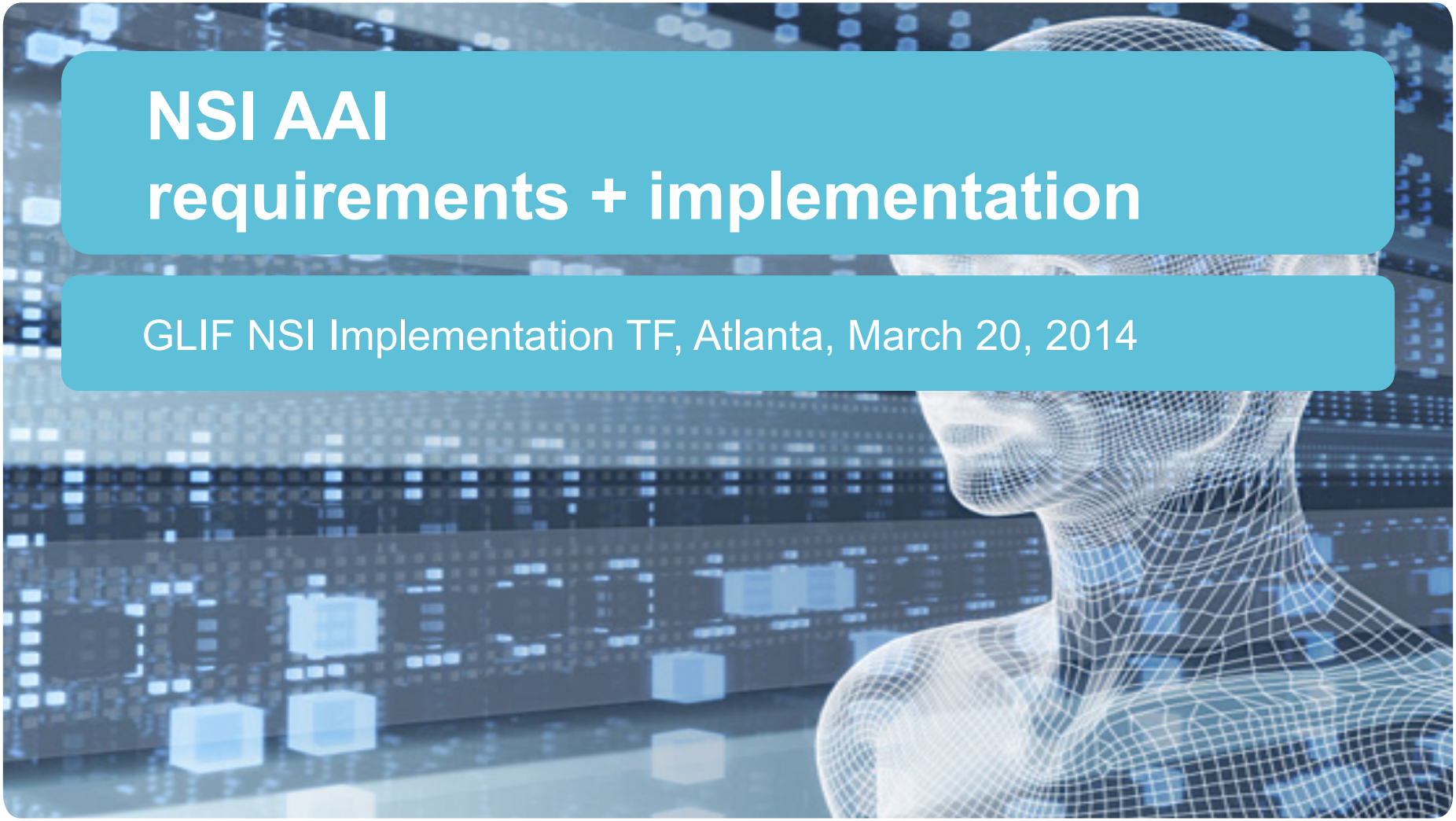


NSI AAI
requirements + implementation

GLIF NSI Implementation TF, Atlanta, March 20, 2014

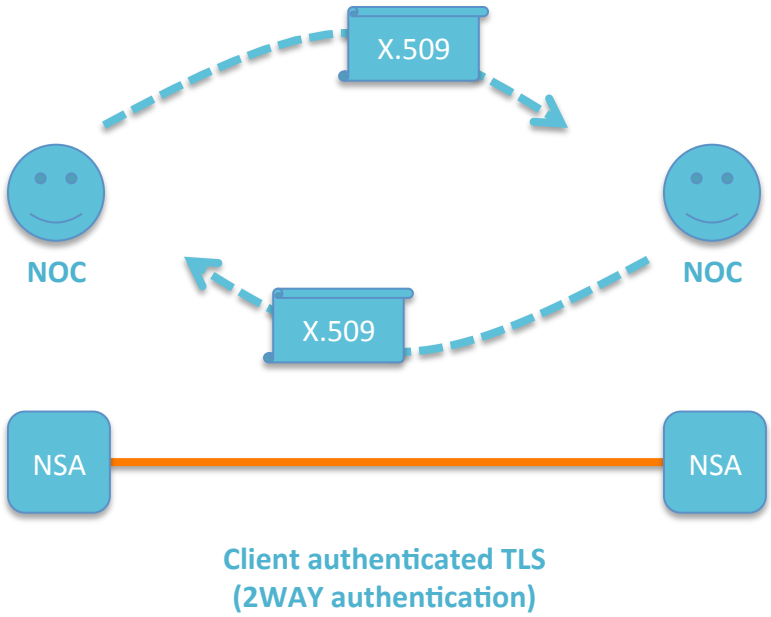
Hans Trompert
SURFnet

Starting points

- NSI is used to reserve valuable resources
- Only authenticated access to the control plane
- Users are already part of one or more existing AAIs
