Oasis SSTC F2F
4th Feb 2004

W25 - Kerberos & SAML

John Hughes, Entegrity Solutions
Tim Alsop, CyberSafe Limited
Current Document Progress

- Two documents:
  - Generalised AuthnRequest Profiles
    - Working Draft 02, 1st February 2004
    - draft-sstc-solution-profile-kerberos-02
  - Kerberos SAML Profiles
    - Working Draft 02, 1st February 2004
    - draft-sstc-solution-profile-kerberos-02
Initial Use Cases
Scope : draft-sstc-solution-profile-kerberos-??

- Provide a secure and trusted mechanism to pass a user identity to the SAML Responder via the SAML Service so that an artifact or assertion can be returned using the authenticated identity of the user.
- Provide a secure and trusted mechanism to allow the SAML Service to communicate with the SAML Responder;
- Provide secure sessions (e.g. mutual authentication, data integrity, confidentiality, channel binding, replay attack detection) between the authentication and authorisation related infrastructure components required for a SAML deployment;
- