ID プロバイダーの SAML SSO の要件

ID プロバイダーの要件

このセクションでは、シスコ コラボレーション アプリケーションに SAML SSO サービスを導入するためにアイデンティティ プロバイダーが満たす必要がある要件の概要を示します。

ID プロバイダーは、次のガイドラインに従う必要があります。

- サポートは SAML 2.0 のみです。
- サービスプロバイダーが開始した SSO のみをサポートします。
- NameID Format 属性を *urn:oasis:names:tc:SAML:2.0:nameid-format:transient* に設定します。
- LDAP 属性にマッピングされた値（SAMAccountName など）に *uid* 属性名を含めるように、IdP で要求を設定します。
- Cisco Unified Communications Manager は、認証要求で ACS URL インデックスを使用します。IdP は、サービスプロバイダーのメタデータで ACS URL へのインデックスを作成できる必要があります。これは SAML 標準に準拠しています。
- SAML アサーションの署名と暗号化の部分で複数の証明書を使用することはサポートされていません。 CSCvq78479を参照してください。

SAML SSO を設定する場合は、Cisco Collaboration Deployment に以下を展開してください。

- Network Time Protocol：Cisco Collaboration Deployment と ID プロバイダーの時刻が同期されるように、NTP を環境に展開します。IdP とシスコ コラボレーション展開の時間差が 3 秒を超えないようにしてください。

- DNS：シスコ コラボレーション アプリケーションと ID プロバイダーは、互いのアドレスを解決できる必要があります。
- [LDAP]：Cisco Collaboration 展開で LDAP ディレクトリ同期を設定する必要があります。ただし、LDAP 認証を無効にすることを推奨します。
- 証明書：シスコ コラボレーション展開と ID プロバイダーの間でメタデータ ファイルを交換する必要があります。メタデータには、コラボレーション展開と ID プロバイダー間の信頼関係を作成するために必要な証明書が含まれています。Tomcat 証明書またはシステム生成の自己署名証明書を使用して、信頼を確立できます。

SAML 契約タイプ

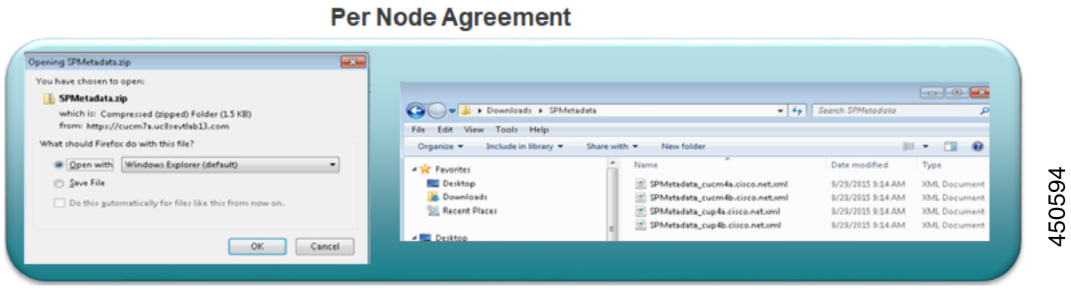
Cisco Unified Communications Manager は、次の 2 種類の SAML メタデータ契約をサポートしています。

- クラスタ全体：この展開では、クラスタ全体をカバーする単一のメタデータ契約を設定する必要があります。
- [ノードごと（Per Node）]：この展開では、クラスタノードごとに個別の契約を使用して、複数のメタデータ契約を設定する必要があります。各クラスタノードには、ID プロバイダーとの個別のメタデータ交換があります。

図 *1 : Cisco Unified Communications Manger* の *2* 種類の *SAML* メタデータ契約

次の図は、ノードごとの契約を使用して Cisco Unified Communications Manager で生成されたメタデータ zip ファイルの内容を示しています。この例では、IM and Presence Service は標準展開（非集中型）を使用して展開されるため、zip ファイルには、Unified Communications Manager および IM and Presence Service クラスタノードごとに個別のメタデータ xml ファイルが含まれています。

