totemomail® Connection to SwissSign CA

This document describes the configuration of **totemo**mail® with the SwissSign CA.

totemo ag
Freihofstrasse 22, CH-8700 Küsnacht, info@totemo.com, www.totemo.com, T +41 44 914 99 00, F +41 44 914 99 99

totemomail®

Contents

1. Introduction

This document describes the configuration of **totemo**mail® with the SwissSign CA. **totemo**mail® supports connection to the SwissSign CA using the RFC2797 interface.

1.1. Conventions Used in This Manual

`Monospaced font`	This font is used for text that appears on the computer screen or text that you should type.
Boldface	This is used for button names, links or checkboxes.
|	The vertical bar is used as a separator for user interface elements. For example Administration | Notifications means that you should click on the **Administration** link or button first and then on **Notifications**.

1.2. Requirements

In order to use the external SwissSign CA with **totemo**mail®, a license with the option **Connectivity to external Certificate Authority for internal user certificates** is required. The minimum requirements regarding the **totemo**mail® build version for the SwissSign CA is the following:

- **totemo**mail® 5.0 Build 577 or newer
- **totemo**mail® 6.0 Build 52 or newer

2. totemomail® PKI Configuration

2.1. Basic Configuration

1. In the administration console under **Certificates | Issuer Certificates** import the **root certificate** files which were provided by SwissSign. After the import, trust these manually via the **Set as trusted** button.
2. Under **Certificates | Issuer Certificates** import the **SSL certificate** which was provided by SwissSign. After the import, trust it manually via the **Set as trusted** button.
3. Under **Certificates | Authentication Certificates** import the **Registration Authority Officer certificate** which was provided by SwissSign. This is a P12-file containing a private key and the corresponding certificate. After the import, set the linked service via the **Set Auth. Service** button to `RFC 2797`.
4. In the administration console, navigate to **Server Options | RFC 2797 conn. | Connection** to configure the connection specific parameters.

   Note: The values for the following properties are provided by SwissSign.

   a. Specify the connection protocol with the property `connection.ssl.protocol`.
   Example: `https://`

   b. Set the server name of the SwissSign CA with the property `connection.ssl.serverName`.
   Example: `ra.swisssign.net`

   c. Set the server port of the SwissSign CA with the property `connection.ssl.serverPort`.
   Example: `443`

   d. Set the request path with the provided information in the property `connection.ssl.url`.
   Example: `/ws/cmc?account=totemoag.ra&product=totemo-perso-gold&validity=3y`

   e. Set the request type by setting the property `security.pkiConnection.rfc2797.requestType` to **POST**.

   f. Set the property `security.pkiConnection.rfc2797.encodeRequestBase64` to **false**.

5. Under **Server Options | RFC 2797 conn. | Connection** the PKI type has to be set via the property `security.pkiConnection.type` to `rfc2797`.
6. Set the issuer DN for SwissSign certificates, as value in the property `security.pkiConnection.rfc2797.issuerDN`. This is used by **totemo**mail® to identify which of the stored certificates where issued by the connected SwissSign CA.
7. To allow that new internal users get their certificates from the external CA automatically after creation, set the property `security.pkiConnection.getFromPKIForNewIntUsers` to `true`.
8. To allow external recipients to get their certificates from the external CA, set the property `security.pkiConnection.getFromPKIForNewRecipients` to `true`.
9. Set the property `security.pkiConnection.certSubjectDN` to the value that should be used as a subject DN within SwissSign certificates.
   Note: The value of this property is provided by SwissSign. When using a SwissSign Silver PKI, the value should only contain the CN. For SwissSign Gold PKI the value may contain organization specific DN attributes.

   Note: The CN (only for SwissSign Gold) and email address attributes in the subject DN will be replaced by the information corresponding to the requesting user.
10. To enable the external CA set the property `security.pkiConnection.enabled` to `true`.
11. Apply the changes with the **Apply Changes** button on the top of the settings/properties page.
12. Restart the **totemo**mail® service.

Note: The requesting user must use an email address with the domain specified by SwissSign.

2.2. Domain Specific Properties

It is possible to configure domain specific properties that are used to request certificates for related users. These properties are used when users' email addresses match the domain for the property. Domain specific properties are created by extending the standard property name with a domain.

The following properties can be used for domain specific configuration:

`security.pkiConnection.certSubjectDN.$DOMAIN_NAME`

`connection.ssl.serverName.$DOMAIN_NAME`

`connection.ssl.url.$DOMAIN_NAME`

`connection.ssl.serverPort.$DOMAIN_NAME`

Note: The variable `$DOMAIN_NAME` above has to be replaced with the domain name, e.g. `connection.ssl.url.totemo.com`.

The Registration Authority Officer certificate can also be assigned to a specific domain under **Certificates | Authentication Certificates** via the **Set Auth. Service** button.

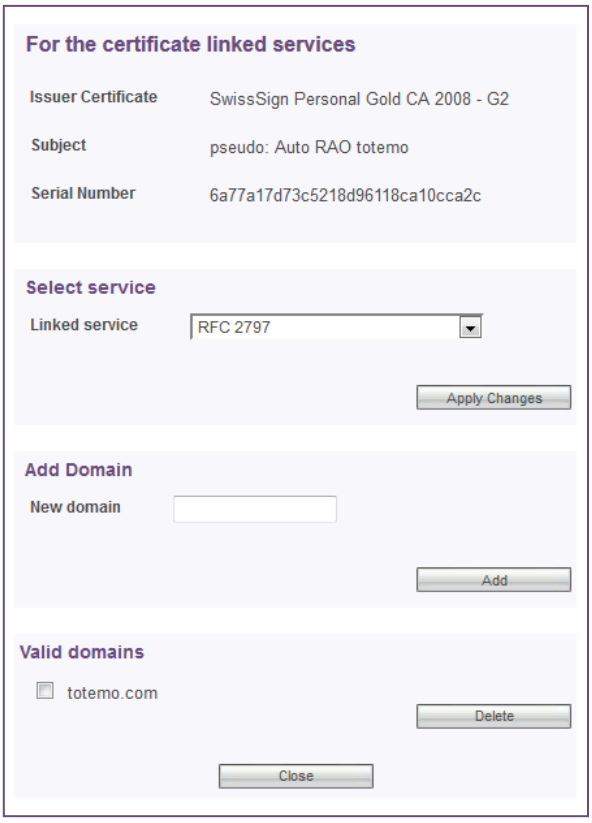

Figure 1: Set authentication service page

Note: The template file rfc2797_domain_specific_properties_template.xml can be used to create the mentioned properties. It contains the placeholder `$DOMAIN_NAME` that has to be replaced with the actual domain. The resulting properties can be afterwards imported with the administration console under **Server Options | Importing and Exporting Properties**.

3. Testing the PKI connection

- If the property `security.pkiConnection.getFromPKIForNewIntUsers` or `security.pkiConnection.getFromPKIForNewRecipients` is enabled, new internal users or recipients can be created to verify that their S/MIME certificate is issued by SwissSign.
- SwissSign certificates may be also manually requested by navigating to **User Management | Users** or **User Management | Recipients**. Click on (“certificate” icon) on one of the users and click on the **Get from CA** button to start a manual request.