TRIDIUM

NS2022

ACCELERATING INNOVATION

TRIDIUM

Single Sign On – Making Enterprise Systems Easy to Access

James Johnson - Tridium

Objectives

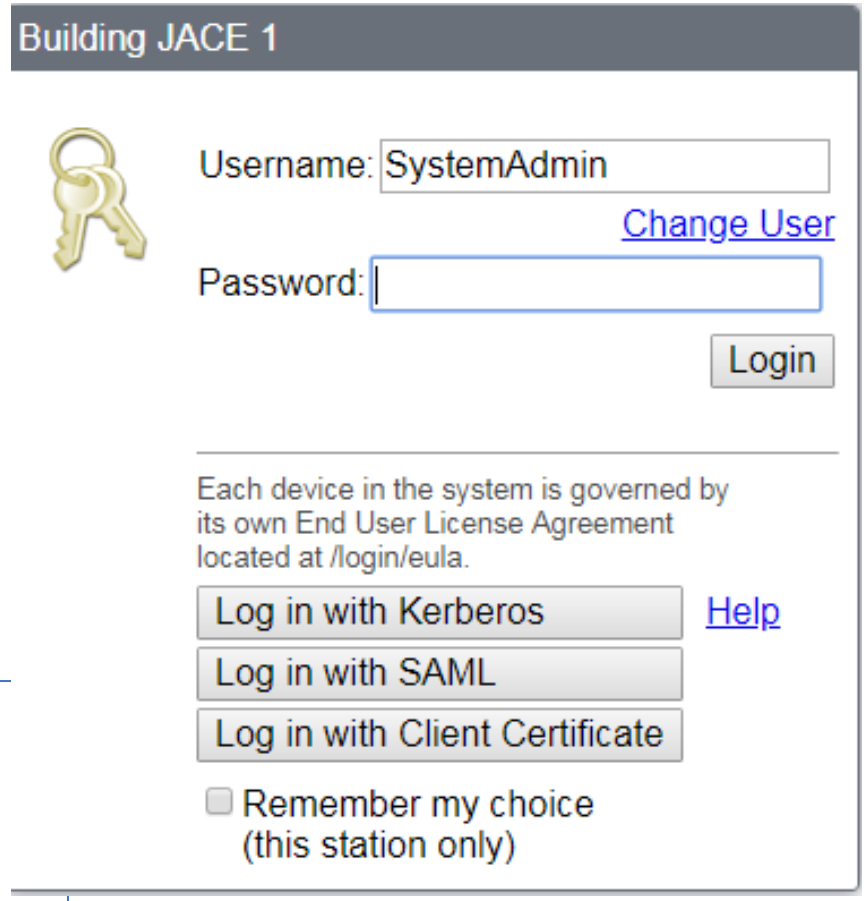
- Single Sign On (SSO)
- LDAP and Kerberos
- SAML
- Client Certificate Authentication
- Browser Based Kiosk Support

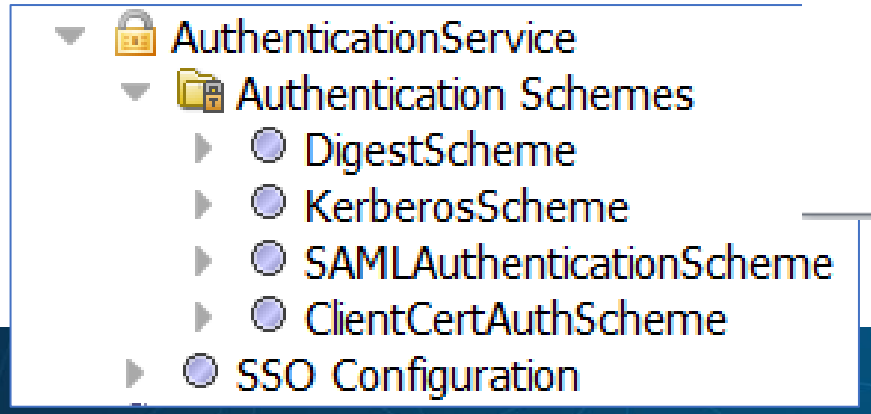
Single Sign On (SSO)

- A property of access control which allows a user to login with a single ID and password to gain access to multiple related applications or servers.
- Mitigates risk for access to third party systems since user passwords are not stored or managed externally.
- Reduces password fatigue.
- Reduces time spent re-entering passwords for the same identity.

Niagara 4 SSO Authentication Schemes

- ldap Palette
  - Lightweight Directory Access Protocol
  - Kerberos
- saml Palette
  - Security Assertion Markup Language
- clientCertAuth Palette
  - PKI Certificate