図 *2 : Cisco Unified Communications Manger* からダウンロードした *UC* メタデータファイル

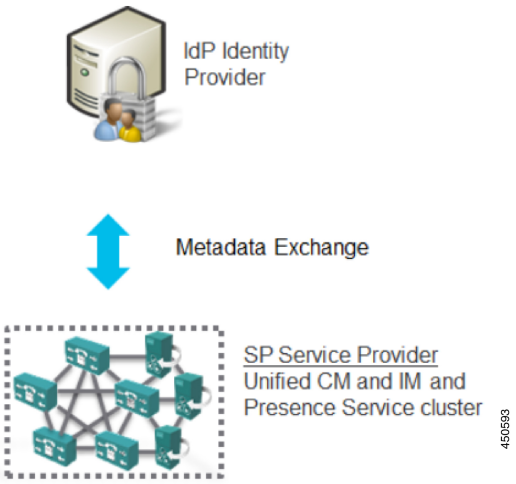


（注） IM and Presence Service の集中配置を使用している場合、IM and Presence 配置はテレフォニークラスタとは別のクラスタにあります。クラスタ全体の契約では、テレフォニークラスタと IM and Presence クラスタのメタデータを個別に生成する必要があります。

メタデータ交換

SAML SSO を設定するプロセスの一環として、UC 展開と ID プロバイダーの間でメタデータファイルを交換する必要があります。

図 *3 : SAML* メタデータ交換



次に、サービス プロバイダー（Cisco Unified Communications Manager）から生成された UC メタデータ ファイルの例を示します。

Cisco Unified Communications Manager からの IdP メタデータファイルのエクスポート

```
<?xml version="1.0" encoding="UTF-8"?>
<!--With Single Cluster agreement the entityID is always the publisher FQDN-->
<md:EntityDescriptor xmlns:md="urn:oasis:names:tc:SAML:2.0:metadata"
ID="cucm0a.identitylab20.ciscolabs.com" entity ID="cucm0a.identitylab20.ciscolabs.com">
    <!--We don't require AuthN or signed Assertions but comply to what the IdP requests-->

     <md:SPSSODescriptor AuthnRequestsSigned="false" WantAssertionsSigned="false"
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>MIIDzzCCA........</ds:X509Certificate>
     </ds:X509Data>
   </ds:KeyInfo>
  </md:KeyDescriptor>
   <!--Certificate for Signing and/or Encryption-->
  <md:KeyDescriptor use="encryption">
    <ds:KeyInfo xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
      <ds:X509Data>
        <ds:X509Certificate>MIIDzzCCA........</ds:X509Certificate>
      </ds:X509Data>
    </ds:KeyInfo>
  </md:KeyDescriptor>
   <!--We only support name-id format transient-->
  <md:NameIDFormat>urn:oasis:names:tc:SAML:2.0:nameid-format:transient</md:NameIDFormat>

         <!--ACS URL for the Client to POST the answer from the IdP, two per node in
the cluster-->
   <md:AssertionConsumerService Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST"

Location="https://cucm0a.identitylab20.ciscolabs.com:8443/ssosp/saml/SSO/alias/cucm0a.identitylab20.ciscolabs.com"
 index="0"/>
              <md:AssertionConsumerService
Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-Redirect"
Location="https://cucm0a.identitylab20.ciscolabs.com:8443/ssosp/saml/SSO/alias/cucm0a.identitylab20.ciscolabs.com"
 index="1"/>
     </md:SPSSODescriptor>
</md:EntityDescriptor>
```

