NameID設定

NameIDはconf/attribute-filter.xmlに記述しなくてもconf/saml-nameid.propertiesとconf/saml-nameid.xmlの設定により、SPメタデータの<NameIDFormat>に従って下記の通り送信します。

SPメタデータの<NameIDFormat>の値	送信する属性
urn:oasis:names:tc:SAML:2.0:nameid-format:transient	transient-id
urn:oasis:names:tc:SAML:2.0:nameid-format:persistent	persistent-id
<NameIDFormat>がない	saml-nameid.propertiesのidp.nameid.saml2.defaultに従う。 デフォルトはurn:oasis:names:tc:SAML:2.0:nameid-format:transient

SPメタデータに複数の<NameIDFormat>がある場合は、SPメタデータの並び順で送信可能な属性を送信します。persistent-idの設定を行っていないなど送信可能な属性がない場合は、//saml2:Subject/saml2:NameID自体が送信されません。

<NameIDFormat>がないSPの場合と<NameIDFormat>がurn:oasis:names:tc:SAML:2.0:nameid-format:persistentの場合の//saml2:Subject/saml2:NameIDの例を下記に示します。

- <NameIDFormat>がないSPの場合

```
<saml2:Subject>
    <saml2:NameID
        Format="urn:oasis:names:tc:SAML:2.0:nameid-format:transient"
        NameQualifier="https://idp.example.ac.jp/idp/shibboleth"
        SPNameQualifier="https://sp1.example.jp/shibboleth-sp">AAdzZWNyZXQxgUnobM3/AN3fn8DfZPDqBp
/GnKNxc5JR4nxXAxDAXZZSg0AZSrDh1Sip1fl9JGYrm2NWjl8zHKxHmbsgS/mFZ1ZlSYQ2U
/Kz7tCQ+SDswixwLRcGg3tDvVSAY8imKSrElGWSm5gMM45D4rkeQONJYr7gQZ13</saml2:NameID>
```

- <NameIDFormat>がurn:oasis:names:tc:SAML:2.0:nameid-format:persistentの場合

```
<saml2:Subject>
    <saml2:NameID
        Format="urn:oasis:names:tc:SAML:2.0:nameid-format:persistent"
        NameQualifier="https://idp.example.ac.jp/idp/shibboleth"
        SPNameQualifier="https://sp2.example.jp/shibboleth-sp">oiUiApwGnBP8pS3HZJ02ZW/aOTI=</saml2:NameID>
```

transient-idの設定

transient-idのデフォルトはCryptoTransientIdに変更になりました。CryptoTransientIdの使用例を下記に示します。

```
<saml2:Subject>
    <saml2:NameID
        Format="urn:oasis:names:tc:SAML:2.0:nameid-format:transient"
        NameQualifier="https://idp.example.ac.jp/idp/shibboleth"
        SPNameQualifier="https://sp1.example.jp/shibboleth-sp">AAdzZWNyZXQxgUnobM3/AN3fn8DfZPDqBp
/GnKNxc5JR4nxXAxDAXZZSg0AZSrDh1Sip1fl9JGYrm2NWjl8zHKxHmbsgS/mFZ1ZlSYQ2U
/Kz7tCQ+SDswixwLRcGg3tDvVSAY8imKSrElGWSm5gMM45D4rkeQONJYr7gQZ13</saml2:NameID>
```

IdP 2系と同じ短いtransient-idを使いたい場合は下記の変更を行います。

- conf/saml-nameid.properties
  idp.transientId.generatorをアンコメントして、値をshibboleth.StoredTransientIdGeneratorに変更します。

conf/saml-nameid.properties

```
# Set to shibboleth.StoredTransientIdGenerator for server-side transient ID storage
idp.transientId.generator = shibboleth.StoredTransientIdGenerator
```

差分

```
 # Set to shibboleth.StoredTransientIdGenerator for server-side transient ID storage
-#idp.transientId.generator = shibboleth.CryptoTransientIdGenerator
+idp.transientId.generator = shibboleth.StoredTransientIdGenerator
```

