Kaltura MediaSpace™
SAML Integration Guide

Version: 5.70 March 2018

Kaltura
open source video

Kaltura Business Headquarters

250 Park Avenue South, 10th floor New York, NY. 10003, USA

Tel.: +1 800 871 5224

Contents

Preface

This preface contains the following topics:

About this Guide

This guide describes how to configure the Security Assertion Markup Language (SAML) module in Kaltura MediaSpace™ (KMS) Version 4.x and 5.x.

NOTE: Please refer to the official and latest product release notes for last-minute updates. Technical support may be obtained directly from: Kaltura Customer Care.

Contact Us:

Please send your documentation-related comments and feedback or report mistakes to knowledge@kaltura.com.

We are committed to improving our documentation and your feedback is important to us.

Audience

This guide is intended for Kaltura partners, community members, and customers who want to understand and configure SAML authentication and authorization in MediaSpace.

To understand thisinformation, you need to be familiar with SAML, authentication and authorization terminology.

Document Conventions

Kaltura uses the following admonitions:

- Note
- Workflow

NOTE: Identifies important information that contains helpful suggestions.

Workflow: Provides workflow information.

1. Step 1
2. Step 2

Related Documentation

In addition to this guide, the following product documentation is available:

- Kaltura MediaSpace
- Kaltura MediaSpace Setup Guide
- Kaltura MediaSpace: Introduction to Authentication and Authorization Solutions

NOTE: Please remember to review all product release notes for known issues and limitations.

SECTION 1

Understanding SAML Implementation in Kaltura MediaSpace

SAML authentication in MediaSpace enables users to log into MediaSpace using their credentials from an organizational SAML based Identity Provider. A user does not require an additional set of credentials for MediaSpace.

When MediaSpace is configured to authenticate using SAML, other authentication methods are disabled.

NOTE: The MediaSpace SAML module supports SAML 2.0. Older Identity Providers that work with SAML 1.0 or SAML 1.1 are not supported by this module.

Understanding SAML Authorization in MediaSpace

A user's *application role* determines the MediaSpace actions that the user is authorized to do. When SAML is used for authorization in MediaSpace, the user's application role is based on membership in organizational groups and specific attribute in the SAML response. The organizational groups are managed in the organization's Identity Provider.

To learn more about the MediaSpace application role, refer to Understanding Application Roles in the Kaltura MediaSpace Setup Guide.

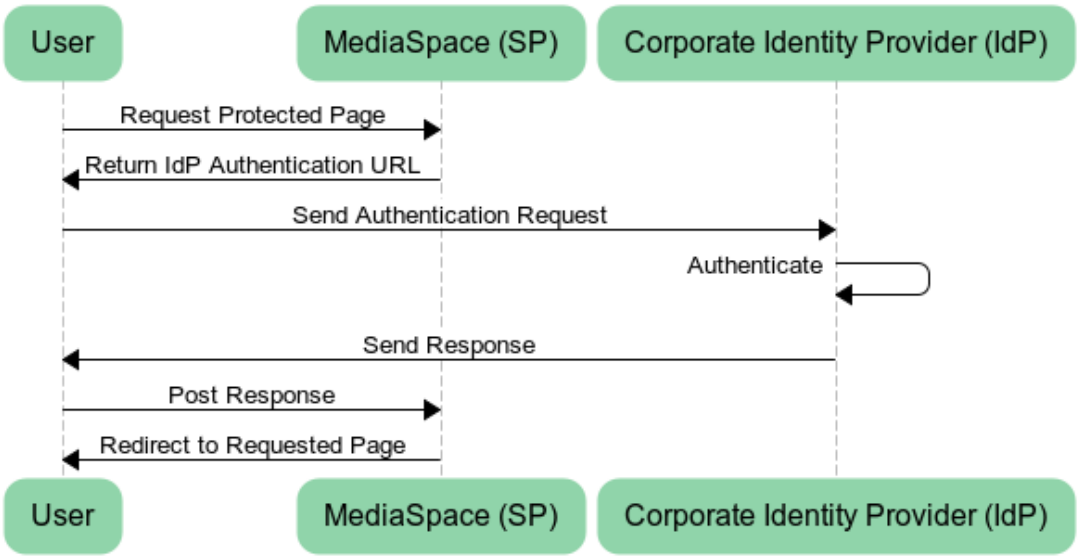
Understanding the SAML Authentication Flow

There are two types of SAML authentication:

- Service Provider Initiated Authentication
- Identity Provider (IdP) Initiated Authentication

Service Provider Initiated Authentication

In this workflow the user attempts to access a resource on MediaSpace that requires authentication. MediaSpace, the Service Provider ("SP") sends an authentication request to the Identity Provider ("IdP"). Both the request and the response are sent through the users' browser via HTTP Get.

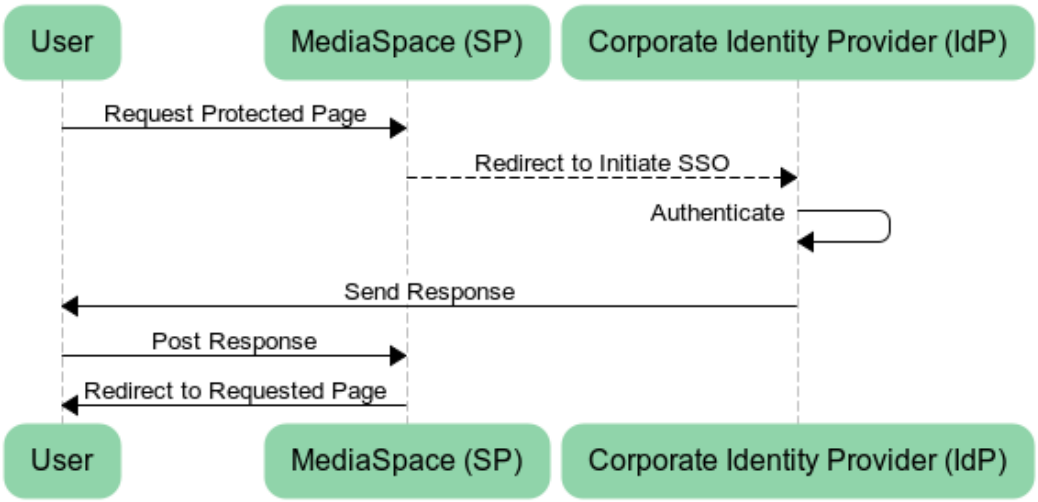


Processing Steps:

1. The user requests access to a MediaSpace page that requires authentication.
2. MediaSpace builds a request and the user's browser sends it to the IdP to handle the authentication.
3. On a successful authentication, The IDP returns an HTML form to the browser with a SAML response. The browser automatically posts the HTML form back to MediaSpace
4. MediaSpace redirects the user to the requested page.

Identity Provider (IdP) Initiated Authentication

In this workflow the entries process is handled by the Identity Provider. MediaSpace will redirect the user to an external URL that handles the authentication and redirects the user back to MediaSpace.



Processing Steps:

1. The user requests access to a MediaSpace page that requires authentication.
2. MediaSpace redirects the user to a URL on the IdP to handle authentication.
3. On a successful authentication, the IDP returns an HTML form to the browser with a SAML response. The browser automatically posts the HTML form back to MediaSpace
4. MediaSpace redirects the user to the requested page

Understanding the SAML Authorization Flow

Depending on your MediaSpace SAML configuration, MediaSpace queries attributes in the SAML response to determine the MediaSpace application role of the authenticated user. You can define a default role for authenticated users and map specific attributes and values to a MediaSpace role in the SAML module configuration.

SECTION 2

Configuring SAML in MediaSpace

This section describes the IdP Metadata Details and provides information on how to set up setup the SAML module for SP initiated and IdP initiated configurations.

Identity Provider (IdP) Metadata Details

The following information about the Identity Provider is required to be able to configure the MediaSpace SAML module:

MediaSpace domain	
SAML Authentication Mode Select one	[ ] IdP Initiated [ ] SP Initiated
If IdP Initiated is used: What is the query string key for the *RelayState* Parameter?	
IdP Metadata XML	
Login URL (optional, if not specified in the IdP metadata)	
Logout URL (optional, if not specified in the IdP metadata)	
Host Name of IdP (optional, if not specified in the IdP metadata)	
IdP Issuer Name (optional, if not specified in the IdP metadata)	
IdP Name (optional, if not specified in the IdP metadata)	
IdP Certificate (optional, if not specified in the IdP metadata)	
Is SAML response encryption required?	
Example of SAML XML Response (optional)	
SAML2 Attribute name where the *User ID* is taken from Note: A persistent and unique user ID for each authenticated user is required. This user ID is used when the user uploads media, comments on media etc. Without this, the user will not be identified properly in MediaSpace.	
SAML2 Attribute name where the *First Name* is taken from	

Note: If this information cannot be provided, the display name will be built form the User ID.	
SAML2 Attribute name where the *Last Name* is taken from Note: If this information cannot be provided, the display name will be built form the User ID	
SAML2 Attribute name where the *Email* is taken from Note: If this information cannot be provided you will not be able to use email notification functionality in MediaSpace.	
Default MediaSpace role for authenticated users Select one:	[ ] viewerRole – User can browse public galleries, is not authorized to upload new content, and does not have a My Media page. [ ] privateOnlyRole – User can upload content to My Media, cannot publish to galleries, and can add media to channels according to entitlements. [ ] adminRole - User can upload content and publish to all galleries. [ ] unmoderatedAdminRole – User can upload content and bypass moderation (when moderation is enabled for an account)
If you can map MediaSpace roles to groups / attributes in the IdP, provide for each group / role the following	SAML2 Attribute Name: SAML Attribute Value: MediaSpace Role:
Provide credentials that can be used to test the configuration. It is best to provide one credential per role. If credentials are not provided we will not be able to test the configuration and authentication.	

The following is an example of the metadata provided by the IdP with the information that should be used:

SAML 2.0 IdP Metadata

Here is the metadata that simpleSAMLphp has generated for you. You may send this metadata document to trusted partners to setup a trusted federation.

You can get the metadata xml on a dedicated URL:

https://openidp.feide.no/simplesaml/saml2/idp/metadata.php

Metadata

In SAML 2.0 Metadata XML format:

```
<?xml version="1.0"?>
<md:EntityDescriptor xmlns:md="urn:oasis:names:tc:SAML:2.0:metadata" xmlns:ds="http://www.w3.org/2000/09/xmldsig#" entityID="https://openidp.feide.no">
  <md:IDPSSODescriptor protocolSupportEnumeration="urn:oasis:names:tc:SAML:2.0:protocol">
    <md:KeyDescriptor use="signing">
      <ds:KeyInfo xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
        <ds:X509Data>
          <ds:X509Certificate>MIICizCCAfQCCQCY8tKaMc0BMjANBgkqhkiG9w0BAQUFADCBiTELMAkGA1UEBhMCTk8xEjAQBgNVBAgTCVRyb25kaGVpbTEQMA4GA1UEChMHVU5JTkVUVDEOMAwGA1UECx
        </ds:X509Data>
      </ds:KeyInfo>
    </md:KeyDescriptor>
    <md:KeyDescriptor use="encryption">
      <ds:KeyInfo xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
        <ds:X509Data>
          <ds:X509Certificate>MIICizCCAfQCCQCY8tKaMc0BMjANBgkqhkiG9w0BAQUFADCBiTELMAkGA1UEBhMCTk8xEjAQBgNVBAgTCVRyb25kaGVpbTEQMA4GA1UECx
        </ds:X509Data>
      </ds:KeyInfo>
    </md:KeyDescriptor>
    <md:SingleLogoutService Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-Redirect" Location="https://openidp.feide.no/simplesaml/saml2/idp/SingleLogoutSer
    <md:NameIDFormat>urn:oasis:names:tc:SAML:2.0:nameid-format:transient</md:NameIDFormat>
    <md:SingleSignOnService Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-Redirect" Location="https://openidp.feide.no/simplesaml/saml2/idp/SSOService.php"
  </md:IDPSSODescriptor>
  <md:ContactPerson contactType="technical">
    <md:GivenName>Feide</md:GivenName>
    <md:SurName>support</md:SurName>
    <md:EmailAddress>support@feide.no</md:EmailAddress>
  </md:ContactPerson>
</md:EntityDescriptor>
```

In simpleSAMLphp flat file format - use this if you are using a simpleSAMLphp entity on the other side:

```
$metadata['https://openidp.feide.no'] = array (
  'metadata-set' => 'saml20-idp-remote',
  'entityid' => 'https://openidp.feide.no',
  'SingleSignOnService' =>
  array (
    0 =>
    array (
      'Binding' => 'urn:oasis:names:tc:SAML:2.0:bindings:HTTP-Redirect',
      'Location' => 'https://openidp.feide.no/simplesaml/saml2/idp/SSOService.php',
    ),
  ),
  'SingleLogoutService' => 'https://openidp.feide.no/simplesaml/saml2/idp/SingleLogoutService.php',
  'certData' => 'MIICizCCAfQCCQCY8tKaMc0BMjANBgkqhkiG9w0BAQUFADCBiTELMAkGA1UEBhMCTk8xEjAQBgNVBAgTCVRyb25kaGVpbTEQMA4GA1UEChMHVU5JTkVUVDEOMAwGA1UECxMFRmVpZGUxGTA
  'NameIDFormat' => 'urn:oasis:names:tc:SAML:2.0:nameid-format:transient',
);
```

Certificates

Download the X509 certificates as PEM-encoded files.

- idp.crt

Configuring Multiple Identity Providers and Multiple Service Providers for SAML Authentication

Kaltura MediaSpace allows for admins to configure multiple IdPs and multiple SPs for SAML authentication. The ability to set multiple providers is based on the admins configuration settings in the Auth module and the admins configuration in the SAML module. Setting multiple IdPs and SPs may be used for site-specific SAML authentication.

When the enableMultiauth field in the Auth module is set to Yes, you can configure multiple SAML configurations for the following:

- SAML IdP initiated configurations
- SAML SP initiated configurations

When the enableMultiIdp field in the SAML module is set to Yes, you can configure multiple SAML authentication providers by adding the relevant parameters for each provider. A new frame is opened to configure and add multiple IdPs The default for the enableMultiIdp field is No.

NOTE: The enableMultiAuth field in the Auth module must to be enabled.

SAML Authentication Configuration Steps

Perform the following steps to setup the SAML module both for SP initiated and IdP initiated configurations. Parameters that are relevant or different between methods are noted as such.

Before you begin:

Make sure that sslSettings is enabled (set to “All site”) in the Auth tab (within the MediaSpace admin). SAML authentication will not work if MediaSpace is working over HTTP or if the sslSettings is set to “Login only” .

To setup the SAML module for SP initiated and IdP initiated configurations

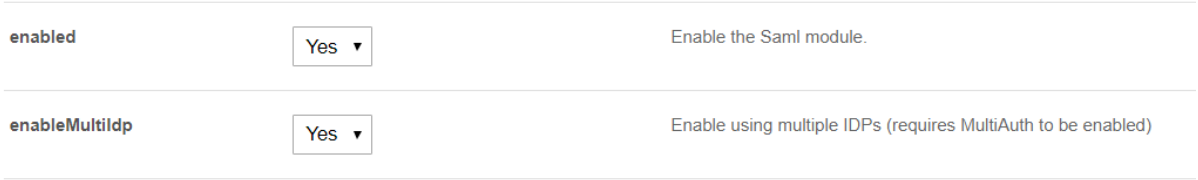
1. In the SAML module configuration, select **Yes** to enable the SAML module.
2. Enter values for the following:

Parameter	Description
enable	Set to Yes.
Metadata mode	
enableMultiIdp	The default is no and you will not be able to set multiple SAML providers. When enableMultiIdp is set to yes ,a new frame is opened to configure and add multiple SAML authentication providers. (The enableMultiAuth field in the Auth module must be enabled.).
loginRedirectUrl	The URL where the user will be redirected when authentication is required. For SP Initiated it would be a URL where the request is posted. For IdP initiated a URL with the entity ID as a parameter. • SP Initiated Example: https://idp.example.com/identity IdP Initiated Example: https://idp.example.com/identity/UnsolicitedSSO?entityID=mediaspaceentityID
logoutRedirectUrl	The URL where the user will be redirected when logging out from MediaSpace. NOTE: On logout, MediaSpace will always expire the MediaSpace session and then optionally redirect the user to this URL. MediaSpace does not expire login session from the identity provider.
relayStateUrlParam	The parameter name that the IdP uses to pass the URL to redirect the user back after a successful login. This defines the default place to redirect the user to in case it is not passed as part of request. For example for PingFederate it would be *TARGET*. For other SAML providers it is typically *RelayState*.

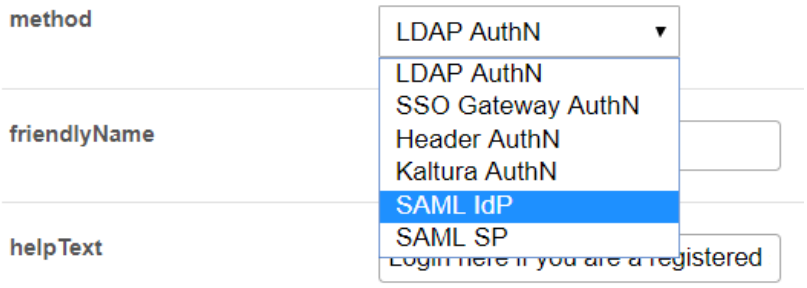
3. Continue with the Common Configuration steps.

To setup the SAML module for SP initiated and IdP initiated configurations using multiple providers (requires enableMultiAuth to be enabled)

1. In the SAML module configuration, select **Yes** to enable the SAML module.
2. Select Yes in the enableMultiIdp field to configure multiple authentication providers for SAML. The default is No.



3. For each IdP you are adding complete the following values in the *multiIdp* section:

uniqueName	Enter a unique name for this IdP, must be alphanumeric.
friendlyName	Enter the text to show in the authN/method selection dropdown in the Auth module. For example  IF the SAML friendlyName is empty, it is taken from the uniqueName.
adapterClass	Select the adapterClass for the authentication method: IdP or SP initiated
loginRedirectUrl	The URL where the user will be redirected when authentication is required. For SP Initiated it would be a URL where the request is posted. For IdP initiated a URL with the entity ID as a parameter. • SP Initiated Example: https://idp.example.com/identity • IdP Initiated Example: https://idp.example.com/identity/UnsolicitedSSO?entityID=mediaspaceentityID
logoutRedirectUrl	The URL where the user will be redirected when logging out from MediaSpace. NOTE: On logout, MediaSpace will always expire the MediaSpace session and then optionally redirect the user to this URL. MediaSpace does not expire login session from the identity provider.
relayStateUrlParam	The param name to append to the URL for relay state when in 'IdpFirst' mode, default is 'RelayState' This defines the default place to redirect the user to in case it is not passed as part of request. For example for PingFederate it would be *TARGET*. For other SAML providers it is typically *RelayState*.
shouldNestRelayState	Select whether to concatenate the relay state as query-string or as URL-encoded query string.
shouldPost	When set to Yes, the SAML request will be posted instead of using get. Default is No.
shouldDecodeRelayState	When set to Yes, the RelayState will be decoded before redirect
idpMetadata	IdP Configurations
host	IdP Host Name

issuer	The issuer name as it appears in the SAML response
name	Friendly name of IdP (English)
certFilePath	The full path on the MediaSpace server where the SAML certificate was placed. Include the file name as well.
certFileContent	This field may be used instead of 'certFilePath'. Leave 'certFilePath' empty in order to use certFileContent.
attributes	
userIdAttribute	(Optional) The SAML attribute containing the user id, when blank, NameID element will be used
firstNameAttribute	(Optional) The SAML attribute containing the first name.
lastNameAttribute	(Optional) The SAML attribute containing the last name.
emailAttribute	(Optional) The SAML attribute containing the email.
defaultRole	The default role for authenticated SAML user
allowDefaultRole	Select Yes or No.
role	The default role for authenticated SAML user

4. Continue with the Common Configuration steps.

Common Configuration

Parameter	Description
enableMetadataEndPoint	Customers that require a standard XML response that exposes the metadata configured on the Service Provider side, can use this configuration. This will expose the configured parameters of the SAML module through the following URL: http://[MediaSpace Server]/saml/index/sp-metadata
useInternalLogoutPage	If set to “Yes” logout will expire the MediaSpace session and display message to user but will not redirect to IdP logout page. For example: **You have signed out from MediaSpace.** **For improved security, we recommend that you close all browser windows at the end of your online session.**
allowKeepAlive	When true, the session will be extended upon user's interaction. The default is false.
logoutText	If useInternalLogoutPage is set to Yes you can define a custom message to users. You can use HTML tags to display a message.
shouldNestRelayState (already configured for multi-authentication)	whether to concatenate the relay state as query-string or as URL-encoded query string.
shouldPost (already configured for multi-authentication)	When true, the SAML request will be posted instead of using get. Default is false
shouldDecodeRelayState (already configured for multi-authentication)	When true, RelayState will be decoded before redirect