- Authorization of endpoints of end to end connection
- Inter domain peering model based on transitive trust
- Traceability of requesting user
- Policy on a per peer basis
- Extensible to do intermediate domain authorization

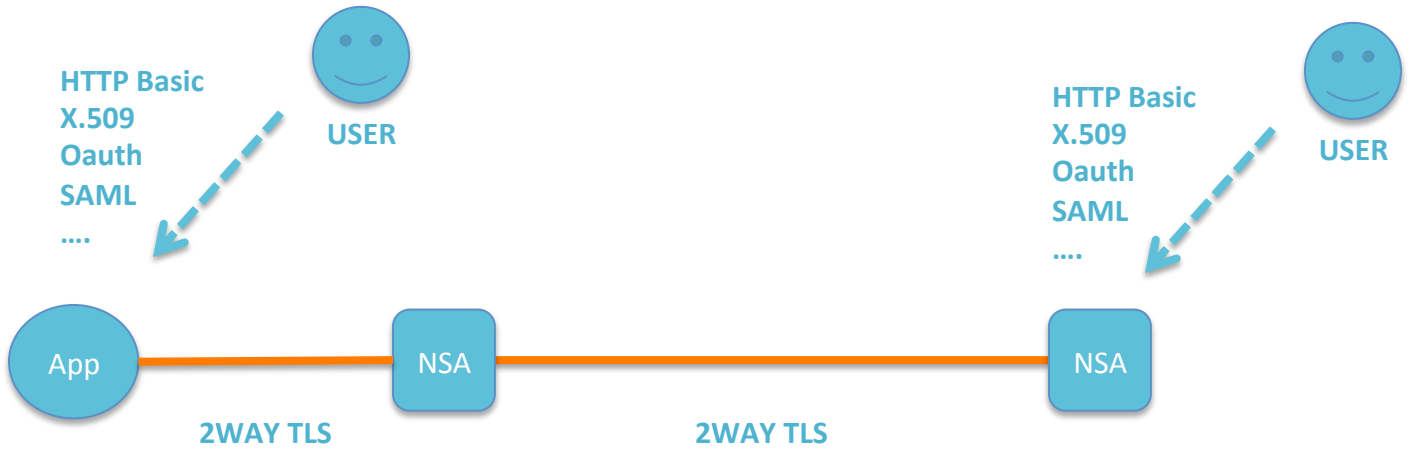
NSI control plane security

- Trusted Certificate Authority
- Trusted CA + exchange of ID
- Exchange of certificates