次に、IDプロバイダー（Active Directoryフェデレーション サービス）から生成されたメタデータ ファイルの例を示します。

ID プロバイダーからのメタデータファイル（Active Directoryフェデレーションサービス）

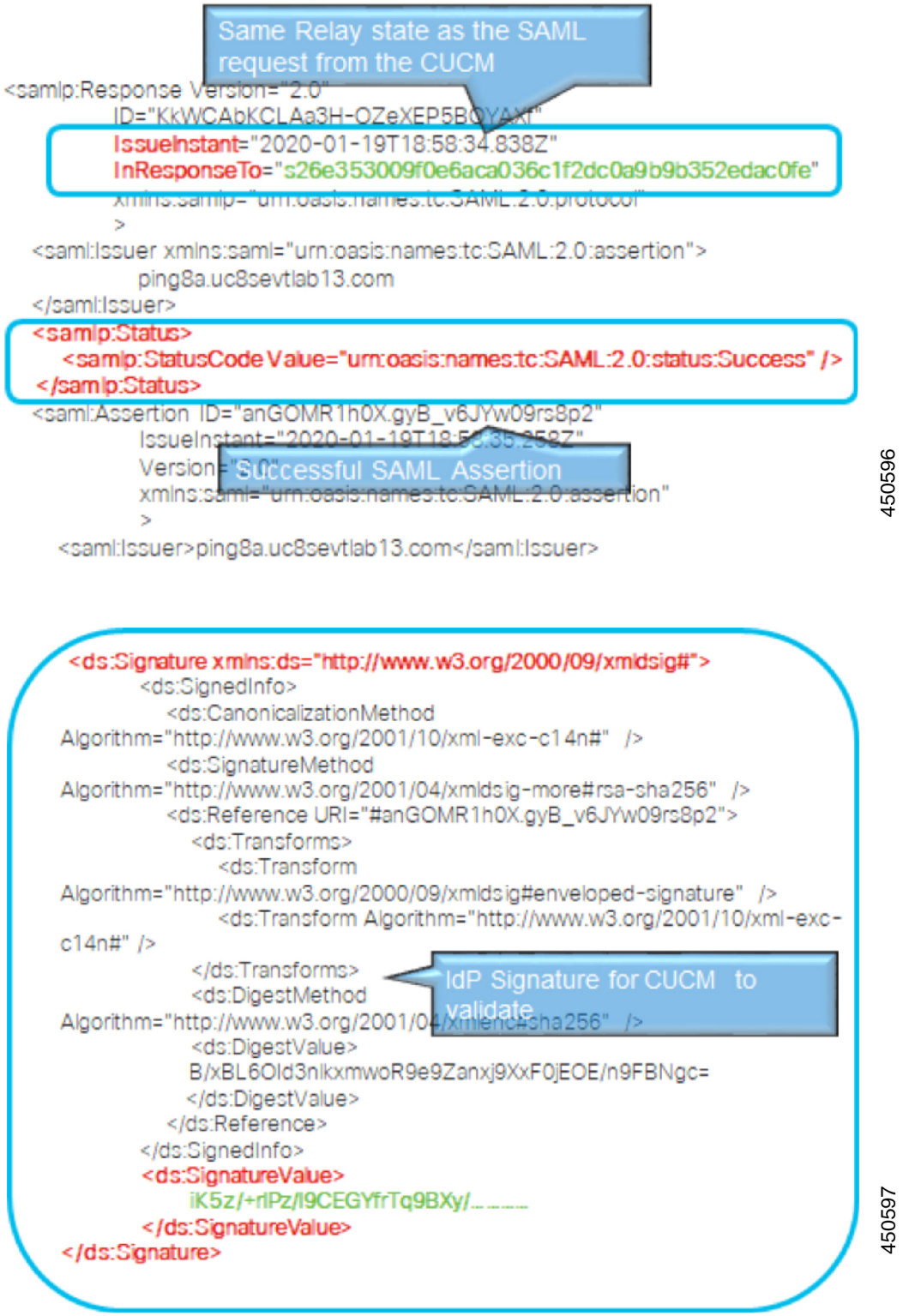
```
<?xml version="1.0"?
<!--entityID=IdP Entity ID-->
<EntityDescriptor xmlns="urn:oasis:names:tc:SAML:2.0:metadata"
ID="_b12fe1b5-6866-40cc-94be-9d9d8cb71916"
   entityID="http://WIN-2019SSO.cisco-dod.com/adfs/services/trust">
 <ds:Signature xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
   <ds:SignedInfo>
     <ds:CanonicalizationMethod Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#"/>
      <ds:SignatureMethod Algorithm="http://www.w3.org/2001/04/xmldsig-more#rsa-sha256"/>

    <ds:Reference URI="#_b12fe1b5-6866-40cc-94be-9d9d8cb71916">
                  <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>
      <!--Sign the metadata provided to the SP for extra security-->
```