5. Complete the following values in the *spMetadata* section:

Parameter	Description
name	The entity ID of the service provider (MediaSpace) as it was configured in your Identity Provider. For example: https://partner_id.mediaspace.kaltura.com (this will be used as the SP entity ID).
host	The host of the MediaSpace instance. For example: partner_id.mediaspace.kaltura.com. NOTE: The host may be configured only with a single URL per KMS instance. If you are using your own alias for MediaSpace (for example: video.company.com) you should use that alias.
relayState	The value for the relative URL to redirect the user after login if a relay state is not passed as part of the authentication request. The default is "/".
nameIdFormat	This field is used for SP initiated mode only. Will not work if NameID is not released. • Transient - Recommended for Shibboleth setup • Persistent - Preferred setup. • None - set to remove the NameIDPolicy element from the SAML request.

certificate – (optional)	When encryption is required for the SAML response, enter the certificate information. Paste the content of the crt file without the comments line. See Generating a Certificate Workflow.
	NOTE: You should paste the content **without** the 2 comment lines *(----BEGIN...* and *-----END...*)
	All text should be in a single line with no spaces, so remove all the breaklines in the generated file
	The certificate value is used to encrypt the response provided by the IdP. The following example shows how the crt file would look including the comment lines and the extra line breaks that should be removed:
	`-----BEGIN CERTIFICATE-----`
	`MIICsDCCAhmgAwIBAgIJALM+uZK9gWbQMA0GCSqGSIb3DQEBBQUAMEUxCzAJBgNV`
	`BAYTAkFVMRMwEQYDVQQIEwpTb21lLVN0YXRlMSEwHwYDVQQKExhJbnRlcm5ldCBX`
	`aWRnaXRzIFB0eSBMdGQwHhcNMTMwNDI0MDgzOTU1WhcNMjMwNDI0MDgzOTU1WjBF`
	`MQswCQYDVQQGEwJBVTETMBEGA1UECBMKU29tZS1TdGF0ZTEhMB8GA1UEChMYSW50`
	`ZXJuZXQgV2lkZ2l0cyBQdHkgTHRkMIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKB`
	`gQC3Pkd3p+a9Yy0TFHuwy6trDlxhKwa0FAwrGlBnJCw4V+XgL5JaymRqICo1Vrk3`
	`MEXFD1hf5GuG17Sm1CXA02XAdzJMemr8RcLjq5dqAPP+6ZZ+3JM9owjvy1LRhMMP`
	`wCUBDeCI3WNvmNDCpnoJp+mBIgyZpr87ecgaCt2626CRKQIDAQABo4GnMIGkMB0G`
	`A1UdDgQWBBTODBaXbjmbJUJ1+gnD7CFKECmp9jB1BgNVHSMEbjBsgBTODBaXbjmb`
	`JUJ1+gnD7CFKECmp9qFJpEcwRTELMAkGA1UEBhMCQVUxEzARBgNVBAgTClNvbWUt`
	`U3RhdGUxITAfBgNVBAoTGEludGVybmV0IFdpZGdpdHMgUHR5IEx0ZIIJALM+uZK9`
	`gWbQMAwGA1UdEwQFMAMBAf8wDQYJKoZIhvcNAQEFBQADgYEAo6LDQVKjODxoL7N/`
	`CXTDMDnZ74gXLnZfOWh4RSQZzg/N5JpHt7RH4KTKpc/uWf0cUVRhUED4Vx3K/hlO`
	`rr8I7ylh6hpD2T8Ecmimx8oXieGrVU5ZuIsMaFxDJFeIvzq6+KtYz+ZaIx2wc6tJ`
	`RCe3NZLDKW3WvwgjKdY+YyOkaTs=`
	`-----END CERTIFICATE-----`

privateKey – (optional)	Copy paste the pem file as is. The privateKey value is used to decrypt the response provided by the IdP.
	`-----BEGIN RSA PRIVATE KEY-----`
	`MIICXQIBAAKBgQC3Pkd3p+a9Yy0TFHuwy6trDlxhKwa0FAwrGlBnJCw4V+XgL5Ja`

Parameter	Description
	ymRqICo1Vrk3MEXFD1hf5GuG17Sm1CXA02XAdzJMemr8RcLjq5dqAPP+6ZZ+3JM9 owjvy1LRhMMPwCUBDeCI3WNvmNDCpnoJp+mBIgyZpr87ecgaCt2626CRKQIDAQAB AoGAURW1+jTJ3bQtFexSb4EwcUcBid3IMZdNayVRvtI63xPGHNXwJUy58lwZUVD2 1Hz/4ptPt98T1a9NuSTXL+RbeXaOFI5nPXQvIV62IsOVrg1l1SkKedkWKM3EPesx iACqtC3xOaV+kjDS1R7x5MNXroMHM/tOKg9xfjmlmckisyECQQDwRh0NSTNGKHEA gNA6TqO3X4G9VkYWE1/KT9MQyc2k41LrKLXD9nd39kgHb7lkozq5r+KmVNo2nki3 mqijZ0aTAkEAwzyYQik8pRkFlBH/UDYLJ96wuGrqYjvQO+94WWzWCZPXBPBlOY5g KG+l5WMfIpvHwsbd0iPaZeCax0INW6LC0wJATRNAuIVVxFiuvymTIlEdpXImrTTi sKwwWza2DzmdFRqy+6qIfD8w3bOMMY5+WzEdYnlwbEjl4wVtcDBVjm1PrwJBALu/ VrAxFaeys0GcOQi6n+m8ZfdCoZjL6kjo1bQxTHczW4/dWYqK1v+rtj4sHvHaGrS9 Ju2BGvHjlxRM+amIkI8CQQCHQNwIyVzMvJxnlHGO0Sz04vKPs4xSVegYmOL3JPOt Rr7FMzBMRp46CSa6p38k4ZnAqP7LvoWWci/AvKvjz/xE -----END RSA PRIVATE KEY-----

6. Complete the following values in the *idpMetadata* section: (already configured for multi-authentication)

Parameter	Description
host	The entity ID of the identity provider. For example: https://openidp.feide.no
issuer	The entity ID of the identity provider. For example: https://openidp.feide.no
name	Friendly display name for the Identity
certFilePath	Provider (only for self-hosted MediaSpace) The absolute file system path of the crt file provided by Identity Provider.
certFileContent	The content of the certification file provided by Identity Provider that is used to validate the signature of the response.