StoredTransientIdの使用例を下記に示します。

```
<saml2:Subject>
    <saml2:NameID
        Format="urn:oasis:names:tc:SAML:2.0:nameid-format:transient"
        NameQualifier="https://idp.example.ac.jp/idp/shibboleth"
        SPNameQualifier="https://sp1.example.jp/shibboleth-sp">_f358fb015b9b45c7d18a4a2647e79c33</saml2:NameID>
```

関連: [Shibboleth Wiki] Disable use of internal encryption key

persistent-idの設定

computedId

computedIdでの設定を下記に示します。

- conf/saml-nameid.xml
  <ref bean="shibboleth.SAML2PersistentGenerator" /> をアンコメントして有効にします。

conf/saml-nameid.xml

```
        <!-- Uncommenting this bean requires configuration in saml-nameid.properties. -->
        <!-- -->
        <ref bean="shibboleth.SAML2PersistentGenerator" />
        <!-- -->
```

差分

```
         <!-- Uncommenting this bean requires configuration in saml-nameid.properties. -->
-        <!--
+        <!-- -->
         <ref bean="shibboleth.SAML2PersistentGenerator" />
-        -->
+        <!-- -->
```

一部のSPにだけpersistent-idを送信したい場合、当該箇所をアンコメントせずに、以下を挿入すると対象SPを指定することができます。

```
        <bean parent="shibboleth.SAML2PersistentGenerator">
            <property name="activationCondition">
                <bean parent="shibboleth.Conditions.RelyingPartyId" c:candidates="#{{'https://test-sp1.gakunin.nii.
ac.jp/shibboleth-sp', 'https://test-sp2.gakunin.nii.ac.jp/shibboleth-sp'}}" />
            </property>
        </bean>
```

- conf/saml-nameid.properties
idp.persistentId.generatorのデフォルトはComputedIdの設定のため、idp.persistentId.sourceAttributeとidp.persistentId.saltのみを設定します。idp.persistentId.saltには他人が推測できないランダムな値を指定してください。古いIdPから設定を引き継ぐ場合は同じ値を指定してください。

conf/saml-nameid.properties

```
# Persistent IDs can be computed on the fly with a hash, or managed in a database

# For computed IDs, set a source attribute and a secret salt:
idp.persistentId.sourceAttribute = uid
#idp.persistentId.useUnfilteredAttributes = true
# Do *NOT* share the salt with other people, it's like divulging your private key.
#idp.persistentId.algorithm = SHA
idp.persistentId.salt = XXXXXXXXXXXXXXXXXXXXXXXXXXX
```

差分

```
 # Persistent IDs can be computed on the fly with a hash, or managed in a database

 # For computed IDs, set a source attribute and a secret salt:
-#idp.persistentId.sourceAttribute = changethistosomethingreal
+idp.persistentId.sourceAttribute = uid
 #idp.persistentId.useUnfilteredAttributes = true
 # Do *NOT* share the salt with other people, it's like divulging your private key.
 #idp.persistentId.algorithm = SHA
-#idp.persistentId.salt = changethistosomethingrandom
+idp.persistentId.salt = XXXXXXXXXXXXXXXXXXXXXXXXXXX
```

- conf/attribute-resolver.xml
idp.persistentId.sourceAttributeで指定した属性がLDAPで定義されているのみでconf/attribute-resolver.xmlの対応するresolver:AttributeDefinitionがコメントアウトされている場合は、当該resolver:AttributeDefinitionをアンコメントします。（以下はsourceAttributeとしてuidを指定した場合の例）

conf/attribute-resolver.xml

```
    <!-- Schema: Core schema attributes-->
    <!-- -->
    <resolver:AttributeDefinition xsi:type="ad:Simple" id="uid" sourceAttributeID="uid">
        <resolver:Dependency ref="myLDAP" />
        <resolver:AttributeEncoder xsi:type="enc:SAML1String" name="urn:mace:dir:attribute-def:uid" encodeType="false" />
        <resolver:AttributeEncoder xsi:type="enc:SAML2String" name="urn:oid:0.9.2342.19200300.100.1.1" friendlyName="uid"
encodeType="false" />
    </resolver:AttributeDefinition>
    <!--
```

