NSI Authentication and Authorization draft 5.1

Hans Trompert, SURFnet
OGF NSI WG meeting Uppsala
22 September 2014

Requirements

- Every NSA must be able to trace back a NSI request to the originating NSA
- It must be possible to identify the originating user of a NSI request
    - This implies that every uRA must authenticate its users
- Attributes needed by any NSA to perform authorization must be transported transparently through the control plane
- Any NSA is allowed to add (additional) authorization attributes to a message
- Every subsequent message after the initial reserve that can change the state of a reservation must be authorized

connectionTrace

- Every entry contains the NSA ID
- Every entry, except the first entry for the uRA, contains the connection ID local to that NSA
- Every entry has an order attribute starting with 0 and monotonically increasing by 1

```xml
<connectionTrace id="urn:uuid:862319f0-2221-11e4-8c21-0800200c9a66">
    <nsa order="0" id="urn:ogf:network:es.net:2013:nsa:nsi-requester" />
    <nsa order="1" id="urn:ogf:network:es.net:2013:nsa:nsi-aggr-west">
        <connectionId>645ababf-0b5a-46ff-a75a-b56892d2e79b</connectionId>
    </nsa>
    <nsa order="2" id="urn:ogf:network:es.net:2013:nsa">
        <connectionId>urn:uuid:866d1a5c-1c1f-4dd2-a00b-656d33aad394</connectionId>
    </nsa>
</connectionTrace>
```

Authorization domains

- To group security attributes per authorization domain
- A authorization domain can be any (existing) authentication/ authorization infrastructure that is used by a NSA to perform (part of) its authorization (e.g. GSI, SURFconext, etc.)
- Every NSA can easily select the security attributes that apply to him

```
<sessionSecurityAttr type="edu.opengrid.authorization">
    <saml:Attribute Name=”…."> 
        <saml:AttributeValue xsi:type="xs:string”>….</saml:AttributeValue>
    </saml:Attribute>
</sessionSecurityAttr>
<sessionSecurityAttr type="net.surf.authorization">
    <saml:Attribute Name=”…."> 
        <saml:AttributeValue xsi:type="xs:string">….</saml:AttributeValue>
    </saml:Attribute>
</sessionSecurityAttr>
```

userID

- userID is a mandatory security attribute
- It contains the authenticated identity of the originating user and stored in the message header by the uRA
- Any NSA along the control plane path of the message is allowed to replace the userID and will thereby take all responsibility for that request from there on

```
<sessionSecurityAttr>
    <saml:Attribute Name="userId">
        <saml:AttributeValue xsi:type="xs:string">hans@surf.net</saml:AttributeValue>
    </saml:Attribute>
</sessionSecurityAttr>
```

Authorization attributes

- All other authorization attributes, possibly grouped by authorization domain, are just added to the message header

```
<sessionSecurityAttr type="edu.opengrid.authorization">
   <saml:Attribute Name="certificate">
      <saml:AttributeValue xsi:type="xs:string">A PEM encoded certificate</saml:AttributeValue>
   </saml:Attribute>
</sessionSecurityAttr>
<sessionSecurityAttr type="net.surf.authorization">
   <saml:Attribute Name="accessToken">
      <saml:AttributeValue xsi:type="xs:string">149ac38c-14cc-a34e-349aa87c71aa</saml:AttributeValue>
   </saml:Attribute>
   <saml:Attribute Name="certificate">
      <saml:AttributeValue xsi:type="xs:string"> A PEM encoded certificate </saml:AttributeValue>
   </saml:Attribute>
</sessionSecurityAttr>
```

Subsequent message authorization

- Every message after the initial reserve request that can change the state of a reservation must be authorized, for NSI CS 2.0 that are:
  - reserve, reserveCommit, reserveAbort, provision, release, terminate
- Every other message may be authorized, for NSI CS 2.0 that are:
  - querySummary, queryRecursive, querySummarySync, queryNotification, queryNotificationSync, queryResult, queryResultSync
- Simplest form of authorization of messages after the initial reserve request is to only allow userID as found in the initial reserve request to change the state of a reservation
- Local policies may always override message authorization, for example to allow a local NOC engineer to terminate a reservation

✉ hans.trompert@surfnet.nl

W www.surfnet.nl

SURF NET