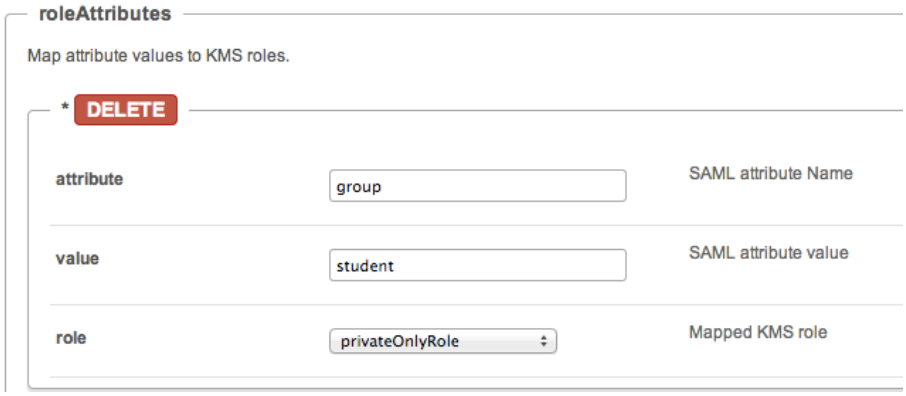
7. Complete the following values in the attributes section: (already configured for multi-authentication)

MediaSpace Attribute	Recommended SAML Attribute Name	Required?
userIdAttribute	SAML 2.0 attribute name, that will be used as the user identifier. Example: SAML 2.0 Persistent NameID or urn:oid:1.3.6.1.4.1.5923.1.1.1.6	No – nameId will be used if empty.
firstNameAttribute	Example: urn:oid:2.5.4.42	No
lastNameAttribute	Example: urn:oid:2.5.4.4	No
emailAttribute	Example: urn:oid:0.9.2342.19200300.100.1.3	No

8. In the **defaultRole** section, select the default role that should be assigned to each user that is authenticated. (already configured for multi-authentication)

NOTE: You can configure the option to retrive the role of the user from the Identity Provider through the *Auth → refreshRoleOnLogin* every time a user logs in. This option allows you also, to define a default role for all users and then manualy overide the role through the MediaSpace user management section.

9. In the **roleAttributes** section, map individual groups and values that are returned in the SAML response to a MediaSpace role. In the following example the SAML response will be parsed to find an attribute named *group*. If the attribute is found in the assertion and its value is student, the user will get the privateOnlyRole.



NOTE: If more than one attrbiute value is found (a user belongs to multiple groups) the user will be mapped to the role that was defined in the last *roleAttribute* found.

10. In the **roleAttributesCSV** section, map attribute values to KMS roles. Each CSV row should contain 3 values: attributeName,attributeValue,mediaSpaceRole. Invalid MediaSpace roles will not be saved. Click Load a new CSV to upload the new file.

    Enter the storageDataEntryId that stores the parsed CSV data.
11. In the **blockAuthorizationAttributes** (optional) map individual groups and values that are returned in the SAML response and should lead to unauthorizing an authenticated user from using MediaSpace.
12. The **unauthorizedBehavior** is applicable only if the blockAuthorizationAttributes is used. If usersuseInternalUnauthorizedPage is in use (set to 'yes') you can optionally set the text to be presented to the unauthorized user. If useInternalUnauthorizedPage is not used, you can specify the URL where the user will be redirected to.
13. Click on **Save** to apply the settings.
14. For authenticating with a single provider:

    Select SAML:IdP Initiated or SAML SP Initiated according to your authentication method.

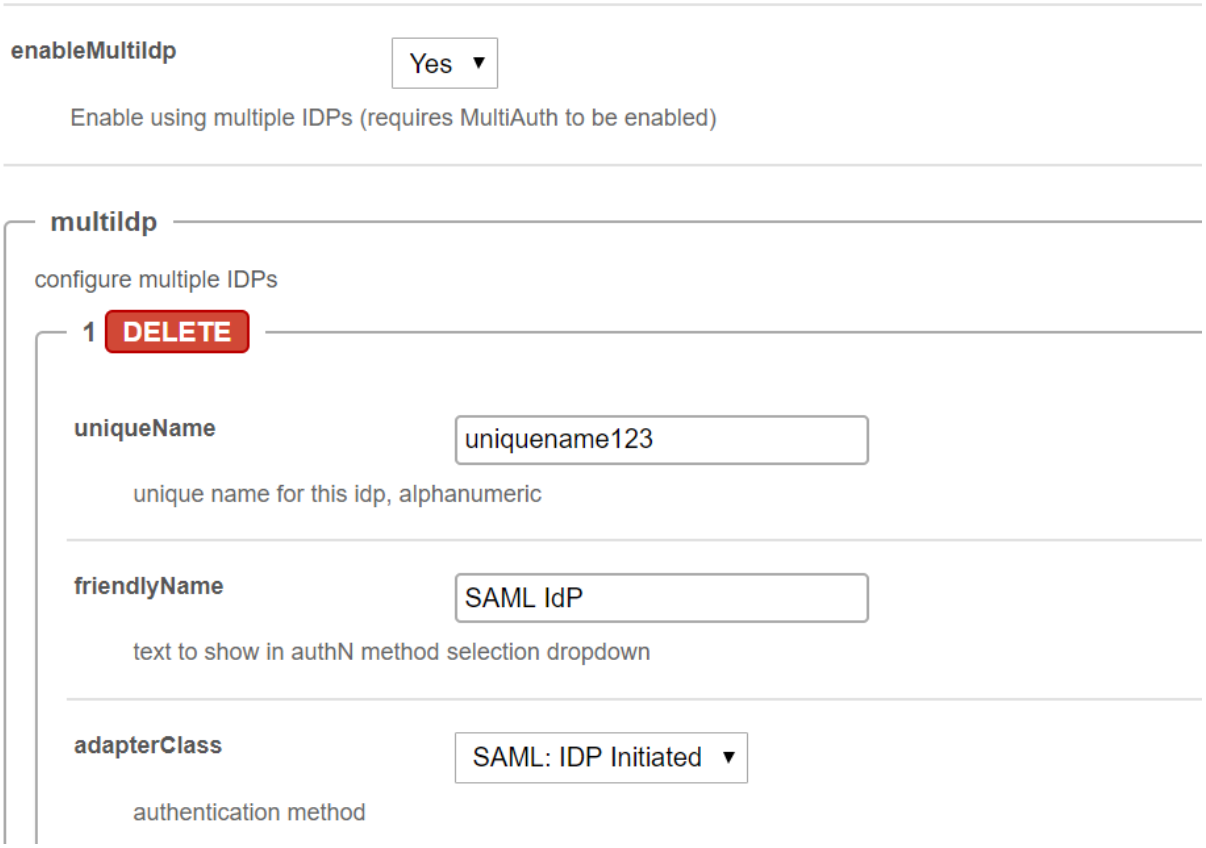
    For authenticating with multiple providers

    a. Go to the *Auth* module and Select Yes in the enableMultiAuth field.
    b. In the SAML Module enable enableMutliIdp.
    c. For each IdP: select the adapter class which may be either IdP or SP Iniated.
    d. After you configured mutliIdPs in the SAML method you can choose the authMethod from the drop-down list.
15. Click on **Save** to save the settings.