差分

```
     <!-- Schema: Core schema attributes-->
-    <!--
+    <!-- -->
     <resolver:AttributeDefinition xsi:type="ad:Simple" id="uid" sourceAttributeID="uid">
         <resolver:Dependency ref="myLDAP" />
         <resolver:AttributeEncoder xsi:type="enc:SAML1String" name="urn:mace:dir:attribute-def:uid" encodeType="false" />
         <resolver:AttributeEncoder xsi:type="enc:SAML2String" name="urn:oid:0.9.2342.19200300.100.1.1" friendlyName="uid"
encodeType="false" />
     </resolver:AttributeDefinition>
+    <!--
```


他の用途に使用しない場合はresolver:AttributeEncoderの2行はコメントアウトしてかまいません。

Shibboleth IdP 3.1の情報

computedIdでの設定を下記に示します。

- conf/saml-nameid.xml
  <ref bean="shibboleth.SAML2PersistentGenerator" /> をアンコメントして有効にします。

conf/saml-nameid.xml

```
<!-- Uncommenting this bean requires configuration in saml-nameid.properties. -->
<!-- -->
<ref bean="shibboleth.SAML2PersistentGenerator" />
<!-- -->
```

- conf/saml-nameid.properties
  idp.persistentId.generatorのデフォルトはComputedIdの設定のため、idp.persistentId.sourceAttributeとidp.persistentId.saltのみを設定します。

conf/saml-nameid.properties

```
# Set to shibboleth.StoredPersistentIdGenerator for db-backed storage
# and uncomment/name the PersistentIdStore bean to use
#idp.persistentId.generator = shibboleth.ComputedPersistentIdGenerator

# Otherwise for computed PersistentIDs set the source attribute and salt.
idp.persistentId.sourceAttribute = uid4persistentId
idp.persistentId.salt = changethistosomethingrandom
```

- conf/attribute-resolver.xmlとconf/attribute-filter.xml
  idp.persistentId.sourceAttributeで指定した属性がLDAPで定義されているのみでconf/attribute-resolver.xmlのresolver:AttributeDefinitionで定義されていない場合は、PersistentIdGeneratorから参照できませんので以下のように定義し、conf/attribute-filter.xmlで送信設定を行います。他の用途に使用しない場合resolver:AttributeEncoderの2行は不要です。

conf/attribute-resolver.xml

```
<!-- ========================================== -->
<!--      PersistentId Definition               -->
<!-- ========================================== -->

<!-- Attribute Definition for %{idp.persistentId.sourceAttribute} -->
<resolver:AttributeDefinition id="%{idp.persistentId.sourceAttribute}" xsi:type="ad:Simple"
    sourceAttributeID="uid">
    <resolver:Dependency ref="myLDAP" />
</resolver:AttributeDefinition>
```

conf/attribute-filter.xml

```
<!--  Release to anyone -->
<afp:AttributeFilterPolicy id="PolicyforAnyone">
    <afp:PolicyRequirementRule xsi:type="basic:ANY" />

    <afp:AttributeRule attributeID="%{idp.persistentId.sourceAttribute}">
        <afp:PermitValueRule xsi:type="basic:ANY" />
    </afp:AttributeRule>

</afp:AttributeFilterPolicy>
```

- conf/intercept/consent-intercept-config.xml
  ユーザ同意画面にて%{idp.persistentId.sourceAttribute}を表示しないように、util:list[@id="shibboleth.consent.attribute-release.BlacklistedAttributeIDs"]に%{idp.persistentId.sourceAttribute}を追加します。

conf/intercept/consent-intercept-config.xml

```
<util:list id="shibboleth.consent.attribute-release.BlacklistedAttributeIDs">
    <value>transientId</value>
    <value>persistentId</value>
    <value>eduPersonTargetedID</value>
    <value>%{idp.persistentId.sourceAttribute}</value>
</util:list>
```

storedId

storedIdでの設定を下記に示します。

MySQL上にデータベース shibboleth が存在することを前提としております。また、MySQL Connector/J (mysql-connector-java-5.1.xx-bin.jar)をインストールしておいてください。

- conf/saml-nameid.xml
  <ref bean="shibboleth.SAML2PersistentGenerator" /> をアンコメントして有効にします。

conf/saml-nameid.xml

```
        <!-- Uncommenting this bean requires configuration in saml-nameid.properties. -->
        <!-- -->
        <ref bean="shibboleth.SAML2PersistentGenerator" />
        <!-- -->
```

差分

```
         <!-- Uncommenting this bean requires configuration in saml-nameid.properties. -->
-        <!--
+        <!-- -->
         <ref bean="shibboleth.SAML2PersistentGenerator" />
-        -->
+        <!-- -->
```

一部のSPにだけpersistent-idを送信したい場合、当該箇所をアンコメントせずに、以下を挿入すると対象SPを指定することができます。

```
        <bean parent="shibboleth.SAML2PersistentGenerator">
            <property name="activationCondition">
                <bean parent="shibboleth.Conditions.RelyingPartyId" c:candidates="#{{'https://test-sp1.gakunin.nii.
ac.jp/shibboleth-sp', 'https://test-sp2.gakunin.nii.ac.jp/shibboleth-sp'}}" />
            </property>
        </bean>
```

- conf/saml-nameid.properties
  idp.persistentId.sourceAttribute, idp.persistentId.salt, idp.persistentId.generatorとidp.persistentId.storeを設定します。idp.persistentId.saltには他人が推測できないランダムな値を指定してください。古いIdPから設定を引き継ぐ場合は同じ値を指定してください。

conf/saml-nameid.properties

```
# Persistent IDs can be computed on the fly with a hash, or managed in a database

# For computed IDs, set a source attribute and a secret salt:
idp.persistentId.sourceAttribute = uid
#idp.persistentId.useUnfilteredAttributes = true
# Do *NOT* share the salt with other people, it's like divulging your private key.
#idp.persistentId.algorithm = SHA
idp.persistentId.salt = XXXXXXXXXXXXXXXXXXXXXXXXXX

# To use a database, use shibboleth.StoredPersistentIdGenerator
idp.persistentId.generator = shibboleth.StoredPersistentIdGenerator
# For basic use, set this to a JDBC DataSource bean name:
idp.persistentId.dataSource = MyDataSource
# For advanced use, set to a bean inherited from shibboleth.JDBCPersistentIdStore
#idp.persistentId.store = MyPersistentIdStore
# Set to an empty property to skip hash-based generation of first stored ID
#idp.persistentId.computed = shibboleth.ComputedPersistentIdGenerator
```

差分

```
 # Persistent IDs can be computed on the fly with a hash, or managed in a database

 # For computed IDs, set a source attribute and a secret salt:
-#idp.persistentId.sourceAttribute = changethistosomethingreal
+idp.persistentId.sourceAttribute = uid
 #idp.persistentId.useUnfilteredAttributes = true
 # Do *NOT* share the salt with other people, it's like divulging your private key.
 #idp.persistentId.algorithm = SHA
-#idp.persistentId.salt = changethistosomethingrandom
+idp.persistentId.salt = XXXXXXXXXXXXXXXXXXXXXXXXXX

 # To use a database, use shibboleth.StoredPersistentIdGenerator
-#idp.persistentId.generator = shibboleth.ComputedPersistentIdGenerator
+idp.persistentId.generator = shibboleth.StoredPersistentIdGenerator
 # For basic use, set this to a JDBC DataSource bean name:
-#idp.persistentId.dataSource = PersistentIdDataSource
+idp.persistentId.dataSource = MyDataSource
 # For advanced use, set to a bean inherited from shibboleth.JDBCPersistentIdStore
 #idp.persistentId.store = MyPersistentIdStore
 # Set to an empty property to skip hash-based generation of first stored ID
 #idp.persistentId.computed = shibboleth.ComputedPersistentIdGenerator
```

- conf/attribute-resolver.xml
  idp.persistentId.sourceAttributeで指定した属性がLDAPで定義されているのみでconf/attribute-resolver.xmlの対応するresolver:AttributeDefinitionがコメントアウトされている場合、当該resolver:AttributeDefinitionをアンコメントします。（以下はsourceAttributeとしてuidを指定した場合の例）

conf/attribute-resolver.xml

```
    <!-- Schema: Core schema attributes-->
    <!-- -->
    <resolver:AttributeDefinition xsi:type="ad:Simple" id="uid" sourceAttributeID="uid">
        <resolver:Dependency ref="myLDAP" />
        <resolver:AttributeEncoder xsi:type="enc:SAML1String" name="urn:mace:dir:attribute-def:uid" encodeType="false" />
        <resolver:AttributeEncoder xsi:type="enc:SAML2String" name="urn:oid:0.9.2342.19200300.100.1.1" friendlyName="uid"
encodeType="false" />
    </resolver:AttributeDefinition>
    <!--
```