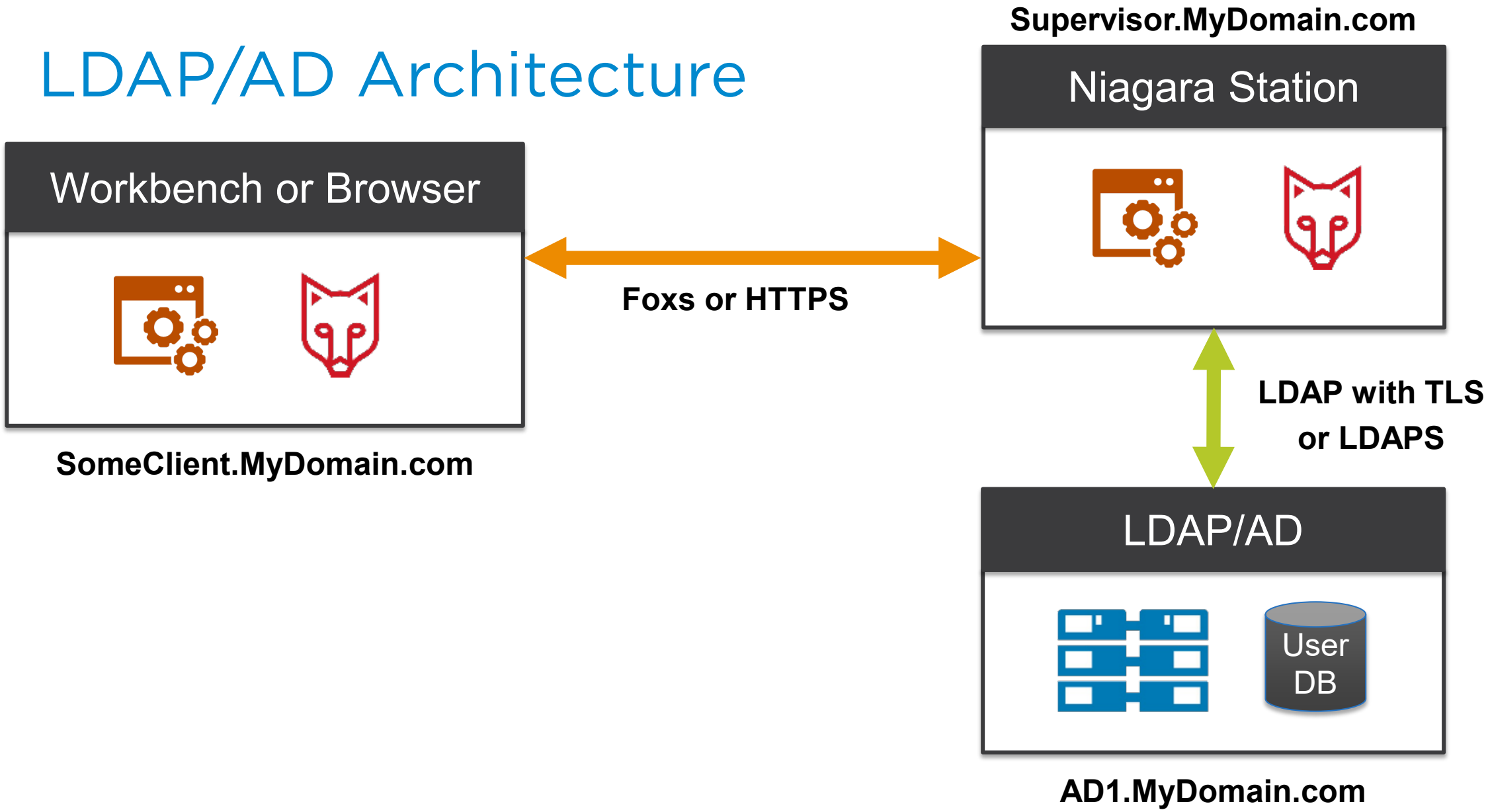




LDAP/AD Authentication

- **Lightweight Directory Access Protocol (LDAP)** is an application protocol for accessing and maintaining distributed directory information services over an IP network.
- **Active Directory (AD)** is a Microsoft specific implementation of an LDAP server.
- **LDAP** is commonly used on corporate networks for managing domain user accounts and the user's access to applications and network resources.
- Provides **single login credentials** but not SSO.