The Identity Provider(s) should be configured accordingly to support authentication requests from MediaSpace.

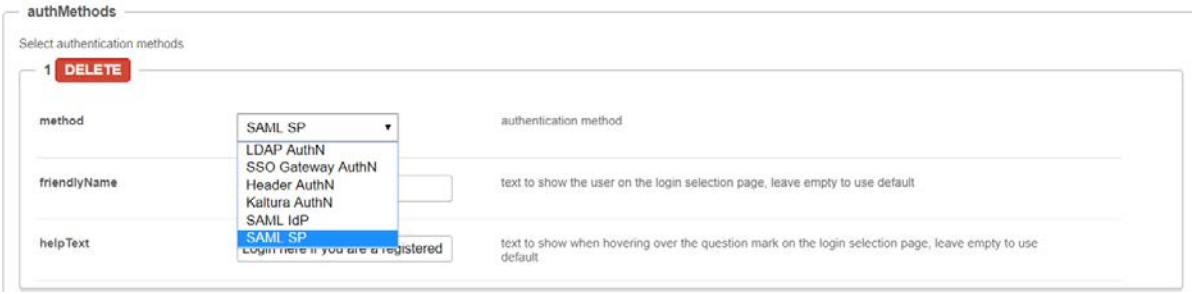
Example of User Interface for Multi-Authentication Configuration for SAML

1. Enable enanbleMultiAuth in the Auth module.
2. Enable enableMultiIdp in the SAML module and set up the IdP Configuration parameters in the SAML module.

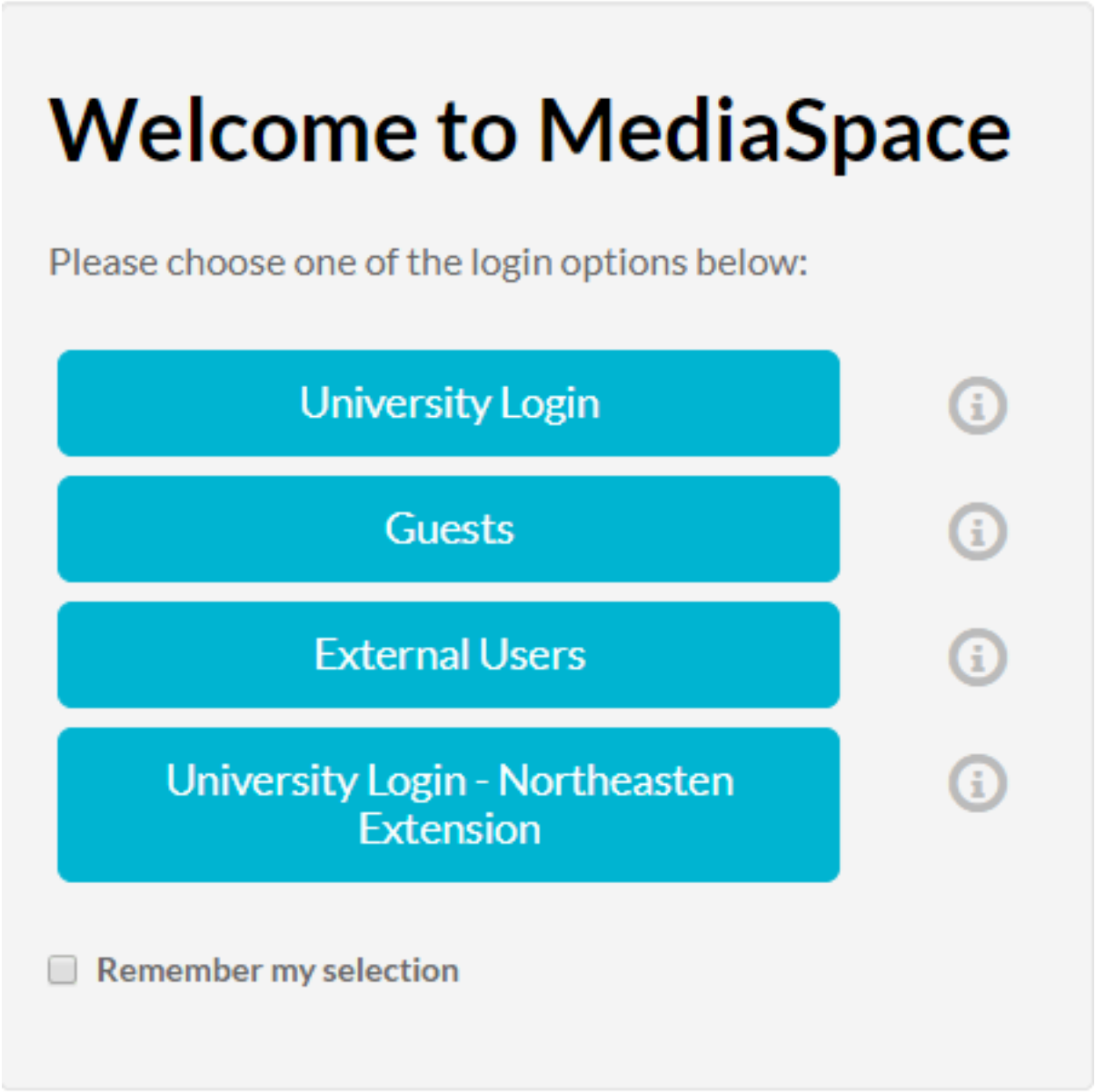


3. Go to the Auth module and slect the authMetho from the drop-down list.

   Example: In the authMethods section in the Auth module, select the chosen name from the drop down menu in the method field, for the SAML SP initiated authentication.



4. Go to your MediaSpace Site and select Login from the User drop down menu.



The University Login Northeastern Extension is configured to authenticate using SAML IdP.

Generating a Certificate Workflow

From Linux:

1. From a Linux or a Mac Terminal window execute the following command:

```
openssl req -new -x509 -days 3652 -nodes -out example.org.crt -
   newkey rsa:2048 -keyout example.org.pem
```

2. You will be prompted by the command line to enter additional data. Make sure to enter the name you used to generate the key for Common Name. In this example example.org. The following shows an example of the output screen:

```
>openssl req -new -x509 -days 3652 -nodes -out example.org.crt -
   newkey rsa:2048 -keyout example.org.pem
Generating a 2048 bit RSA private key
.....................................................+++
..............+++
writing new private key to 'example.org.pem'
-----
You are about to be asked to enter information that will be
   incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished
   Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [AU]:US
State or Province Name (full name) [Some-State]:New York
Locality Name (eg, city) []:New York
Organization Name (eg, company) [Internet Widgits Pty
   Ltd]:Kaltura
Organizational Unit Name (eg, section) []:
Common Name (e.g. server FQDN or YOUR name) []:example.org
Email Address []:
```

From Windows:

- Use OpenSSL. After downloading and extracting the package, execute the following from a command line in the extracted folder:

```
req  –new  –x509  –days  3652  –nodes  –config
   c:\openssl\openssl.cnf  –out  example.org.crt  –keyout
   example.org.pem
```

Both suggested options will generate two files:

- example.org.crt – This is the certificate containing the public key.
- example.org.pem – This is the private key. Please note that this file must be protected.