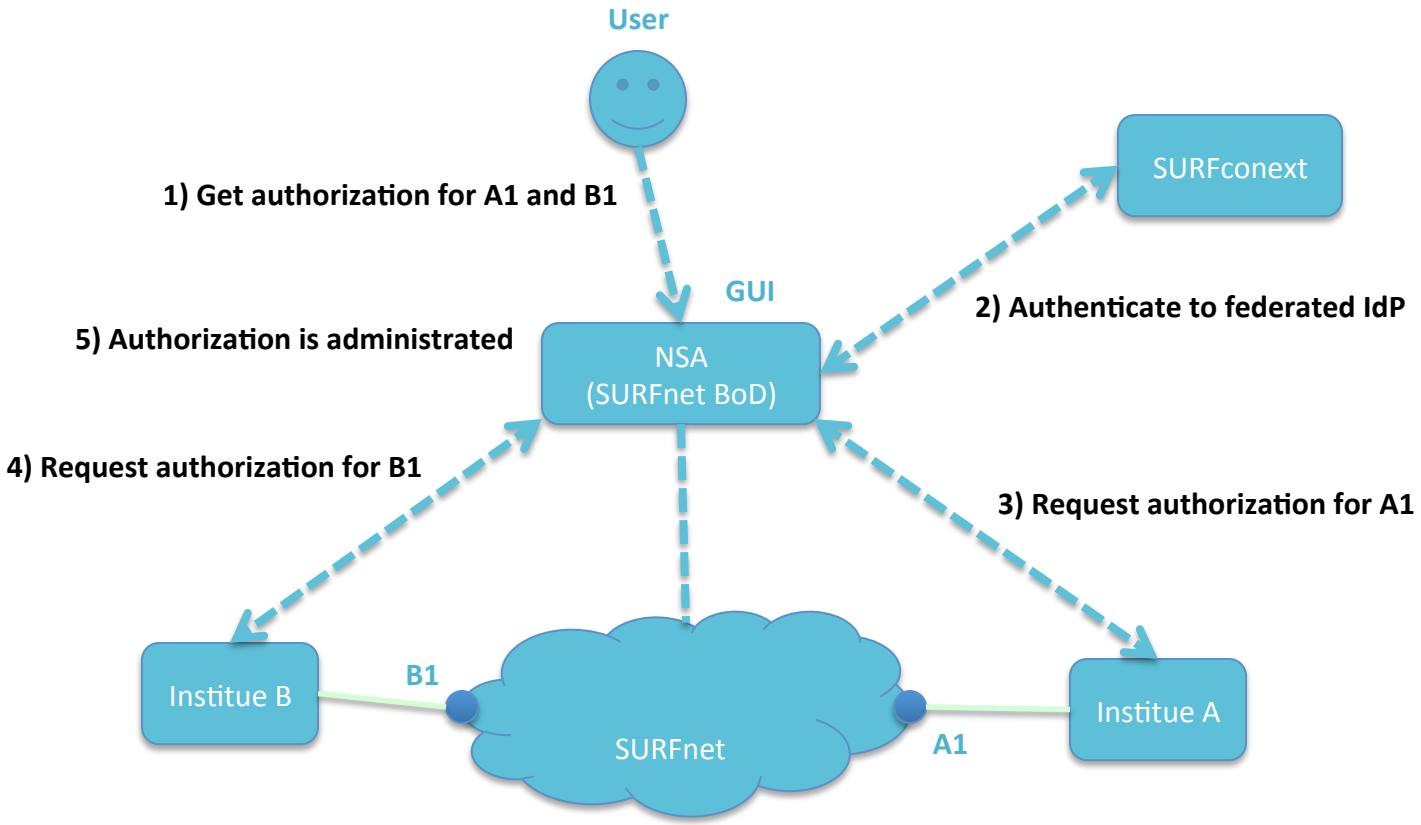


User authentication

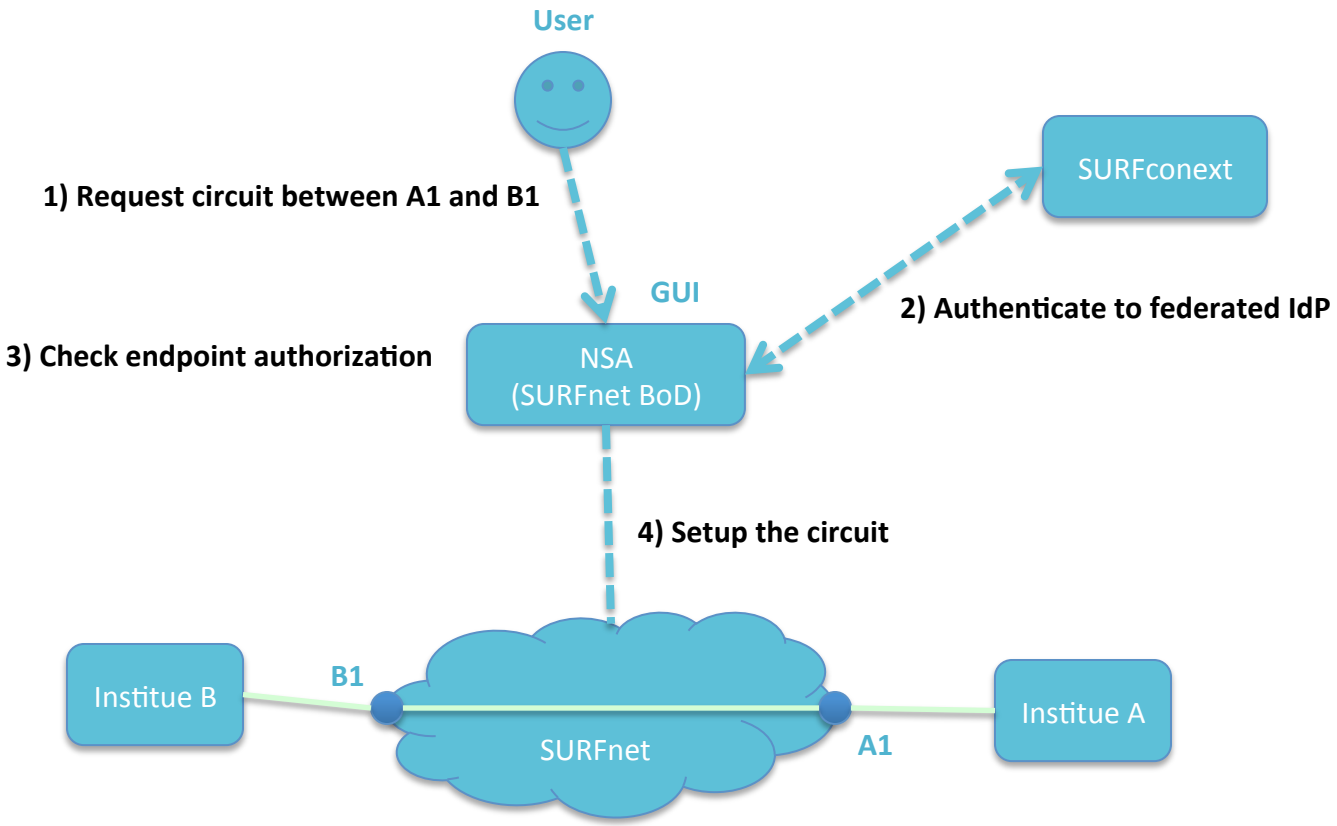
User access to control plane is authenticated