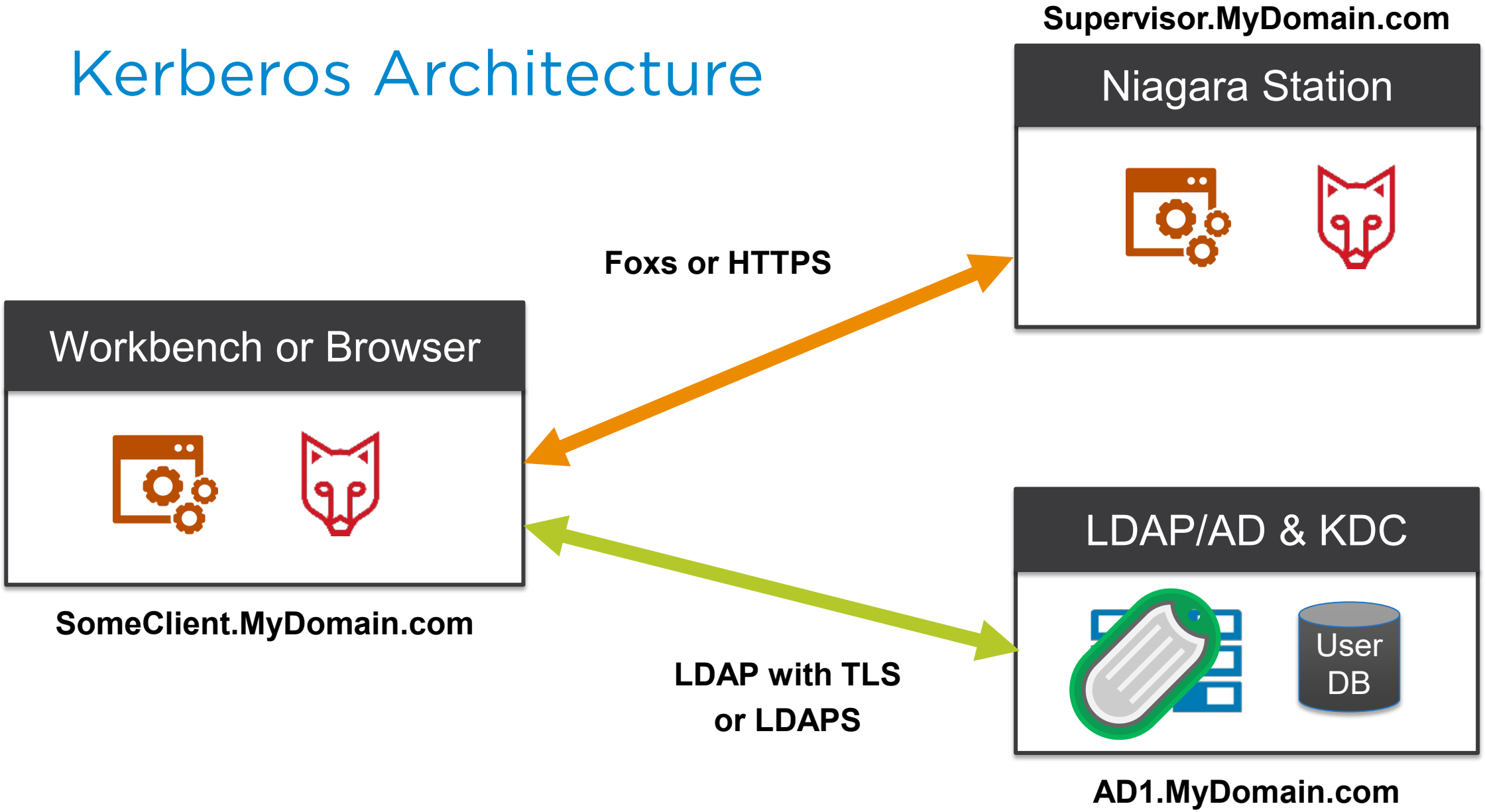
LDAP/AD Architecture



Kerberos

- An open-source computer network authentication protocol that uses **tickets to verify identity of users** to control access to network resources.
- Clients **retrieve tickets** from a **Key Distribution Center** (KDC).
- Setup using **Kerberos Scheme** from ldap palette.
- Requires **configuring key tab** file.
- Requires **configuring the client browser**.

Kerberos Architecture



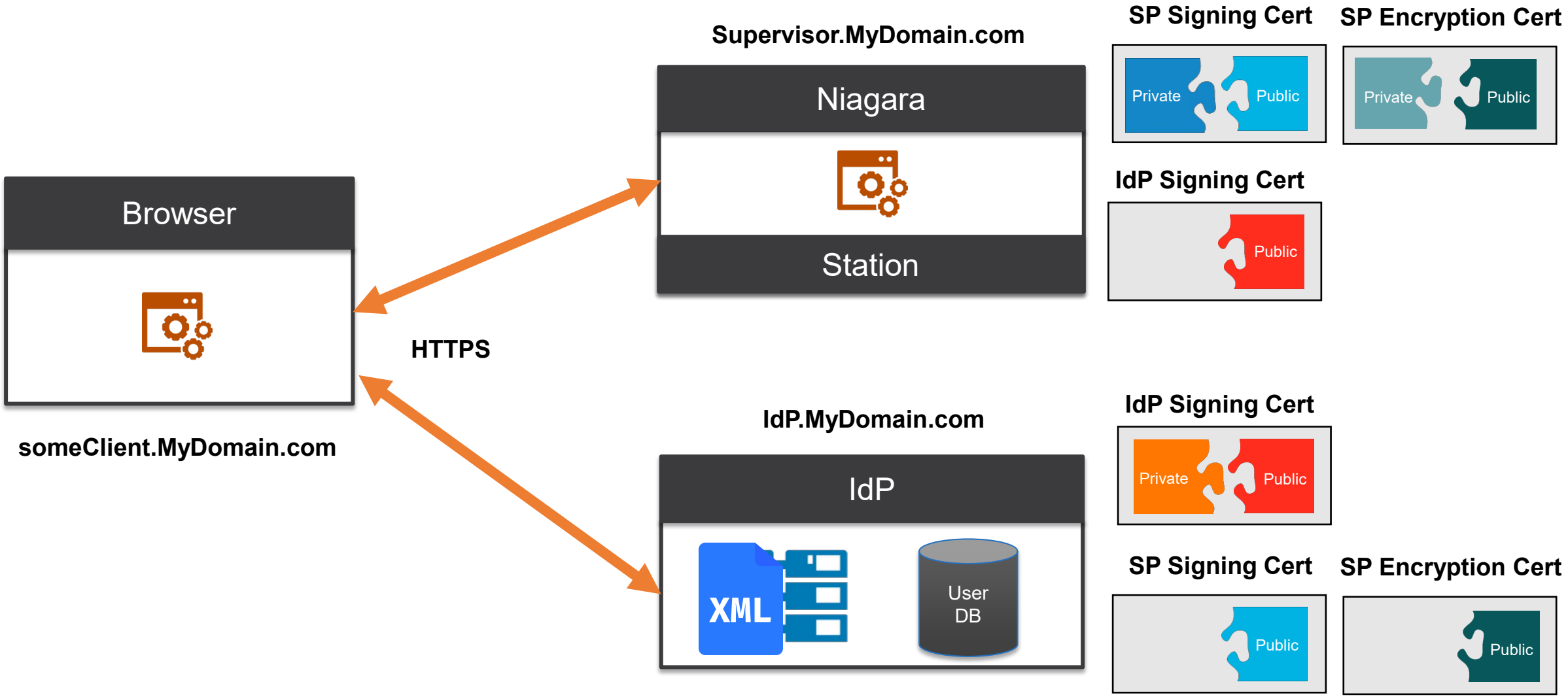
Security Assertion Markup Language (SAML)

- An open standard for exchanging **authentication and authorization data** in the form of **messages** passed between security domains.
- Messages **may be encrypted** and are **typically signed** using a PKI certificate.
- Since **Niagara 4.4 version, SAML 2.0** is supported.
- Works with popular third party **on premise and cloud based SAML Identity Providers** such as OpenAM, Salesforce, Active Directory, etc.
- Since **Niagara 4.9** version, a **Niagara based SAML Idp Service** is supported in place of third party IdP.