差分

```
     <!-- Schema: Core schema attributes-->
-    <!--
+    <!-- -->
     <resolver:AttributeDefinition xsi:type="ad:Simple" id="uid" sourceAttributeID="uid">
         <resolver:Dependency ref="myLDAP" />
         <resolver:AttributeEncoder xsi:type="enc:SAML1String" name="urn:mace:dir:attribute-def:uid" encodeType="false" />
         <resolver:AttributeEncoder xsi:type="enc:SAML2String" name="urn:oid:0.9.2342.19200300.100.1.1" friendlyName="uid"
encodeType="false" />
     </resolver:AttributeDefinition>
+    <!--
```

他の用途に使用しない場合はresolver:AttributeEncoderの2行はコメントアウトしてかまいません。

- shibpidテーブルの作成
shibpidテーブルを作成します。

shibpid

```
CREATE TABLE shibpid (
    localEntity VARCHAR(255) NOT NULL,
    peerEntity VARCHAR(255) NOT NULL,
    persistentId VARCHAR(50) NOT NULL,
    principalName VARCHAR(50) NOT NULL,
    localId VARCHAR(50) NOT NULL,
    peerProvidedId VARCHAR(50) NULL,
    creationDate TIMESTAMP NOT NULL,
    deactivationDate TIMESTAMP NULL,
    PRIMARY KEY (localEntity, peerEntity, persistentId)
) ENGINE=InnoDB DEFAULT CHARSET=utf8;
```

- conf/global.xml
conf/global.xmlでbean MyDataSourceを定義します。ユーザ同意の情報をMySQLに保存する設定もしくはuApproveJP等で設定済みの場合、重複となるためこの定義は不要です。

conf/global.xml

```
    <!-- Use this file to define any custom beans needed globally. -->

    <!-- A DataSource bean suitable for use in the idp.persistentId.dataSource property. -->
    <bean id="MyDataSource"
        class="org.apache.commons.dbcp2.BasicDataSource"
        p:driverClassName="com.mysql.jdbc.Driver"
        p:url="jdbc:mysql://localhost:3306/shibboleth"
        p:username="username"
        p:password="password"
        p:maxTotal="10"
        p:maxIdle="5"
        p:maxWaitMillis="15000"
        p:testOnBorrow="true"
        p:validationQuery="select 1"
        p:validationQueryTimeout="5" />
```

差分

```
     <!-- Use this file to define any custom beans needed globally. -->

+    <!-- A DataSource bean suitable for use in the idp.persistentId.dataSource property. -->
+    <bean id="MyDataSource"
+        class="org.apache.commons.dbcp2.BasicDataSource"
+        p:driverClassName="com.mysql.jdbc.Driver"
+        p:url="jdbc:mysql://localhost:3306/shibboleth"
+        p:username="username"
+        p:password="password"
+        p:maxTotal="10"
+        p:maxIdle="5"
+        p:maxWaitMillis="15000"
+        p:testOnBorrow="true"
+        p:validationQuery="select 1"
+        p:validationQueryTimeout="5" />
```

Shibboleth IdP 3.1の情報

- conf/saml-nameid.xml
  <ref bean="shibboleth.SAML2PersistentGenerator" />をアンコメントして有効にします。

conf/aml-nameid.xml

```
<!-- Uncommenting this bean requires configuration in saml-nameid.properties. -->
<!-- -->
<ref bean="shibboleth.SAML2PersistentGenerator" />
<!-- -->
```

- conf/saml-nameid.properties
  idp.persistentId.generator, idp.persistentId.store, idp.persistentId.sourceAttributeとidp.persistentId.saltを設定します。

conf/saml-nameid.properties

```
# Set to shibboleth.StoredPersistentIdGenerator for db-backed storage
# and uncomment/name the PersistentIdStore bean to use
idp.persistentId.generator = shibboleth.StoredPersistentIdGenerator
idp.persistentId.store = PersistentIdStore
# Set this to null to skip hash-based generation of first stored ID
#idp.persistentId.computed = shibboleth.ComputedPersistentIdGenerator

# Otherwise for computed PersistentIDs set the source attribute and salt.
idp.persistentId.sourceAttribute = uid4persistentId
idp.persistentId.salt = changethistosomethingrandom
```