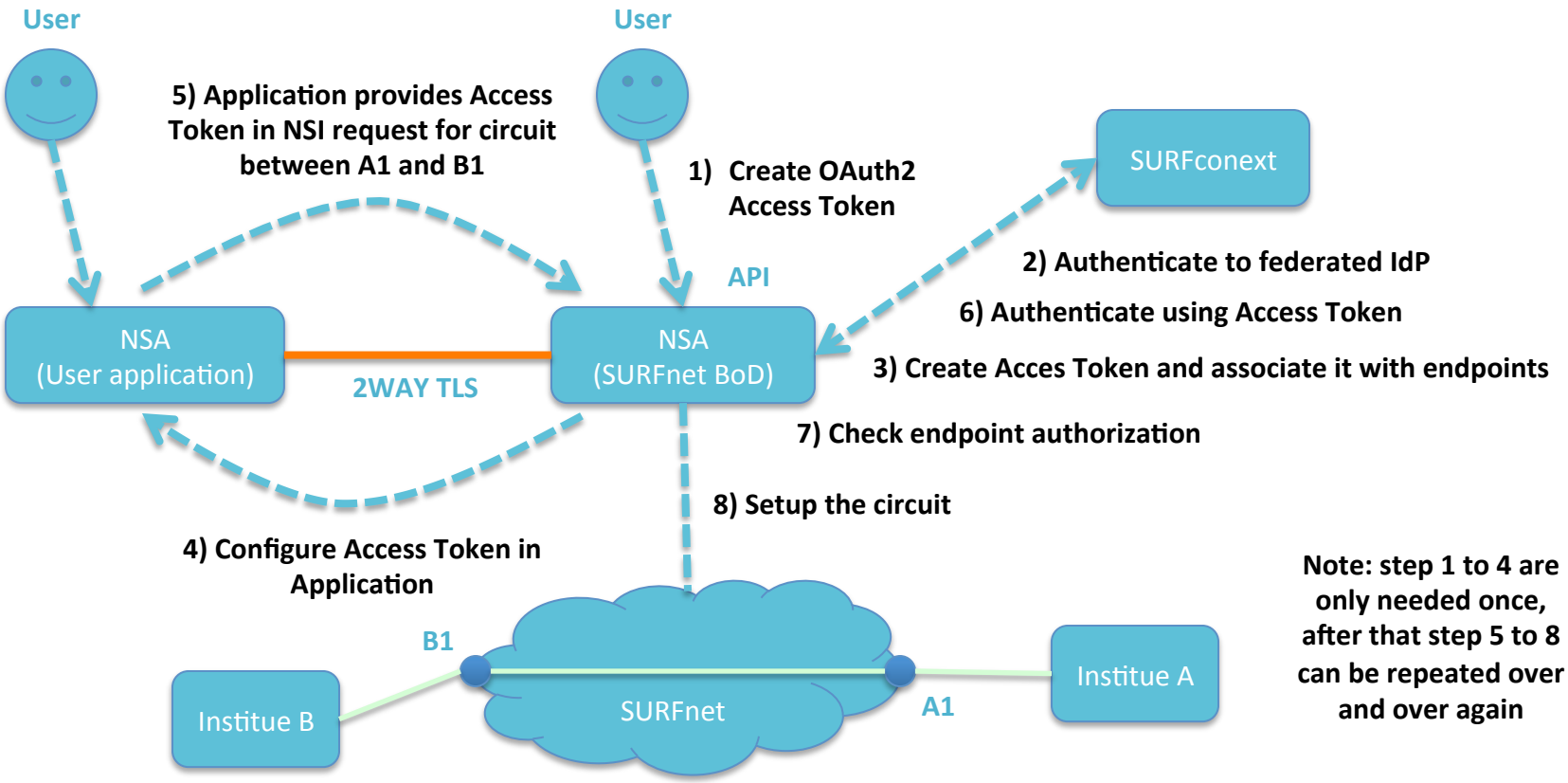
SURFnet: user authorization



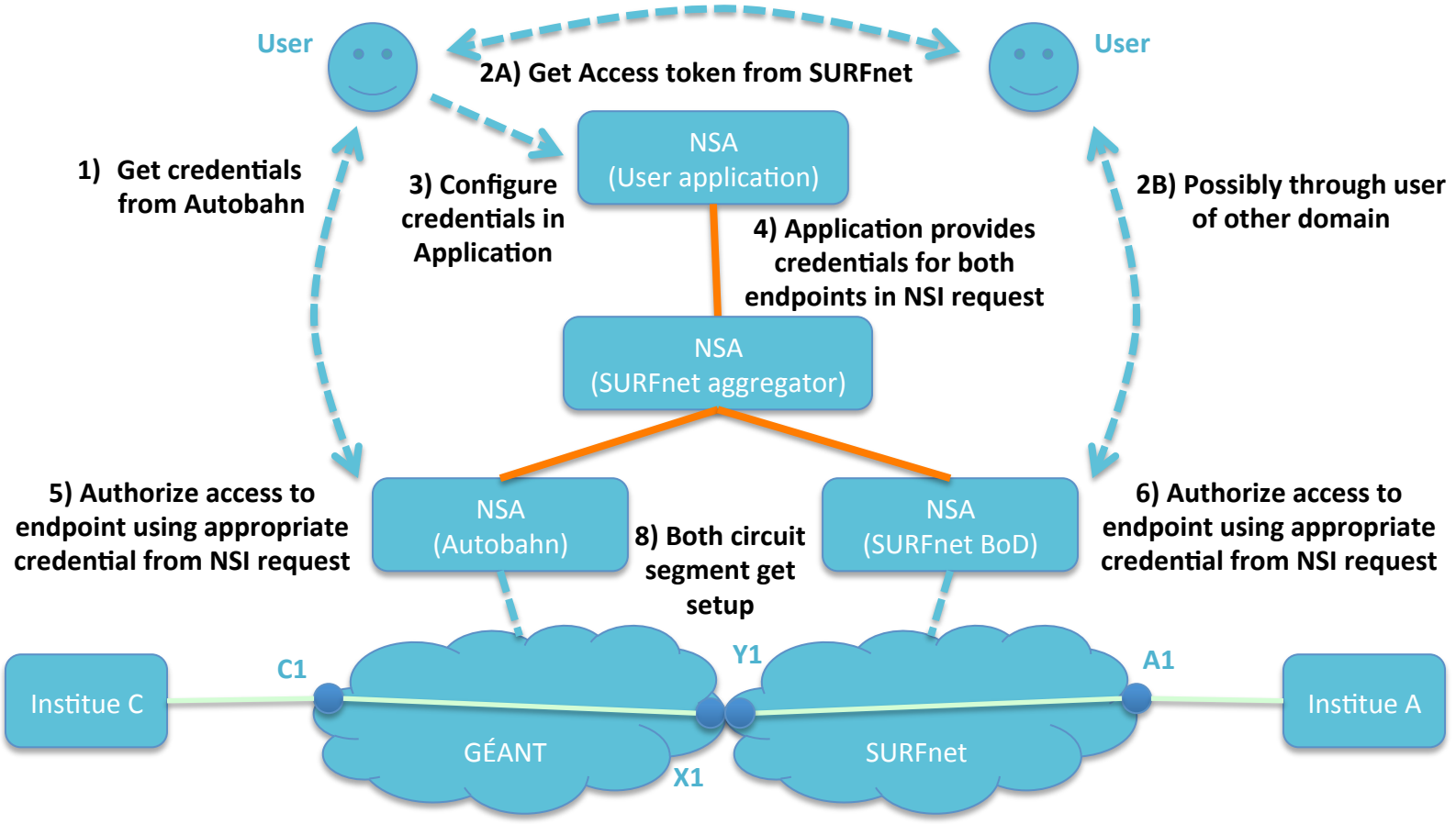
SURFnet: setup circuit via GUI



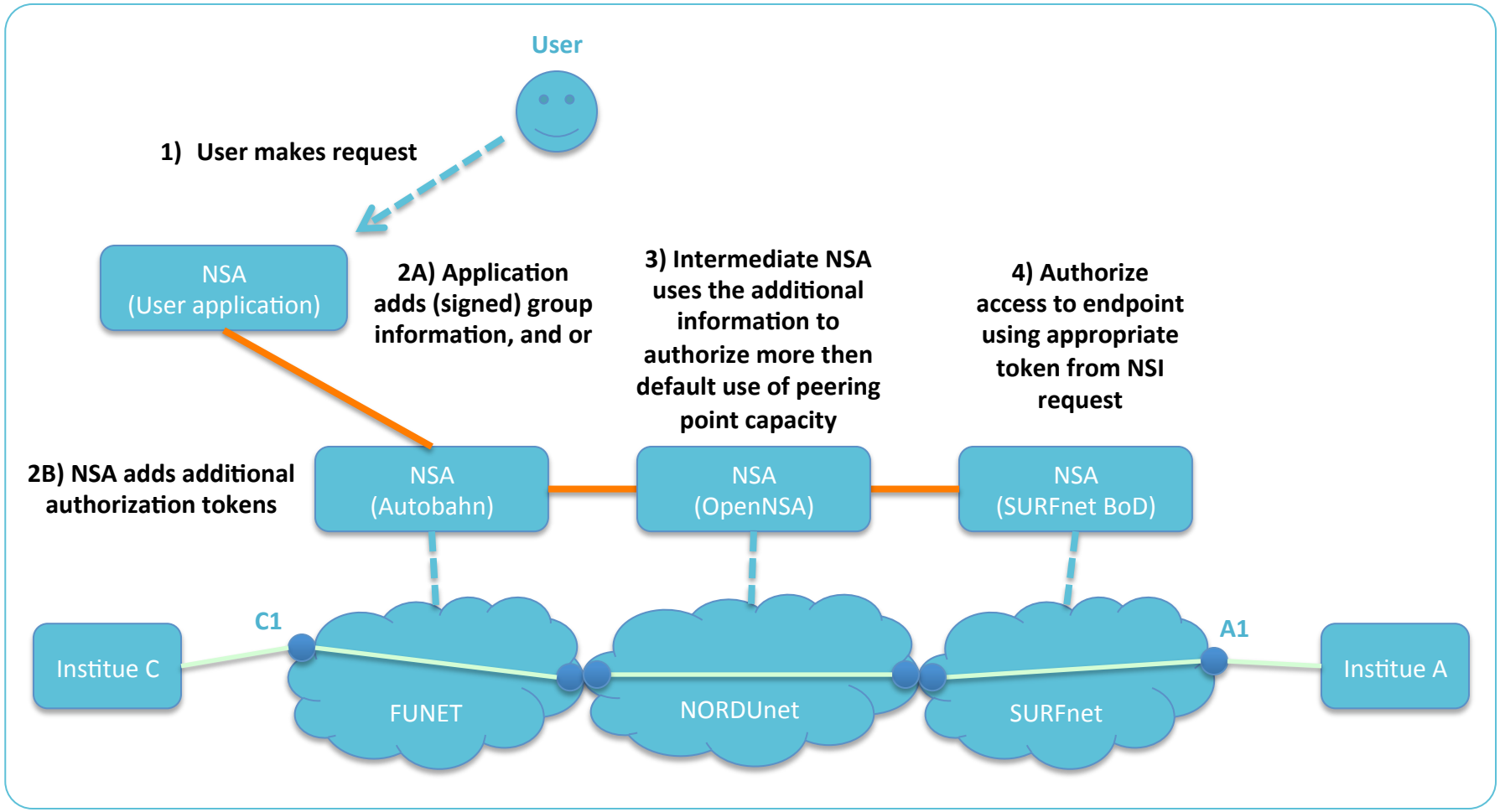
SURFnet: setup circuit via API



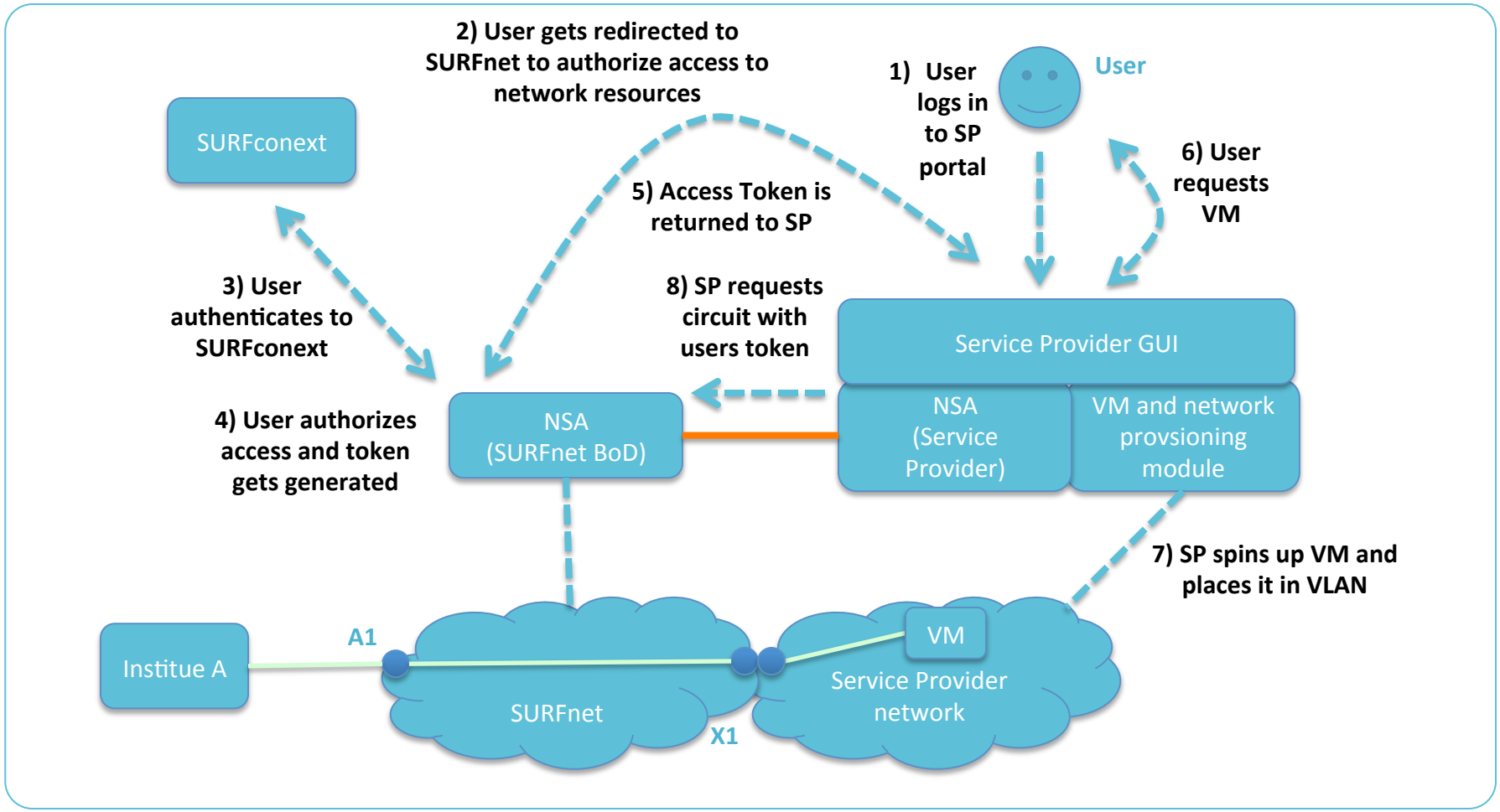
Multi domain endpoint authorization



Multi domain peering point authorization



SURFnet: Service Provider support



NORDUnet/SURFnet: NSI message header

The information in the NSI header will be extended with:

- Identity information of the originating user (mandatory)
  - User ID (mandatory)
  - Group IDs (optional)
  - Added as sessionSecurityAttr to the NSI header
- Endpoint authorization tokens (optional)
  - E.g. OAuth2 Access Token
  - E.g. X.509 certificate
  - E.g. SAML Enhance Client or Proxy Profile