Important Terms

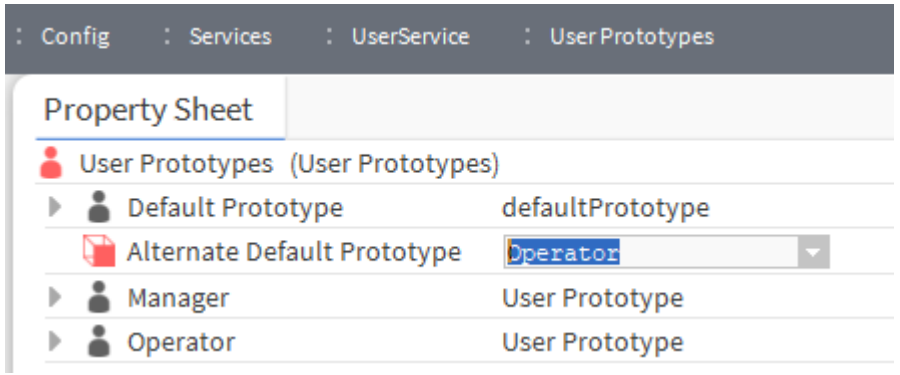
- **Assertion** – a package of information (XML) that supplies statements made by a SAML authority.
- **Attribute** – a piece of information which determines the properties of a field or tag in a database.
- **Identity Provider (IdP)** – a system entity that issues authentication assertions.
- **Service Provider (SP)** – a system entity that receives and accepts authentication assertions.

SAML Architecture



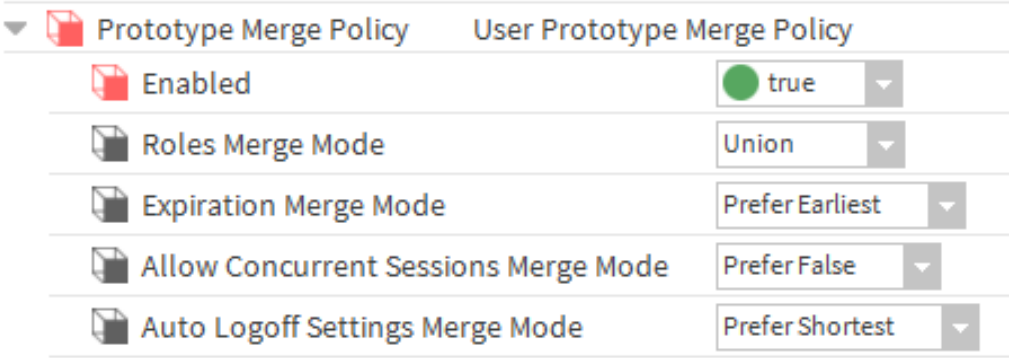
SAML User Prototypes

- The **defaultPrototype** is a **baja:User** component used with Niagara user synchronization and legacy LDAP/AD authentication.
- **LDAP, AD** and **SAML** authentication utilize a newer **baja:UserPrototype** component found in the baja, ldap and saml palettes.
- **Alternate Default Prototype** should be configured to select a baja:UserPrototype and is used if no matching prototype is detected.



Prototype Merge Policy (4.12)

- Available for SAML and LDAP authentication schemes.
- Configures merge behavior for properties when multiple prototype matches are detected.

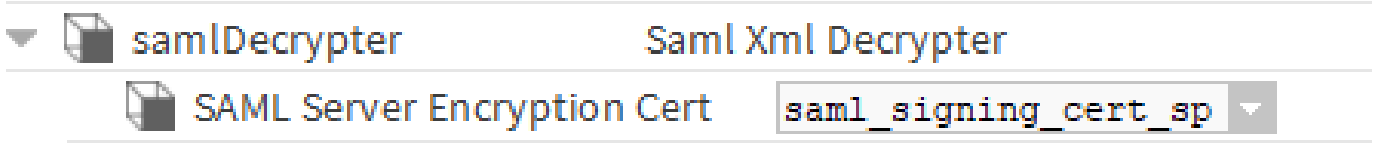


SAML Authentication Scheme

- **Entity ID** – URL to identify the station (SP) SAML services.
- **IdP Host URL –** redirect URL to IdP server.
- **IdP Login Path** – appended to IdP Host URL to specify the IdP login page URL.
- **Idp Cert** – certificate provided by the IdP admin which must be in the station's trust store. Used to validate messages signed by and received from the IdP.
- **SAML Server Cert** – certificate in the station's key store which must be provided to the IdP admin. Used to sign messages sent to the IdP.

