SureLC

SAML SSO Implementation Guide

Contents

Revision History

Version Number	Date of Revision	Author	Section/Page changed	Details of changes
1.0	2022-11-30	Alex Oleynik	1-10	Initial version.
1.1	2023-07-18	Alex Oleynik	5	FirstName, LastName attributes changed to mandatory. Added agentId optional attribute.
1.2	2023-10-11	Alex Oleynik	7	Added attributes description for carrier user roles.

1. About SureLC SSO

SureLC has its own SSO implementation based on the Security Assertion Markup Language (SAML 2.0) standard which defines a framework for exchanging security information between online business partners.

1.1. Description of SureLC SSO

SureLC SSO allows third-party/partner applications to have hyperlinks acting as entry points into the SureLC application.

In this scenario, using SAML terminology, the partner application acts as asserting party (IdP - identity provider), and SureLC acts as a relying party (SP - service provider). An asserting party is a system entity that makes SAML assertions. It is also sometimes called a SAML authority. A relying party is a system entity that uses assertions it has received.

For security reasons, HTTPS is used as a transport protocol and assertions should be signed with valid certificates.

1.2. Destination login overview

SureLC SSO supports two sign-in flows: Idp initiated and SP initiated.

- For the IdP-initiated sign-in flow, a user authenticated by IdP tries to access SureLC from a partner website. SureLC expects to receive authentication statements and attribute statements in upcoming assertions.
- For SP-initiated flow, a not authenticated user tries to access SureLC. In this case, he will be redirected to the IdP login endpoint provided in SAML metadata. After successful login by IdP, he will be redirected back to SureLC.

SureLC SAML SSO allows two types of users to login into the system: agency workers and producers. Each role uses a different application which should be specified in the appropriate attribute.

2. Process of SSO configuration.

The process of SureLC SSO configuration consists of several steps:

1. Partner applications should be able to create signed SAML assertion with attributes statement using SAML HTTP POST Binding.
2. The partner should be able to create SAML metadata XML.
3. Create a public/private key pair for assertion signing and export the public key certificate in X.509 format encoded according to Internet RFC 1421 Certificate Encoding Standard.
4. Contact Surancebay and provide the issuer identifier, public key certificate, and SAML metadata.

2.1. SureLC information required for SSO.

Assertions should provide a persistent user ID inside the tag Subject/NameID. It will be captured during the first login and bound to the created user record.

2.1.1 Producer role

SureLC SAML implementation requires the following attributes to be presented in the assertion for the producer role:

Attribute name	Value
application	producer
firstName	Producer’s first name
lastName	Producer’s last name

The following attributes are optional and can be provided to streamline producer registration:

Attribute name	Value
agentId	Agent ID from the agency’s AMS system. Can be later obtained via REST API.

email	Producer’s email
ssn	Producer’s ssn
dob	Producer’s DOB in the format mm/dd/yyyy
cell	Producer’s cell
phone	Producer’s phone
fax	Producer’s fax
dba	Type of DoingBusinessAs for the producer: “P” - individual “B” - business entity “S” - licensed only agent-solicitor “I” - institutional agent
solicitingForId	When the value of dba is S(see above) the (SureLC) id of the producer that the agent is soliciting for. (Can be retrieved using SureLC API)
branch	Name of the affiliation, when applicable

2.1.2 Agency user role

SureLC SAML implementation requires the following attributes to be presented in the assertion for the agency user role:

Attribute name	**Value**
application	bga
roles	comma-separated roles list (agencyWorker,subAgencyWorker)
email	User’s email
firstName	User’s first name
lastName	User’s last name

2.1.3 Carrier user role

SureLC SAML implementation requires the following attributes to be presented in the assertion for the carrier user role:

Attribute name	Value
application	carriers
roles	comma-separated roles list (carrierWorker,carrierManager)
email	User's email
firstName	User's first name
lastName	User's last name

2.2. SAML endpoints.

UAT environment:
Entity ID: https://uat.surancebay.com/samlbr/saml/SSO
ACS URL: https://uat.surancebay.com/samlbr/saml/SSO
Metadata URL: https://uat.surancebay.com/samlbr/saml/metadata

Production environment:
Entity ID: https://surelc.surancebay.com/samlbr/saml/SSO
ACS URL: https://surelc.surancebay.com/samlbr/saml/SSO
Metadata URL: https://surelc.surancebay.com/samlbr/saml/metadata

2.3. Assertion signing.

SureLC SSO implementation verifies assertion digital signature. It selects the appropriate key by checking the assertion "Issuer" field. Please make sure that the issuer identifier provided to SureLC is the same as used in the assertion.