SAML Response Example

```
<samlp:Response xmlns:samlp="urn:oasis:names:tc:SAML:2.0:protocol"
xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion"
ID="_3ab056b68b199b976b49198cfa6b9e28b0317c4c6a" Version="2.0" IssueInstant="2013-04-
24T08:51:16Z" Destination="http://damian.mediaspace.kaltura.com/user/authenticate"
InResponseTo="_8d32fa51f5ef2b70fe6d619000c5aedb143bfb937c">
              <saml:Issuer>https://openidp.feide.no</saml:Issuer>
              <ds:Signature xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
                           <ds:SignedInfo>
                                        <ds:CanonicalizationMethod
Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#"/>
                                        <ds:SignatureMethod
```

```
Algorithm="http://www.w3.org/2000/09/xmldsig#rsa-sha1"/>
                                        <ds:Reference
URI="#_3ab056b68b199b976b49198cfa6b9e28b0317c4c6a">
                                                <ds:Transforms>
                                                        <ds:Transform
Algorithm="http://www.w3.org/2000/09/xmldsig#enveloped-signature"/>
                                                        <ds:Transform
Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#"/>
                                                </ds:Transforms>
                                                <ds:DigestMethod
Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"/>

<ds:DigestValue>pTsLnZhfAW6Zn/LRxATMmed1zag=</ds:DigestValue>
                                        </ds:Reference>
                                </ds:SignedInfo>

<ds:SignatureValue>iN+urKe/LFlwPyRCgvAY85QvDDSUb43vx8Rk7UpSKO/mGdcoJJNkc/GUBpUtEopqBDbCFE4HQX5
Gr8rMWdEgLV9oTyYLmCKrRSyIewsx8flL/w6swcCKTVWph1lnLGgqXOr7DSTpj0TvsQQPygifovbvc9rh6g72ONJPEj84g
sQ=</ds:SignatureValue>
                                <ds:KeyInfo>
                                        <ds:X509Data>

<ds:X509Certificate>MIICizCCAfQCCQCY8tKaMc0BMjANBgkqhkiG9w0BAQUFADCBiTELMAkGA1UEBhMCTk8xEjAQBg
NVBAgTCVRyb25kaGVpbTEQMA4GA1UEChMHVU5JTkVUVDEOMAwGA1UECxMFRmVpZGUxGTAXBgNVBAMTEG9wZW5pZHAuZmVp
ZGUubm8xKTAnBgkqhkiG9w0BCQEWGmFuZHJlYXMuc29sYmVyZ0B1bmluZXR0Lm5vMB4XDTA4MDUwODA5MjI0OFoXDTM1MD
kyMzA5MjI0OFowgYkxCzAJBgNVBAYTAk5PMRIwEAYDVQQIEwlUcm9uZGhlaW0xEDAOBgNVBAoTB1VOSU5FVFQxDjAMBgNV
BAsTBUZlaWRlMRkwFwYDVQQDExBvcGVuaWRwLmZlaWRlLm5vMSkwJwYJKoZIhvcNAQkBFhphbmRyZWFzLnNvbGJlcmdAdW
5pbmV0dC5ubzCBnzANBgkqhkiG9w0BAQEFAAOBjQAwgYkCgYEAt8jLoqI1VTlxAZ2axiDIThWcAOXdu8KkVUWaN/SooO9O
0QQ7KRUjSGKN9JK65AFRDXQkWPAu4HlnO4noYlFSLnYyDxI66LCr71x4lgFJjqLeAvB/GqBqFfIZ3YK/NrhnUqFwZu63nL
rZjcUZxNaPjOOSRSDaXpv1kb5k3jOiSGECAwEAATANBgkqhkiG9w0BAQUFAAOBgQBQYj4cAafWaYfjBU2zi1ElwStIaJ5n
yp/s/8B8SAPK2T79McMyccP3wSW13LHkmM1jwKe3ACFXBvqGQN0IbcH49hu0FKhYFM/GPDJcIHFBsiyMBXChpye9vBaTNE
BCtU3KjjyG0hRT2mAQ9h+bkPmOvlEo/aH0xR68Z9hw4PF13w==</ds:X509Certificate>
                                        </ds:X509Data>
                                </ds:KeyInfo>
                        </ds:Signature>
                        <samlp:Status>
                                <samlp:StatusCode
Value="urn:oasis:names:tc:SAML:2.0:status:Success"/>
                        </samlp:Status>
                        <saml:Assertion xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xmlns:xs="http://www.w3.org/2001/XMLSchema" ID="_37b2602c8e0327a7896367288c195e0982fea1e511"
Version="2.0" IssueInstant="2013-04-24T08:51:16Z">
                                <saml:Issuer>https://openidp.feide.no</saml:Issuer>
                                <ds:Signature xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
                                        <ds:SignedInfo>
                                                <ds:CanonicalizationMethod
Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#"/>
                                                <ds:SignatureMethod
Algorithm="http://www.w3.org/2000/09/xmldsig#rsa-sha1"/>
                                                <ds:Reference
URI="#_37b2602c8e0327a7896367288c195e0982fea1e511">
                                                        <ds:Transforms>

<ds:Transform Algorithm="http://www.w3.org/2000/09/xmldsig#enveloped-signature"/>

<ds:Transform Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#"/>
                                                        </ds:Transforms>
                                                        <ds:DigestMethod
Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"/>

<ds:DigestValue>jVKo/6IZjEllyA5lYjgXxJQ3YmQ=</ds:DigestValue>
                                                </ds:Reference>
                                        </ds:SignedInfo>

<ds:SignatureValue>NCKBpIuggEjdNm7QL16oOrKXUmZQ2eaQbANtyIVqrRs67tUnExRcac3Vrqiso4H/4FQRGdWdS1f
6Yh2uo0psItwzTuPkDrv2QotuWSiAFo54bABDj9Q+wVKBqk1ShgiQ7RCBoJDK1V1k/A7dm7CMCGW2GNYZl8q35tgKccJzv
7o=</ds:SignatureValue>
                                        <ds:KeyInfo>
```

```
                                                        <ds:X509Data>

<ds:X509Certificate>MIICizCCAfQCCQCY8tKaMc0BMjANBgkqhkiG9w0BAQUFADCBiTELMAkGA1UEBhMCTk8xEjAQBg
NVBAgTCVRyb25kaGVpbTEQMA4GA1UEChMHVU5JTkVUVDEOMAwGA1UECxMFRmVpZGUxGTAXBgNVBAMTEG9wZW5pZHAuZmVp
ZGUubm8xKTAnBgkqhkiG9w0BCQEWGmFuZHJlYXMuc29sYmVyZ0B1bmluZXR0Lm5vMB4XDTA4MDUwODA5MjI0OFoXDTM1MD
kyMzA5MjI0OFowgYkxCzAJBgNVBAYTAk5PMRIwEAYDVQQIEwlUcm9uZGhlaW0xEDAOBgNVBAoTB1VOSU5FVFQxDjAMBgNV
BAsTBUZlaWRlMRkwFwYDVQQDExBvcGVuaWRwLmZlaWRlLm5vMSkwJwYJKoZIhvcNAQkBFhphbmRyZWFzLnNvbGJlcmdAdW
5pbmV0dC5ubzCBnzANBgkqhkiG9w0BAQEFAAOBjQAwgYkCgYEAt8jLoqI1VTlxAZ2axiDIThWcAOXdu8KkVUWaN/SooO9O
0QQ7KRUjSGKN9JK65AFRDXQkWPAu4HlnO4noYlFSLnYyDxI66LCr71x4lgFJjqLeAvB/GqBqFfIZ3YK/NrhnUqFwZu63nL
rZjcUZxNaPjOOSRSDaXpv1kb5k3jOiSGECAwEAATANBgkqhkiG9w0BAQUFAAOBgQBQYj4cAafWaYfjBU2zi1ElwStIaJ5n
yp/s/8B8SAPK2T79McMyccP3wSW13LHkmM1jwKe3ACFXBvqGQN0IbcH49hu0FKhYFM/GPDJcIHFBsiyMBXChpye9vBaTNE
BCtU3KjjyG0hRT2mAQ9h+bkPmOvlEo/aH0xR68Z9hw4PF13w==</ds:X509Certificate>
                                                        </ds:X509Data>
                                                </ds:KeyInfo>
                                        </ds:Signature>
                                        <saml:Subject>
                                                <saml:NameID
SPNameQualifier="damian.mediaspace.kaltura.com" Format="urn:oasis:names:tc:SAML:2.0:nameid-
format:transient">_18d5ad80174e8498d0703c9f5b1976566a50704f9f</saml:NameID>