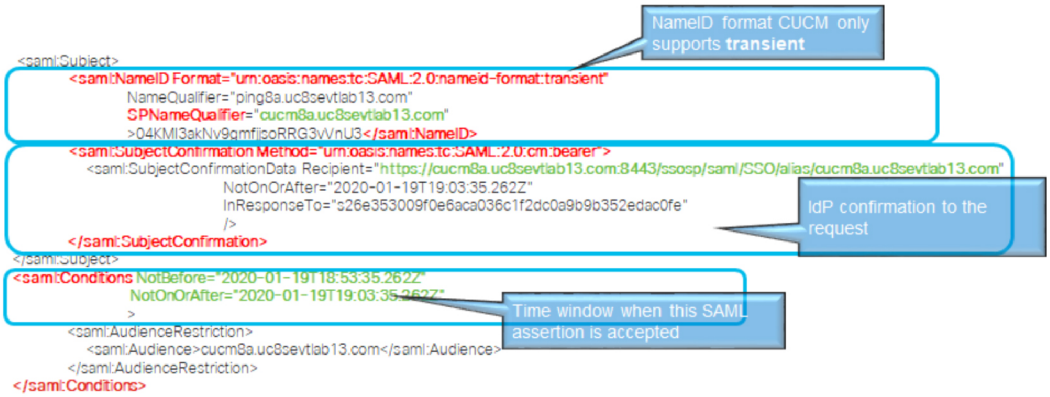
```
      <ds:DigestMethod Algorithm="http://www.w3.org/2001/04/xmlenc#sha256"/>
      <ds:DigestValue>VAcIv2uw6zG8YVVWP0IDYMZ/e7CN9o4oR8XBGiysujY=</ds:DigestValue>
    </ds:Reference>
   </ds:SignedInfo>
   <ds:SignatureValue>44RAgZ17YfwLdcRodZPcZ5PH05sLVbkDx4uAYq+EC4K+ZhiTs8aUZQ/.........
   </ds:SignatureValue>
   <KeyInfo xmlns="http://www.w3.org/2000/09/xmldsig#">
  <X509Data>
   <IDPSSODescriptor
protocolSupportEnumeration="http://docs.oasis-open.org/ws-sx/ws-trust/200512
http://schemas.xmlsoap.org/ws/2005/02/trust
http://docs.oasis-open.org/wsfed/federation/200706"
ServiceDisplayName="administrator.cisco-dod.com">
 <KeyDescriptor use="encryption">
   <KeyInfo xmlns="http://www.w3.org/2000/09/xmldsig#">
     <X509Data>
  <X509Certificate>MIIGHzCCBQegAwIBAgITHAAADUerWbVHyqoM.........
  </X509Certificate>
     </X509Data>
   </KeyInfo>
 </KeyDescriptor>
 <KeyDescriptor use="signing">
   <KeyInfo xmlns="http://www.w3.org/2000/09/xmldsig#">
     <X509Data>
         <!--Cert for signing and/or encrypting the SAML Assertion-->
  <X509Certificate>MIIC7jCCAdagAwIBAgIQJH7di/.........</ds:X509Certificate>
    </KeyInfo>
 </KeyDescriptor>
   <!--Single Sign On Service details for HTTP-Redirect and HTTP-POST-->
   <SingleSignOnService Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-Redirect"
Location="https://win-2019sso.cisco-dod.com/adfs/ls/"/
   <SingleSignOnService Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST"
Location="https://win-2019sso.cisco-dod.com/adfs/ls/"/>
   <!--NameID format offer for this agreement-->
   <NameIDFormat>urn:oasis:names:tc:SAML:1.1:nameid-format:emailAddress</NameIDFormat>
   <NameIDFormat>urn:oasis:names:tc:SAML:2.0:nameid-format:persistent</NameIDFormat>
   <NameIDFormat>urn:oasis:names:tc:SAML:2.0:nameid-format:transient</NameIDFormat>
   <AssertionConsumerService Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST"
Location="https://win-2019sso.cisco-dod.com/adfs/ls/" index="0" isDefault="true"/>
  <AssertionConsumerService Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-Artifact"
 Location="https://win-2019sso.cisco-dod.com/adfs/ls/" index="1"/>
  <AssertionConsumerService Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-Redirect"
 Location="https://win-2019sso.cisco-dod.com/adfs/ls/" index="2"/>
   </IDPSSODescriptor>
</EntityDescriptor>
```