A public key certificate can be self-signed.

Example of keys and certificate generation using Java keytool:

keytool -genkey -alias ga -keystore ga.jks -validity 3650

Export public keys certificates to ga.cert file:

keytool -export -alias ga -keystore ga.jks -file ga.cert -rfc

Created ga.cert file should be sent to SureLC.

3. Assertion example.

```
<?xml version="1.0" encoding="UTF-8"?>
<saml2p:Response xmlns:saml2p="urn:oasis:names:tc:SAML:2.0:protocol"
                 Destination="http://uat.surancebay.com/samlbr/saml/SSO"
                 ID="ade5c2e0-5498-4c9b-b35f-44775bbe1e40"
                 IssueInstant="2013-11-19T13:58:30.604Z" Version="2.0"
                 xmlns:xs="http://www.w3.org/2001/XMLSchema">
    <saml2:Issuer xmlns:saml2="urn:oasis:names:tc:SAML:2.0:assertion">
        http://ga.com
    </saml2: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#dsa-sha1"/>
            <ds:Reference URI="#ade5c2e0-5498-4c9b-b35f-44775bbe1e40">
                <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#">
                        <ec:InclusiveNamespaces
                                xmlns:ec="http://www.w3.org/2001/10/xml-exc-c14n#"
                                PrefixList="xs"/>
                    </ds:Transform>
                </ds:Transforms>
                <ds:DigestMethod
                        Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"/>
                <ds:DigestValue>SkdxsBMPJJ3krHRzUgJqIw4cH1U=</ds:DigestValue>
            </ds:Reference>
        </ds:SignedInfo>
        <ds:SignatureValue>
            kkucBejU8qGEnEDwgoJw8+OfN11gf3JZS5S8TTQWin3FCbGVTUppzw==
        </ds:SignatureValue>
        <ds:KeyInfo>
            <ds:X509Data>
                <ds:X509Certificate>
```

```
MIIDETCCAs+gAwIBAgIEUDURGTALBgcqhkjOOAQDBQAwbDEQMA4GA1UEBhMHVW5rbm93bjEQMA4G
A1UECBMHVW5rbm93bjEQMA4GA1UEBxMHVW5rbm93bjEQMA4GA1UEChMHVW5rbm93bjEQMA4GA1UE
CxMHVW5rbm93bjEQMA4GA1UEAxMHVW5rbm93bjAeFw0xMjA4MjIxNzA0MjVaFw0yMjA4MjAxNzA0
MjVaMGwxEDAOBgNVBAYTB1Vua25vd24xEDAOBgNVBAgTB1Vua25vd24xEDAOBgNVBAcTB1Vua25v
d24xEDAOBgNVBAoTB1Vua25vd24xEDAOBgNVBAsTB1Vua25vd24xEDAOBgNVBAMTB1Vua25vd24w
ggG3MIIBLAYHKoZIzjgEATCCAR8CgYEA/X9TgR11EilS30qcLuzk5/YRt1I870QAwx4/gLZRJmlF
XUAiUftZPY1Y+r/F9bow9subVWzXgTuAHTRv8mZgt2uZUKWkn5/oBHsQIsJPu6nX/rfGG/g7V+fG
qKYVDwT7g/bTxR7DAjVUE1oWkTL2dfOuK2HXKu/yIgMZndFIAccCFQCXYFCPFSMLzLKSuYKi64QL
8Fgc9QKBgQD34aCF1ps93su8q1w2uFe5eZSvu/o66oL5V0wLPQeCZ1FZV4661FlP5nEHEIGAtEkW
cSPoTCgWE7fPCTKMyKbhPBZ6i1R8jSjgo64eK7OmdZFuo38L+iE1YvH7YnoBJDvMpPG+qFGQiaiD
3+Fa5Z8GkotmXoB7VSVkAUw7/s9JKgOBhAACgYB70rTPsck7jBIrU+qKs0Ght3oE/efsNQLzHQOw
RZ8Rqj/GWExCN+2Lm8j2duKS3lum0JGLX4aKofGYpqlr3qwoRuwmLZVqzGVaNcpUE5a9Y25i6bPp
EJ3i87NDLkX+5k7niaXUSl46V/2Z72vRRK1AAoMFuMuJWcDLSCgYfDcazTALBgcqhkjOOAQDBQAD
LwAwLAIUT3bOz5wEaEaGaRSm/pRO7Kc5+pMCFDiAZ1nfPYUxZPPPE3gjgec7z5OE
```

```
                </ds:X509Certificate>
            </ds:X509Data>
        </ds:KeyInfo>
    </ds:Signature>
    <saml2p:Status>
        <saml2p:StatusCode Value="urn:oasis:names:tc:SAML:2.0:status:Success"/>
    </saml2p:Status>
    <saml2:Assertion xmlns:saml2="urn:oasis:names:tc:SAML:2.0:assertion"
                     ID="1ab4009a-744b-44c6-b01f-5fb7f2b790b1"
                     IssueInstant="2013-11-19T13:58:30.505Z" Version="2.0">
        <saml2:Issuer>http://ga.com</saml2:Issuer>
        <saml2:Subject>
            <saml2:NameID