  - Added as sessionSecurityAttr to the NSI header
- Connection trace (mandatory)
  - Hop by hop control plane connection trace
  - Added using the “any” to the bottom of the NSI header

Originating user identity information

The originating user identity information consists of:

- Exactly one User ID
  - E.g. eduPersonPrincipalName
  - E.q. eduPersonTargetedID
- Optionally one or more Group IDs

Example:

```
<sessionSecurityAttr>
   <Attribute Name="user" Type="eduPersonTargetedID">
      <AttributeValue>
         364adcea4cf741169235be6f903ba6f0
      </AttributeValue>
   </Attribute>
   <Attribute Name="group">
      <AttributeValue>nordu.net</AttributeValue>
      <AttributeValue>dev.nordu.net</AttributeValue>
   </Attribute>
</sessionSecurityAttr>
```

Endpoint authorization tokens: e.g. OAuth2 Access Token

Example:

```
<sessionSecurityAttr>
   <saml:Attribute Name="nl.surfnet.auth.token">
      <saml:AttributeValue>
         <saml:Attribute Name="o-auth-token">
            <saml:AttributeValue>
               58c19348-8e2a-4aa9-af35-d3e75e516086
            </saml:AttributeValue>
         </saml:Attribute>
      </saml:AttributeValue>
   </saml:Attribute>
</sessionSecurityAttr>
```

Endpoint authorization tokens: e.g. signed group ID

Example:

```
<sessionSecurityAttr>
   <saml:Attribute Name="net.nordu.auth.group">
      <saml:AttributeValue>
         <saml:Attribute Name="group">
            <saml:AttributeValue>nordunet.lhc</saml:AttributeValue>
         </saml:Attribute>
         <ds:Signature>
            <ds:SignedInfo>
               <ds:CanonicalizationMethod Algorithm=""></ds:CanonicalizationMethod>
                  <ds:SignatureMethod Algorithm=""></ds:SignatureMethod>
                  <ds:Reference>
                     <ds:DigestMethod Algorithm=""></ds:DigestMethod>
                     <ds:DigestValue>
                        OmHNngBYeBRnojeiGM82uurYfwrrAm20OIbQZAYRxS/6BbLK/LaVLI8cUkZotA7I
                        XyHY68O70IOKRT3HbiyORR5jp5V6oobztoHxszJWjtkCDEamoW2Cw3b+mo3mxHF3
                        EtFRz3uxprqYJPYRmgT6K2NTfBvUyEIXynC6atpHMrjfwsZ4KKYshMj0jqeoY4u7
                     </ds:DigestValue>
                  </ds:Reference>
               </ds:SignedInfo>
            <ds:SignatureValue></ds:SignatureValue>
         </ds:Signature>
      </saml:AttributeValue>
   </saml:Attribute>
</sessionSecurityAttr>
```

