrehoz egy cookie-t a felhasználó gépén, ami ezt a

preferenciát megőrzi a böngésző bezárásáig.

> **Info**
>
> Amennyiben a felhasználó egyszer bejelölte a tanúsítványos autentikációt a teljes munkamenetre, azt nem tudja kikapcsolni, csak a böngésző újraindításával.

Shibboleth IdP konfiguráció

Az IdP konfigurációjában meg kell adni ezt a hibrid autentikációs módot, mégpedig a következőképpen (`${SHIB_HOME}/conf/handler.xml`):

```
<LoginHandler xsi:type="UsernamePassword"
  authenticationDuration="240"
  jaasConfigurationLocation="file://PATH/TO/IDP/conf/login.config"
  authenticationServletURL="/Authn/UserPasswordX509">

<AuthenticationMethod>urn:oasis:names:tc:SAML:2.0:ac:classes:unspecified</AuthenticationMethod
>
</LoginHandler>
```

Ez a konfigurációs részlet azt közli az IdP-vel, hogy az autentikációs modul nem specifikált autentikációs mód esetén működik. Ezt a módot alapértelmezetté tehetjük a `${SHIB_HOME}/conf/relying_party.xml` fájlban:

```
...
<DefaultRelyingParty provider="..."
  defaultSigningCredentialRef="..."
  defaultAuthenticationMethod="urn:oasis:names:tc:SAML:2.0:ac:classes:unspecified">
...
```

Változat #1
cziernorbert hozta létre 2026-04-14 13:22:20 CEST
cziernorbert frissítette 2026-04-14 13:24:26 CEST