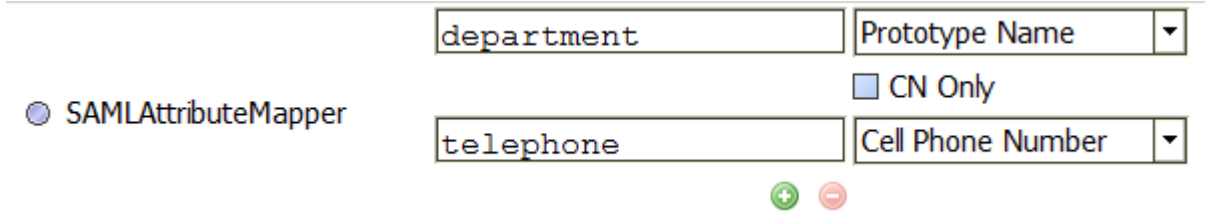
SAML Encrypted Assertions

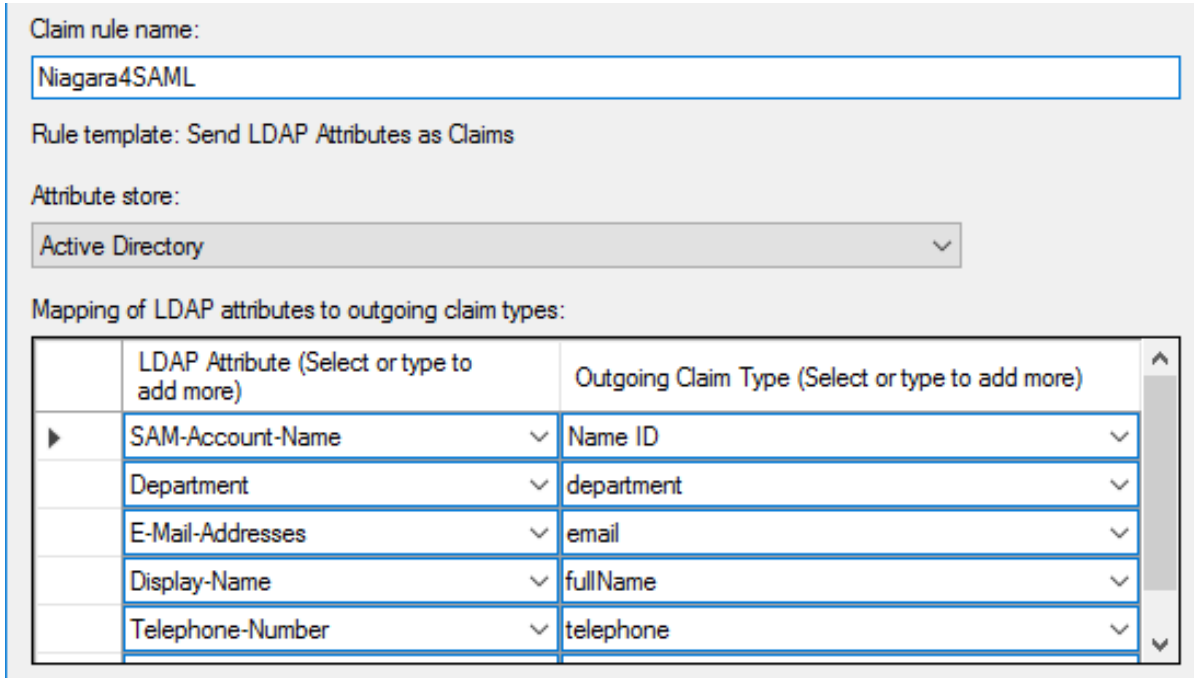
- Optional for IdP to encrypt assertions sent to SP.
- Must add SAML Xml Decrypter to SAML Authentication Scheme.
- IdP requires public key from specified certificate to encrypt assertions.
- Station (SP) requires the private key from specified certificate in its key store to decrypt received assertions.



SAML Attribute Mapper

- Defines attributes by name from the SAML assertion sent by IdP and maps the attribute values to properties on the Niagara user account.
- SAML DevTools extension in Chrome may be used to view claims response from IdP.





SAML Assertions

Request Response SAML


```
<samlp:Response
    ID="_06044e98-e293-471c-a904-3a3f727a3ee9"
    Version="2.0"
    IssueInstant="2019-08-01T19:54:46.456Z"
    Destination="https://jace25.training.lan/saml/assertionConsumerService"
    Consent="urn:oasis:names:tc:SAML:2.0:consent:unspecified"
    InResponseTo="_ae150362-f9d2-4981-be55-cdf7c9e679f1"
    xmlns:samlp="urn:oasis:names:tc:SAML:2.0:protocol">
    <Issuer
        xmlns="urn:oasis:names:tc:SAML:2.0:assertion">http://idp.training.lan/adfs/services/trust
    </Issuer>
    <samlp:Status>
        <samlp:StatusCode
            Value="urn:oasis:names:tc:SAML:2.0:status:Success" />
    </samlp:Status>
    <Assertion
        ID="_acccf060-40f6-4fd8-8504-13ef076c6559"
        IssueInstant="2019-08-01T19:54:46.425Z"
        Version="2.0"
        xmlns="urn:oasis:names:tc:SAML:2.0:assertion">
        <Issuer>http://idp.training.lan/adfs/services/trust</Issuer>
        <ds:Signature
```



```
<AttributeStatement>
    <Attribute
        Name="department">
        <AttributeValue>NiagaraOperators</AttributeValue>
    </Attribute>
    <Attribute
        Name="email">
        <AttributeValue>pjfry@planetexpress.com</AttributeValue>
    </Attribute>
    <Attribute
        Name="fullName">
        <AttributeValue>Phillip J. Fry</AttributeValue>
    </Attribute>
    <Attribute
        Name="telephone">
        <AttributeValue>804-555-1212</AttributeValue>
    </Attribute>
</AttributeStatement>
```


- Browser extensions or SAML log are useful to debug.
- View attribute key names and values in assertion.