- conf/global.xml
  idp.persistentId.storeの値をconf/global.xmlで定義します。

conf/global.xml (Tomcat 7の場合)

```
<!-- Use this file to define any custom beans needed globally. -->
<bean id="MyDataSource"
      class="org.apache.tomcat.dbcp.dbcp.BasicDataSource"
      p:driverClassName="com.mysql.jdbc.Driver"
      p:url="jdbc:mysql://localhost:3306/shibboleth"
      p:username="username"
      p:password="password"
      p:maxActive="10"
      p:maxIdle="5"
      p:maxWait="15000"
      p:testOnBorrow="true"
      p:validationQuery="select 1"
      p:validationQueryTimeout="5" />

<bean id="PersistentIdStore"
      class="net.shibboleth.idp.saml.nameid.impl.JDBCPersistentIdStore"
      p:dataSource-ref="MyDataSource" />
```

conf/global.xml (Tomcat 8の場合)

```
<!-- Use this file to define any custom beans needed globally. -->
<bean id="MyDataSource"
      class="org.apache.tomcat.dbcp.dbcp2.BasicDataSource"
      p:driverClassName="com.mysql.jdbc.Driver"
      p:url="jdbc:mysql://localhost:3306/shibboleth"
      p:username="username"
      p:password="password"
      p:maxIdle="5"
      p:maxTotal="10"
      p:maxWaitMillis="15000"
      p:testOnBorrow="true"
      p:validationQuery="select 1"
      p:validationQueryTimeout="5" />

<bean id="PersistentIdStore"
      class="net.shibboleth.idp.saml.nameid.impl.JDBCPersistentIdStore"
      p:dataSource-ref="MyDataSource" />
```

Tomcat 8付属のDBCP2から、p:maxActiveはp:maxTotalに、p:maxWaitはp:maxWaitMillisに変更になりました。

- conf/attribute-resolver.xmlとconf/attribute-filter.xml
  idp.persistentId.sourceAttributeで指定した属性がLDAPで定義されているのみでconf/attribute-resolver.xmlのresolver:AttributeDefinitionで定義されていない場合は、PersistentIdGeneratorから参照できませんので以下のように定義し、conf/attribute-filter.xmlで送信設定を行います。他の用途に使用しない場合resolver:AttributeEncoderの2行は不要です。

conf/attribute-resolver.xml

```
<!-- ========================================== -->
<!--      PersistentId Definition               -->
<!-- ========================================== -->

<!-- Attribute Definition for %{idp.persistentId.sourceAttribute} -->
<resolver:AttributeDefinition id="%{idp.persistentId.sourceAttribute}" xsi:type="ad:Simple"
    sourceAttributeID="uid">
    <resolver:Dependency ref="myLDAP" />
</resolver:AttributeDefinition>
```

conf/attribute-filter.xml

```
<!--  Release to anyone -->
<afp:AttributeFilterPolicy id="PolicyforAnyone">
    <afp:PolicyRequirementRule xsi:type="basic:ANY" />

    <afp:AttributeRule attributeID="%{idp.persistentId.sourceAttribute}">
        <afp:PermitValueRule xsi:type="basic:ANY" />
    </afp:AttributeRule>

</afp:AttributeFilterPolicy>
```

- conf/intercept/consent-intercept-config.xml
  ユーザ同意画面にて%{idp.persistentId.sourceAttribute}を表示しないように、util:list[@id="shibboleth.consent.attribute-release.BlacklistedAttributeIDs"]に%{idp.persistentId.sourceAttribute}を追加します。

conf/intercept/consent-intercept-config.xml

```
<util:list id="shibboleth.consent.attribute-release.BlacklistedAttributeIDs">
    <value>transientId</value>
    <value>persistentId</value>
    <value>eduPersonTargetedID</value>
    <value>%{idp.persistentId.sourceAttribute}</value>
</util:list>
```