

添付バージョンのTOTPプラグインのソースの修正について

本課題に添付のバージョンは開発元の配布物(0.5.1.1.tar.gz)をShibboleth IdP V4で動かすため、および複数のデバイスを登録できないようにするため以下の修正を行っております。

```
diff -ru 0.5.1.1original/Shibboleth-IdP3-TOTP-Auth-0.5.1.1/pom.xml Shibboleth-IdP3-TOTP-Auth-0.5.1.1/pom.xml
--- 0.5.1.1original/Shibboleth-IdP3-TOTP-Auth-0.5.1.1/pom.xml      2015-12-23 18:21:08.000000000 +0900
+++ Shibboleth-IdP3-TOTP-Auth-0.5.1.1/pom.xml      2020-09-03 14:07:04.115087661 +0900
@@ -2,17 +2,12 @@
 <project xmlns="http://maven.apache.org/POM/4.0.0" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
   xsi:schemaLocation="http://maven.apache.org/POM/4.0.0 http://maven.apache.org/xsd/maven-4.0.0.xsd">
   <modelVersion>4.0.0</modelVersion>
-  <parent>
-    <groupId>net.shibboleth.idp</groupId>
-    <artifactId>idp-parent</artifactId>
-    <version>3.2.0</version>
-  </parent>
   <groupId>net.kvak.shibboleth</groupId>
   <artifactId>totpauth-parent</artifactId>
   <version>0.5.1</version>
   <packaging>pom</packaging>
-  <name>Shibboleth IdP v3 TOTP auth parent</name>
-  <description>TOTP based authentication module for Shibboleth IdP v3</description>
+  <name>Shibboleth IdP v4 TOTP auth parent</name>
+  <description>TOTP based authentication module for Shibboleth IdP v4</description>

   <modules>
     <module>totpauth-api</module>
@@ -21,18 +16,25 @@

   <properties>
     <project.build.sourceEncoding>UTF-8</project.build.sourceEncoding>
-    <maven.compiler.version>3.2</maven.compiler.version>
-    <maven.compiler.source>1.7</maven.compiler.source>
-    <maven.compiler.target>1.7</maven.compiler.target>
-    <shib.idp.version>3.2.0</shib.idp.version>
+    <maven.compiler.version>3.8.1</maven.compiler.version>
+    <maven.compiler.source>11</maven.compiler.source>
+    <maven.compiler.target>11</maven.compiler.target>
+    <shib.idp.version>4.0.0</shib.idp.version>
+    <gson.version>2.3.1</gson.version>
+    <mobile.auth.version>0.5.1</mobile.auth.version>
+    <com.warrenstrange.version>0.5.0</com.warrenstrange.version>
-    <org.springframework ldap.version>2.0.4.RELEASE</org.springframework ldap.version>
+    <org.springframework ldap.version>2.3.2.RELEASE</org.springframework ldap.version>
+<opensaml.groupId>org.opensaml</opensaml.groupId>
+<opensaml.version>3.4.3</opensaml.version>
   </properties>

   <repositories>
-  <repository>
+<repository>
+  <id>Central Maven repository</id>
+  <name>Central Maven repository https</name>
+  <url>https://repo.maven.apache.org/maven2</url>
+</repository>
+  <repository>
     <id>shib-release</id>
     <url>https://build.shibboleth.net/nexus/content/groups/public</url>
     <snapshots>
@@ -135,6 +137,13 @@

   <!-- Provided Dependencies -->
+<dependency>
+  <groupId>javax.servlet</groupId>
+  <artifactId>javax.servlet-api</artifactId>
+  <version>4.0.1</version>
+  <scope>system</scope>
+  <systemPath>/usr/share/tomcat/lib/servlet-api.jar</systemPath>

```

```

+</dependency>

    <!-- Runtime Dependencies -->

diff -ru 0.5.1.1original/Shibboleth-IdP3-TOTP-Auth-0.5.1.1/totpauth-api/pom.xml Shibboleth-IdP3-TOTP-Auth-0.5.1.1/totpauth-api/pom.xml
--- 0.5.1.1original/Shibboleth-IdP3-TOTP-Auth-0.5.1.1/totpauth-api/pom.xml    2015-12-23 18:21:08.000000000 +0900
+++ Shibboleth-IdP3-TOTP-Auth-0.5.1.1/totpauth-api/pom.xml    2020-09-03 08:41:15.644092773 +0900
@@ -19,5 +19,9 @@
     <artifactId>junit</artifactId>
     <scope>test</scope>
   </dependency>
+  <dependency>
+    <groupId>${opensaml.groupId}</groupId>
+    <artifactId>opensaml-profile-api</artifactId>
+  </dependency>
 </dependencies>
</project>
diff -ru 0.5.1.1original/Shibboleth-IdP3-TOTP-Auth-0.5.1.1/totpauth-impl/pom.xml Shibboleth-IdP3-TOTP-Auth-0.5.1.1/totpauth-impl/pom.xml
--- 0.5.1.1original/Shibboleth-IdP3-TOTP-Auth-0.5.1.1/totpauth-impl/pom.xml    2015-12-23 18:21:08.000000000 +0900
+++ Shibboleth-IdP3-TOTP-Auth-0.5.1.1/totpauth-impl/pom.xml    2020-09-03 10:39:01.067723893 +0900
@@ -165,6 +165,14 @@
     <type>test-jar</type>
   </dependency>

+<dependency>
+  <groupId>javax.servlet</groupId>
+  <artifactId>javax.servlet-api</artifactId>
+  <version>4.0.1</version>
+  <scope>system</scope>
+  <systemPath>/usr/share/tomcat/lib/servlet-api.jar</systemPath>
+</dependency>
+
   </dependencies>

   <build>
diff -ru 0.5.1.1original/Shibboleth-IdP3-TOTP-Auth-0.5.1.1/totpauth-impl/src/main/resources/conf/authn/totp-authn-beans.xml Shibboleth-IdP3-TOTP-Auth-0.5.1.1/totpauth-impl/src/main/resources/conf/authn/totp-authn-beans.xml
--- 0.5.1.1original/Shibboleth-IdP3-TOTP-Auth-0.5.1.1/totpauth-impl/src/main/resources/conf/authn/totp-authn-beans.xml    2015-12-23 18:21:08.000000000 +0900
+++ Shibboleth-IdP3-TOTP-Auth-0.5.1.1/totpauth-impl/src/main/resources/conf/authn/totp-authn-beans.xml    2020-09-03 11:25:11.816320352 +0900
@@ -37,10 +37,10 @@
   </bean>

   <bean id="contextSource" class="org.springframework.ldap.core.support.LdapContextSource">
-    <property name="url" value="LDAP_SERVER_URL" />
-    <property name="base" value="BASE_DN" />
-    <property name="userDn" value="MANAGERS_DN" />
-    <property name="password" value="PASSWORD" />
+    <property name="url" value="{idp.attribute.resolver.LDAP.LdapURL}" />
+    <property name="base" value="{idp.attribute.resolver.LDAP.baseDN}" />
+    <property name="userDn" value="{idp.attribute.resolver.LDAP.bindDN}" />
+    <property name="password" value="{idp.attribute.resolver.LDAP.bindDNCredential}" />
   </bean>

   <bean id="ldapTemplate" class="org.springframework.ldap.core.LdapTemplate">
diff -ru 0.5.1.1original/Shibboleth-IdP3-TOTP-Auth-0.5.1.1/totpauth-impl/src/main/resources/flows/authn/Totp/Totp-flow.xml Shibboleth-IdP3-TOTP-Auth-0.5.1.1/totpauth-impl/src/main/resources/flows/authn/Totp/Totp-flow.xml
--- 0.5.1.1original/Shibboleth-IdP3-TOTP-Auth-0.5.1.1/totpauth-impl/src/main/resources/flows/authn/Totp/Totp-flow.xml    2015-12-23 18:21:08.000000000 +0900
+++ Shibboleth-IdP3-TOTP-Auth-0.5.1.1/totpauth-impl/src/main/resources/flows/authn/Totp/Totp-flow.xml    2020-09-03 10:45:29.231389337 +0900
@@ -26,6 +26,8 @@
     result="viewScope.custom" />
   </on-render>

+  <transition on="RegisterToken" to="RegisterToken" />
+  <transition on="GenerateTokenSecrets" to="GenerateTokenSecrets" />
+  <transition on="proceed" to="ExtractTotpFromForm" />
</view-state>

```

```

diff -ru 0.5.1.1original/Shibboleth-IdP3-TOTP-Auth-0.5.1.1/totpauth-impl/src/main/resources/views/totp-register.vm Shibboleth-IdP3-
TOTP-Auth-0.5.1.1/totpauth-impl/src/main/resources/views/totp-register.vm
--- 0.5.1.1original/Shibboleth-IdP3-TOTP-Auth-0.5.1.1/totpauth-impl/src/main/resources/views/totp-register.vm    2015-12-23 18:21:
08.000000000 +0900
+++ Shibboleth-IdP3-TOTP-Auth-0.5.1.1/totpauth-impl/src/main/resources/views/totp-register.vm    2020-09-03 13:35:56.952302974 +0900
@@ -35,6 +35,7 @@
    <p class="error">${errorMessage}</p><br>
    #end
    <form action="${flowExecutionUrl}" method="post">
+    #parse("csrf/csrf.vm")

    <li> Download the Google Authenticator to your mobile phone </li>
    <li> Open the app and scan the QR-code or manually enter code: <strong>${sharedSecret}</strong></li>
diff -ru 0.5.1.1original/Shibboleth-IdP3-TOTP-Auth-0.5.1.1/totpauth-impl/src/main/resources/views/totp.vm Shibboleth-IdP3-TOTP-Auth-
0.5.1.1/totpauth-impl/src/main/resources/views/totp.vm
--- 0.5.1.1original/Shibboleth-IdP3-TOTP-Auth-0.5.1.1/totpauth-impl/src/main/resources/views/totp.vm    2020-09-03 14:12:29.725752266
+0900
+++ Shibboleth-IdP3-TOTP-Auth-0.5.1.1/totpauth-impl/src/main/resources/views/totp.vm    2020-09-03 13:34:09.613458942 +0900
@@ -1,6 +1,7 @@
#set ($rpContext = $profileRequestContext.getSubcontext('net.shibboleth.idp.profile.context.RelyingPartyContext'))
#set ($userName = $authenticationContext.getSubcontext('net.shibboleth.idp.authn.context.UsernamePasswordContext', true).
getUsername())
#set ($errorMessage = $authenticationContext.getSubcontext('net.kvak.shibboleth.totpauth.api.authn.context.TokenUserContext').
getErrorMessage())
+set ($s = $authenticationContext.getSubcontext('net.kvak.shibboleth.totpauth.api.authn.context.TokenUserContext', true).getState())
##
<!DOCTYPE html>
<html>
@@ -29,13 +30,17 @@
    <div class="content">
      <div class="column one">
        #parse("login-error.vm")
-
+      #if ( "$s" != "REGISTER" )
+      <div>To register on a very first time please enter any 6-digit number to display a registration button.</div>
+      <div>Also please make sure that your device has correct time set!</div>
+      #end

      <form action="${flowExecutionUrl}" method="post">
+      #parse("csrf/csrf.vm")

      <div class="form-element-wrapper">
        <label for="tokenNumber">Token code</label>
-        <input class="form-element form-field" id="j_tokenNumber" name="j_tokenNumber" type="text" autofocus>
+        <input class="form-element form-field" id="j_tokenNumber" name="j_tokenNumber" type="text">
      </div>

      <div class="form-element-wrapper">
@@ -43,7 +48,10 @@
        onClick="this.childNodes[0].nodeValue='<springMessageText("idp.login.pleasewait", "Logging in, please wait...")'"
        >#springMessageText("idp.login.login", "Login")</button>

-      <br><br><button type="submit" name="registerToken" formaction="${flowExecutionUrl&_eventId=RegisterToken}">Register a
new Token</button>
+      <br><br>
+      #if ( "$s" == "REGISTER" )
+      <button type="submit" name="registerToken" formaction="${flowExecutionUrl&_eventId=RegisterToken}">Register a new Token<
/button>
+      #end

    </div>
  </form>

```