Connection trace

A connection trace consists of a list of connection URNs and is added to the bottom of the NSI header

Connection URN = NSA URN + ':' + connection ID

Example:

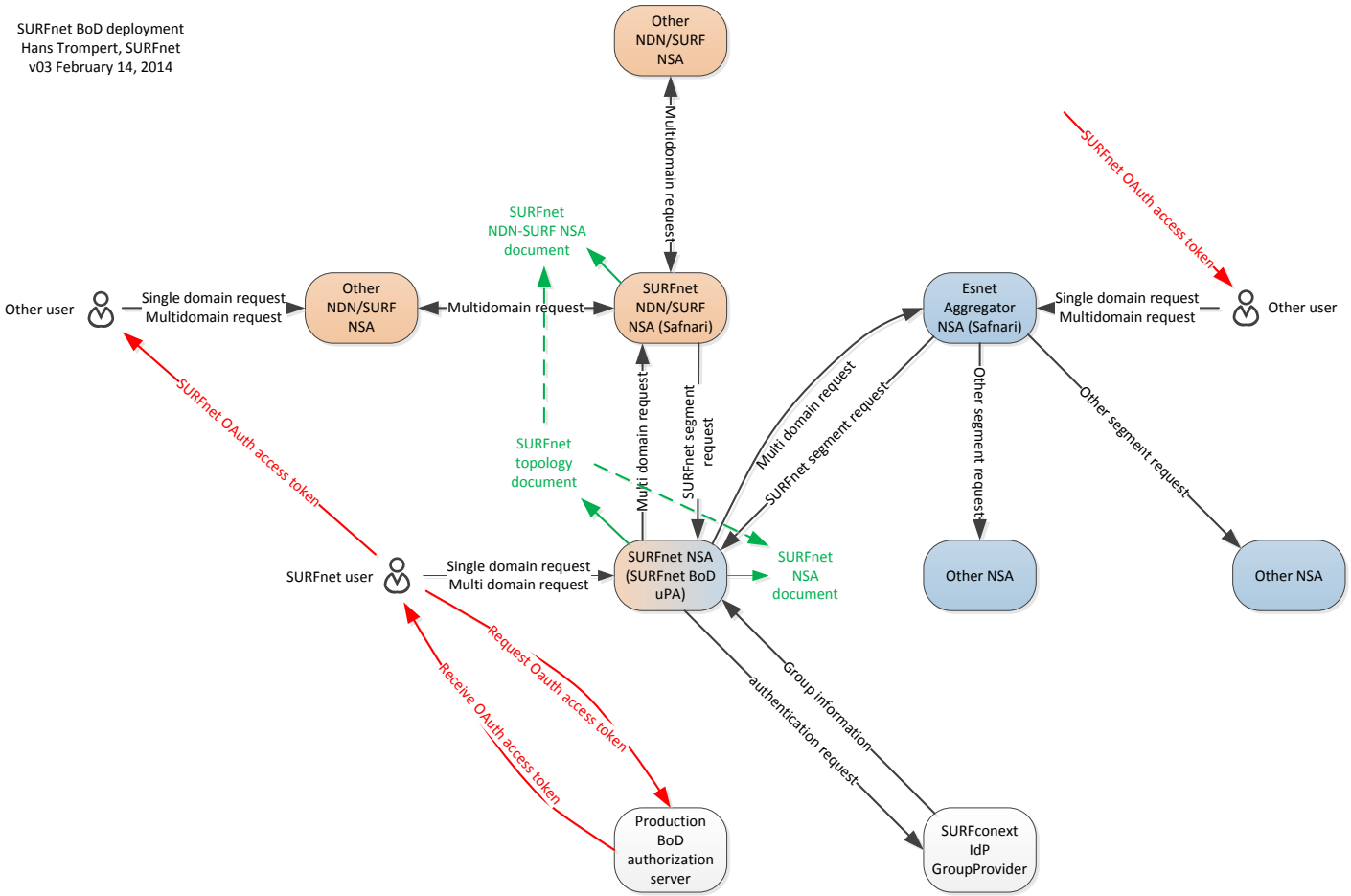
NSA: urn:ogf:network:aruba.net:nsa
Connection Id: AR-Tfe07c58e3fff
Connection URN: urn:ogf:network:aruba.net:nsa:AR-Tfe07c58e3fff

```
<ConnectionTrace>
   <Connection Index="1">urn:ogf:network:aruba:2013:nsa:AR-Tfe07c58e3fff</Connection>
   <Connection Index="2">urn:ogf:network:bonaire:2013:nsa:BO-s7780</Connection>
   <Connection Index="3">urn:ogf:network:curacao:2013:nsa:CU-1234</Connection>
</ConnectionTrace>
```

AAI implementation: who and when

- Implemented by
  - NORDUnet
  - SURFnet
  - GÉANT
- Implementation March 2014
- Beta testing April 2014
- Production May 2014

SURFnet planned deployment



hans.trompert[at]surfnet.nl

www.surfnet.nl