                    Format="urn:oasis:names:tc:SAML:2.0:nameid-format:persistent">
                5555-5555-5
            </saml2:NameID>
        </saml2:Subject>
        <saml2:Conditions NotBefore="2013-11-19T13:58:15.505Z"
                          NotOnOrAfter="2013-11-19T13:59:00.505Z"/>
        <saml2:AuthnStatement>
            <saml2:AuthnContext>
                <saml2:AuthnContextClassRef>
                    urn:oasis:names:tc:SAML:2.0:ac:classes:PasswordProtectedTransport
                </saml2:AuthnContextClassRef>
            </saml2:AuthnContext>
        </saml2:AuthnStatement>
        <saml2:AttributeStatement>
            <saml2:Attribute Name="application">
                <saml2:AttributeValue
                        xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
                        xsi:type="xs:string">producer
                </saml2:AttributeValue>
            </saml2:Attribute>
            <saml2:Attribute Name="lastName">
                <saml2:AttributeValue
                        xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
                        xsi:type="xs:string">Smith
                </saml2:AttributeValue>
            </saml2:Attribute>
            <saml2:Attribute Name="phone">
                <saml2:AttributeValue
                        xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
                        xsi:type="xs:string">1234567890
```

```
                </saml2:AttributeValue>
            </saml2:Attribute>
            <saml2:Attribute Name="fax">
                <saml2:AttributeValue
                        xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
                        xsi:type="xs:string">123456789
                </saml2:AttributeValue>
            </saml2:Attribute>
            <saml2:Attribute Name="email">
                <saml2:AttributeValue
                        xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
                        xsi:type="xs:string">joe.smith@surancebay.com
                </saml2:AttributeValue>
            </saml2:Attribute>
            <saml2:Attribute Name="cell">
                <saml2:AttributeValue
                        xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
                        xsi:type="xs:string">5653454321
                </saml2:AttributeValue>
            </saml2:Attribute>
            <saml2:Attribute Name="ssn">
                <saml2:AttributeValue
                        xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
                        xsi:type="xs:string">191645845
                </saml2:AttributeValue>
            </saml2:Attribute>
            <saml2:Attribute Name="firstName">
                <saml2:AttributeValue
                        xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
                        xsi:type="xs:string">Joe
                </saml2:AttributeValue>
            </saml2:Attribute>
        </saml2:AttributeStatement>
    </saml2:Assertion>
</saml2p:Response>

Highlighted parts are:
producer                  - selected application
http://ga.com              - Issuer identifier
nameid-format:persistent - NameId required type
5555-5555-5               - user ID used for authentication
```

Links

1. SAML overview http://wiki.oasis-open.org/security/Saml2TechOverview

2. SAML spec http://saml.xml.org

3. OpenSAML library https://wiki.shibboleth.net/confluence/display/OpenSAML/Home