                                                <saml:SubjectConfirmation
Method="urn:oasis:names:tc:SAML:2.0:cm:bearer">
                                                        <saml:SubjectConfirmationData
NotOnOrAfter="2013-04-24T08:56:16Z"
Recipient="http://damian.mediaspace.kaltura.com/user/authenticate"
InResponseTo="_8d32fa51f5ef2b70fe6d619000c5aedb143bfb937c"/>
                                                </saml:SubjectConfirmation>
                                        </saml:Subject>
                                        <saml:Conditions NotBefore="2013-04-24T08:50:46Z"
NotOnOrAfter="2013-04-24T08:56:16Z">
                                                <saml:AudienceRestriction>

<saml:Audience>damian.mediaspace.kaltura.com</saml:Audience>
                                                </saml:AudienceRestriction>
                                        </saml:Conditions>
                                        <saml:AuthnStatement AuthnInstant="2013-04-24T08:51:16Z"
SessionNotOnOrAfter="2013-04-24T16:51:16Z"
SessionIndex="_2b2053d785ab116b42ca5e57a9e9a7a40ff1673895">
                                                <saml:AuthnContext>

<saml:AuthnContextClassRef>urn:oasis:names:tc:SAML:2.0:ac:classes:Password</saml:AuthnContextC
lassRef>
                                                </saml:AuthnContext>
                                        </saml:AuthnStatement>
                                        <saml:AttributeStatement>
                                                <saml:Attribute Name="uid"
NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:uri">
                                                        <saml:AttributeValue
xsi:type="xs:string">roman-kreichman</saml:AttributeValue>
                                                </saml:Attribute>
                                                <saml:Attribute Name="givenName"
NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:uri">
                                                        <saml:AttributeValue
xsi:type="xs:string">Roman</saml:AttributeValue>
                                                </saml:Attribute>
                                                <saml:Attribute Name="sn"
NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:uri">
                                                        <saml:AttributeValue
xsi:type="xs:string">Kreichman</saml:AttributeValue>
                                                </saml:Attribute>
                                                <saml:Attribute Name="cn"
NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:uri">
                                                        <saml:AttributeValue
xsi:type="xs:string">Roman Kreichman</saml:AttributeValue>
                                                </saml:Attribute>
                                                <saml:Attribute Name="mail"
NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:uri">
                                                        <saml:AttributeValue
xsi:type="xs:string">roman.kreichman@kaltura.com</saml:AttributeValue>
                                                </saml:Attribute>
```

```
                                        <saml:Attribute Name="eduPersonPrincipalName"
NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:uri">
                                                <saml:AttributeValue
xsi:type="xs:string">roman-kreichman@rnd.feide.no</saml:AttributeValue>
                                        </saml:Attribute>
                                        <saml:Attribute Name="eduPersonTargetedID"
NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:uri">
                                                <saml:AttributeValue
xsi:type="xs:string">bdb1871794ce63c792caa42adc93f233df652e01</saml:AttributeValue>
                                        </saml:Attribute>
                                        <saml:Attribute
Name="urn:oid:0.9.2342.19200300.100.1.1" NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-
format:uri">
                                                <saml:AttributeValue
xsi:type="xs:string">roman-kreichman</saml:AttributeValue>
                                        </saml:Attribute>
                                        <saml:Attribute Name="urn:oid:2.5.4.42"
NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:uri">
                                                <saml:AttributeValue
xsi:type="xs:string">Roman</saml:AttributeValue>
                                        </saml:Attribute>
                                        <saml:Attribute Name="urn:oid:2.5.4.4"
NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:uri">
                                                <saml:AttributeValue
xsi:type="xs:string">Kreichman</saml:AttributeValue>
                                        </saml:Attribute>
                                        <saml:Attribute Name="urn:oid:2.5.4.3"
NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:uri">
                                                <saml:AttributeValue
xsi:type="xs:string">Roman Kreichman</saml:AttributeValue>
                                        </saml:Attribute>
                                        <saml:Attribute
Name="urn:oid:0.9.2342.19200300.100.1.3" NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-
format:uri">
                                                <saml:AttributeValue
xsi:type="xs:string">roman.kreichman@kaltura.com</saml:AttributeValue>
                                        </saml:Attribute>
                                        <saml:Attribute
Name="urn:oid:1.3.6.1.4.1.5923.1.1.1.6" NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-
format:uri">
                                                <saml:AttributeValue
xsi:type="xs:string">roman-kreichman@rnd.feide.no</saml:AttributeValue>
                                        </saml:Attribute>
                                        <saml:Attribute
Name="urn:oid:1.3.6.1.4.1.5923.1.1.1.10" NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-
format:uri">
                                                <saml:AttributeValue
xsi:type="xs:string">bdb1871794ce63c792caa42adc93f233df652e01</saml:AttributeValue>
                                        </saml:Attribute>
                                </saml:AttributeStatement>
                        </saml:Assertion>
</samlp:Response>
```