SAML Metadata URL (4.8)

- Simplifies IdP configuration by providing metadata via XML.
- https://<host>/saml/samlrp/metadata?scheme=<schemeName>

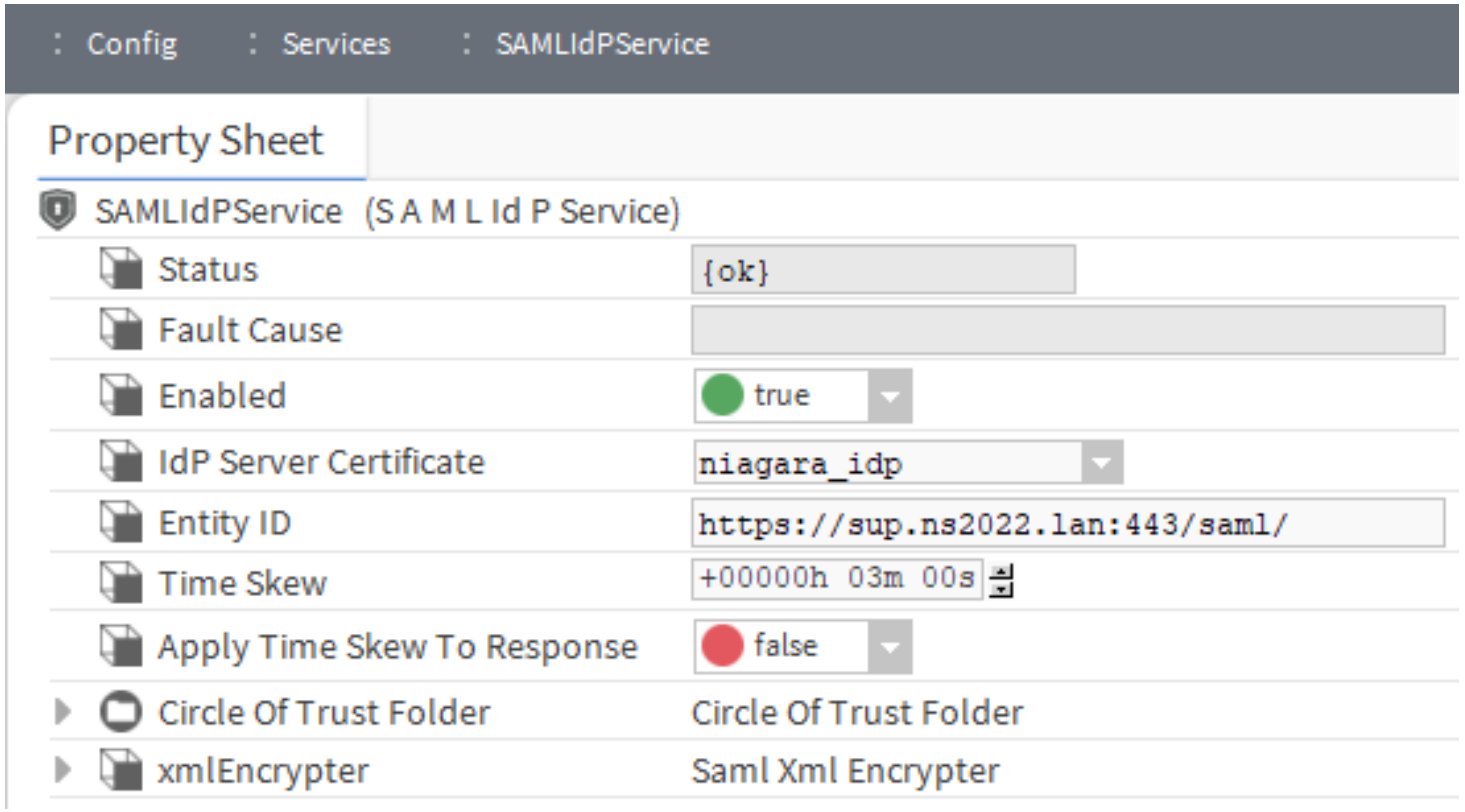
bldg1f1.ns2022.lan/saml/samlrp/metadata?scheme=NiagaraIdP_NS2022

This XML file does not appear to have any style information associated with it. The document tree is shown below.


```
▼<md:EntityDescriptor xmlns:md="urn:oasis:names:tc:SAML:2.0:metadata" validUntil="2024-03-18T18:51:41Z" cacheDuration="PT6048005" entityID="https://bldg1f1.ns2022.lan:443/saml/">
  ▼<md:SPSSODescriptor AuthnRequestsSigned="true" WantAssertionsSigned="true" 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>MIIEKzCCAxOgAwIBAgIMdtwHRF3zlB79i30gMA0GCSqGSIb3DQEBCwUAMH4xHTAbBgNVBAMMFHNhbWxfc2lnbmluZ19jZXJ0X3NwMRgwFgYDVQQLDA9UcmlkaXVtIFN1cHBvcnQxEDAOBgNVBAoMB
          </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>MIIEKzCCAxOgAwIBAgIMdtwHRF3zlB79i30gMA0GCSqGSIb3DQEBCwUAMH4xHTAbBgNVBAMMFHNhbWxfc2lnbmluZ19jZXJ0X3NwMRgwFgYDVQQLDA9UcmlkaXVtIFN1cHBvcnQxEDAOBgNVBAoMB
          </ds:X509Data>
        </ds:KeyInfo>
      </md:KeyDescriptor>
      <md:NameIDFormat>urn:oasis:names:tc:SAML:1.1:nameid-format:unspecified</md:NameIDFormat>
      <md:AssertionConsumerService Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST" Location="https://bldg1f1.ns2022.lan:443/saml/assertionConsumerService" index="1"/>
    </md:SPSSODescriptor>
  </md:EntityDescriptor>
```