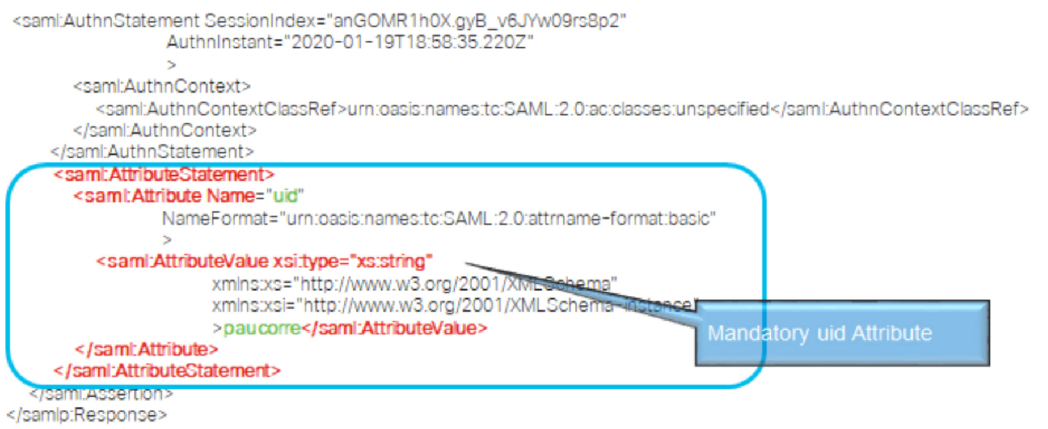
SAML アサーション

次に、ID プロバイダーから Cisco Unified Communications Manager に送信される SAML アサーションの例を示します。

図 *4 : SAML* アサーションの例



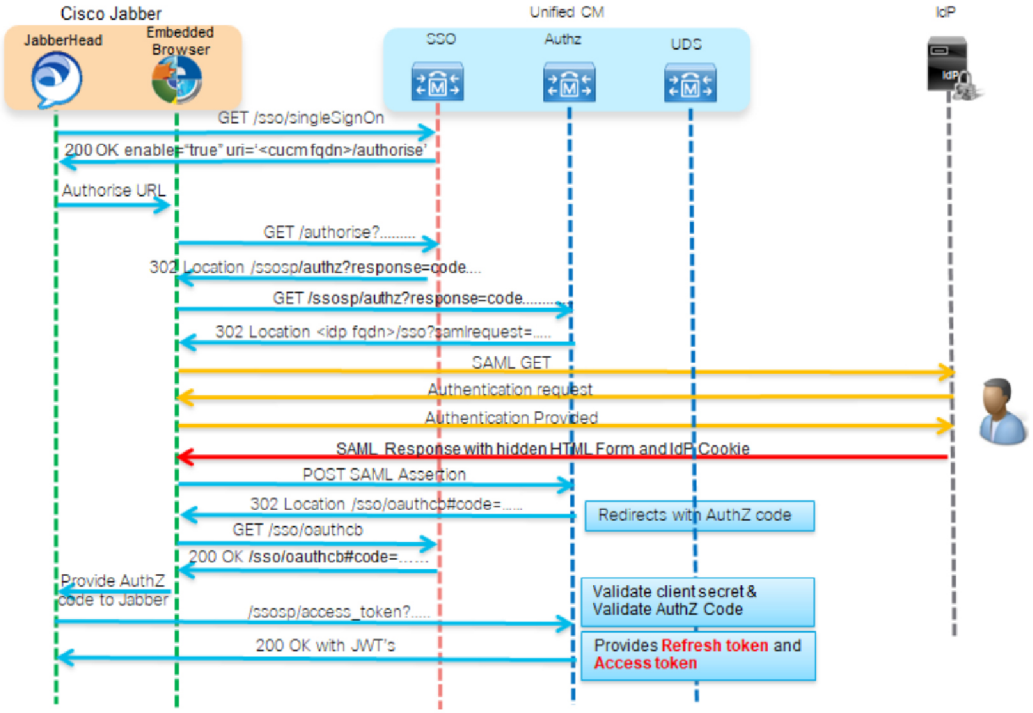




SAML OAuth 認証フロー

次に、ID プロバイダーを使用した OAuth 認証要求の認証フローの例を示します。

図 *5 : SAML OAuth* 認証フロー



翻訳について
このドキュメントは、米国シスコ発行ドキュメントの参考和訳です。リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動/変更されている場合がありますことをご了承ください。あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。