Update the SSO signing and encryption key

When the SSO signing and encryption key needs to be updated, it's performed in three distinct steps in order to enable a rollover period for existing integrations to update their metadata.

In principle, the procedure follows the following steps:

1. Start rollover period: Include the new certificate in the SSO metadata and deliver the updated metadata to all SAML SP application integrations.
2. Change the SSO signing and encryption key.
   a. All identity provider integrations as well as non-SAML SP application integrations should be updated now, since the key rollover described here works only with SAML SP integrations
3. Inform all integrations to retrieve the updated the SSO metadata with only the new key.

> **Important**
>
> All integrations encrypting some data to SSO with SSO's encryption key. Once the key is updated (i.e. the second step is finished, but 2.a step is not finished), SSO will not be able to decrypt their encrypted data before the final metadata with only the new key is updated to those integrations.
>
> These integrations include at least:
>
> - SAML2 Service Providers, that include encrypted subject in AuthnRequests or LogoutRequests.
>   - Ubisecure SAML SP component includes no subject in either element, unless explicitly done so in an AuthnRequestEventListener implemented by the integrator.
> - All identity providers
>
> To enable key rollover in these cases, Ubisecure SSO needs to be able to use two encryption keys simultaneously. This is a new feature and you can contact our support to enquire it's availability in future versions.

Step-by-step guide for Windows

> All commands are expected to be run in a PowerShell console.
>
> Command `java` requires Java Runtime Environment to be installed.

Preliminary steps to prepare the PowerShell session.

1. Change the current folder to ubilogin folder.

```
cd "C:\Program Files\Ubisecure\ubilogin-sso\ubilogin"
```

Steps for creating the new key in SSO config file and adding it to the SSO SAML2 metadata.

1. Create a new key pair in the SSO config file. Keysize can be set as desired.

```
java -jar ..\tools\ubikt.jar -ubilogin win32.config -generate -keysize 2048
```

2. Export the public key from the SSO config file in XML format in a separate XML-file.

```
java -jar ..\tools\ubikt.jar -ubilogin win32.config -publickey key.xml -xml

# or if you want expose the certificate instead of plain public key, use the command below instead
#java -jar ..\tools\ubikt.jar -ubilogin win32.config -cert key.xml -xml
```

3. Download the SAML2 metadata from SSO.

```
$metadata = Invoke-WebRequest -Uri https://sso.example.com:8443/uas/saml2/metadata.xml
```

4. Add the public key in a XML form into the metadata.xml.

```
$keydesc = "<md:KeyDescriptor>$(Get-Content "key.xml")</md:KeyDescriptor>"
$metadata.Content -replace "(</md:KeyDescriptor>)", "`$1$keydesc" | Set-Content -path "metadata.xml"
```

5. The created metadata.xml now contains the new certificate and can be delivered to all integrations (applications and identity providers) for the duration of the rollover period.

Steps for updating the SSO signing and encryption key

1. Ensure that the new win32.config is valid with ubikt.

```
java -jar ../tools/ubikt.jar -ubilogin win32.config
```

Expected output is something like:

```
Version: 3
Subject: CN=Ubilogin, DC=test
Issuer: CN=Ubilogin, DC=test
NotBefore: 2016-09-05T00:00:00Z
NotAfter: 2027-09-05T00:00:00Z
SerialNumber: 38a456e1ee22802b
SigAlg: SHA256withRSA
SHA256: d91b88d280f529ba38d3489ccd7a7d27fe7c2ff71a2c7ffd94d6caa9284d62c1
SHA1: 275de983cbb2656acdfb5e19685addb4490981dd
MD5: 9ec19c1972861a48bc8a0f95f22cbaff
```

2. Stop SSO Server.

```
net stop UbiloginServer
```

3. Run SSO setup script.

```
.\setup.cmd
```

4. Update SSO Tomcat.

```
.\config\tomcat\update.cmd
```

5. Import secrets.ldif to Ubilogin Directory.

```
.\ldap\adam\import.cmd .\ldap\secrets.ldif
```

6. Start SSO Server.

```
net start UbiloginServer
```

7. SSO metadata with only the new certificate is now available in the SSO SAML2 metadata URL https://sso.example.com:8443/uas/saml2/metadata.xml to be fetched by integrations.

Related articles

- Add Organizations/Users to Ubisecure extranet
- IDP Initiated SSO if SP doesn’t initiate login
- Use an unsolicited SSO or an IDP initiated SSO
- Upgrade and migrate to new version of PostgreSQL
- Disable encryption of SAML logout requests