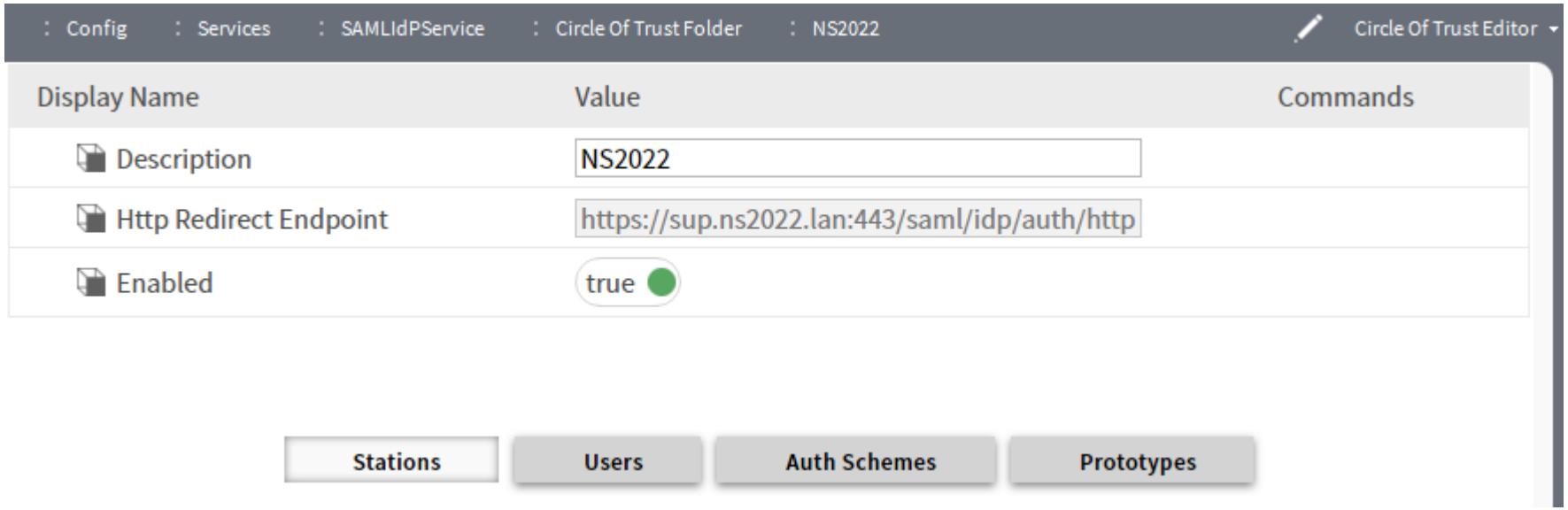
SAML Idp Service (4.9)

- Native Niagara based Identity Provider (IdP).
- Typically setup in the supervisor station.
- Requires samlDP feature in license.



Circle Of Trust (COT)

- Component which defines a group of stations to which designated users have access via SAML authentication.
- Each COT has its own HTTP Redirect Endpoint URL.
- Can define multiple COT components under the SAML IdP Service.



COT Editor

- **Stations** – configures which stations are included.
- **User** – configures which station users are included.
- **Auth Schemes** – configures authentication schemes such as LDAP where a local user may not exist to be assigned. Enabling an authentication scheme allows all users who log in with that scheme to utilize SAML SSO.
- **Prototypes** – defines place holder names for user prototypes used in the remote stations to assign role, nav file and other properties to users created via SAML authentication.

COT – SAML Prototypes

- Configures the user prototype for each COT.
- Only lists COT components which have the user enabled.
- Configured on user prototype for authentication schemes such as LDAP.

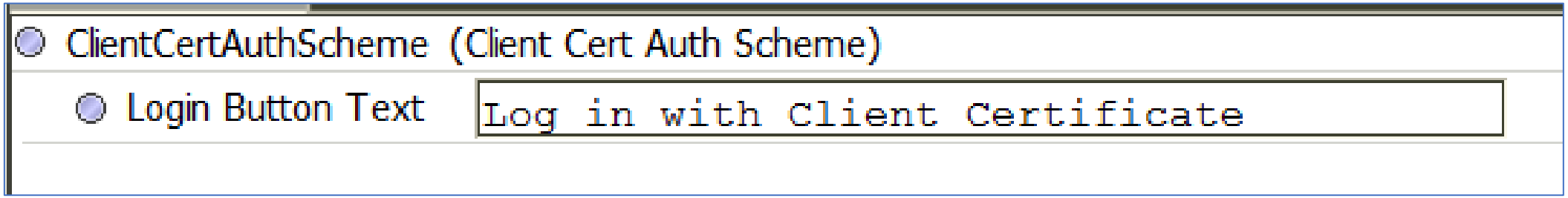
Default Web Profile	HTML5 Hx Profile
SAML Prototypes	SAML CoT Prototypes
NS2022	☑ Manager ☐ Operator
training	☑ MySweetPrototype
Mobile Web Profile	Default Hx Profile

Configure Niagara IdP and SAML Scheme

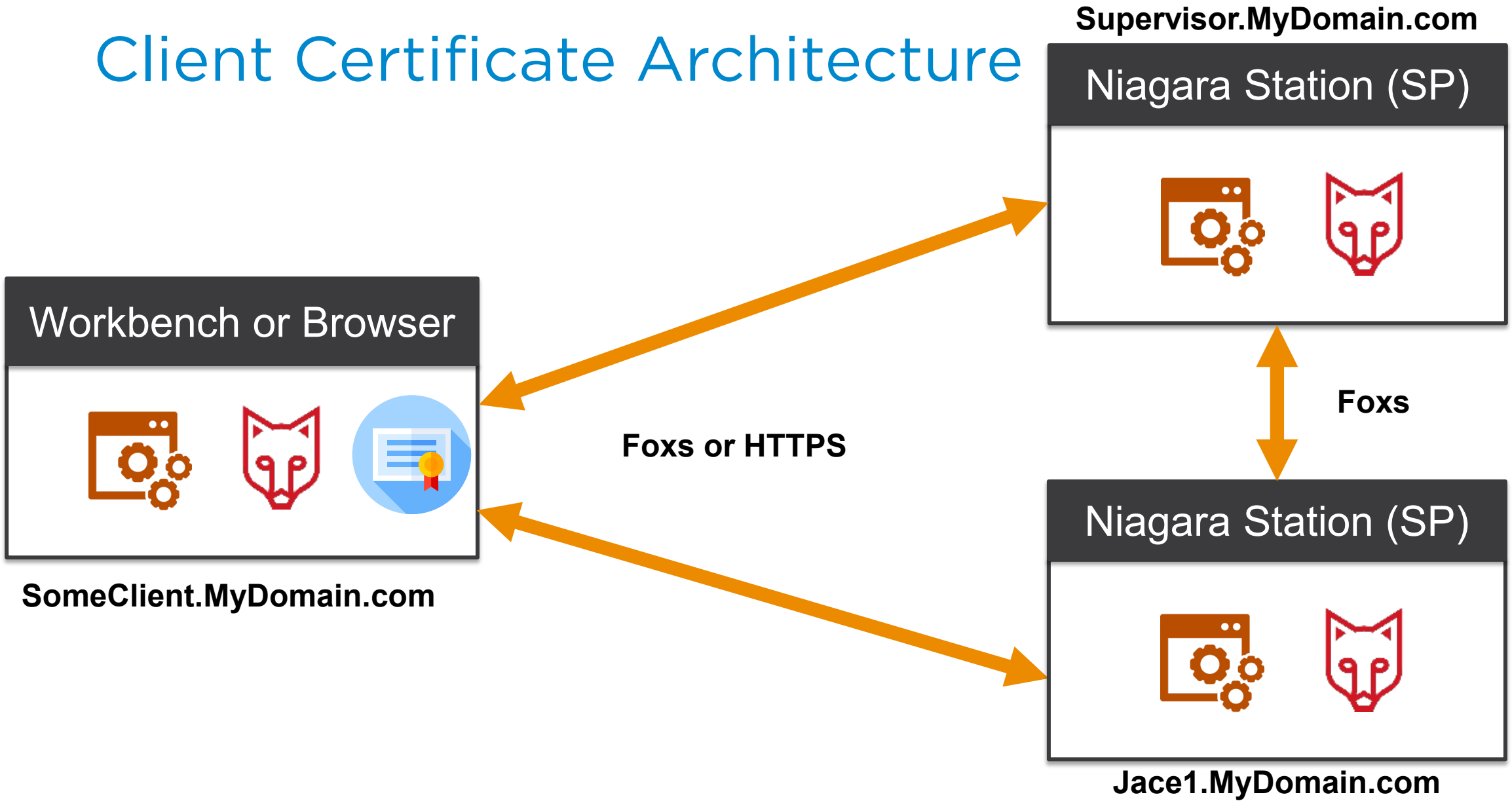
- Manually add/configure SAML Idp Service including COT and user's SAML prototypes.
- Either manually or using set property job step, setup user prototypes in remote stations.
- Use the provisioning job step to:
  - Add and configure the SAML Authentication Scheme to remote stations.
  - Import the public signing certificate from the supervisor to the trust store of each remote station.
  - Generate a unique certificate in the remote station's user key store to be used for signing/encrypting SAML messages.
  - Assign the remote station's certificate to the applicable station Service Provider (SP) under the COT in the supervisor.

Client Certificate Authentication (4.8)

- Provides authentication using PKI certificate instead of traditional username and password.
- Extended key usage must be TLS Web Client Authentication.
- User must export public key from their certificate and share with the Niagara system administrator.



Client Certificate Architecture



Kiosk Support – Client Authentication (4.8)

- Browser based kiosks can utilize certificates in the client's key store for station authentication.
- Station SSO configuration or client browser cookie may allow the browser client to automatically attempt certificate authentication.
- Browser client may be configured to automatically select a specific certificate for a given URL.

Summary

- Niagara 4 supports **SSO** through various authentication schemes such as LDAP/AD with **Kerberos, SAML** and **Client Certificate**.
- SSO mitigates risk for access to third party systems, reduces password fatigue and reduces time spent re-entering passwords for the same identity.
- **SAML** is an open standard for exchanging **authentication and authorization data** in the form of encrypted messages passed between security domains.
- Both on premise and cloud based IdPs are supported.
- Niagara specific user properties such as roles, nav files and web profiles are **configured with user prototypes**.
- Client certificate authentication in conjunction with SSO simplifies browser-based kiosk authentication.

Questions

NS2022
ACCELERATING INNOVATION

TRIDIUM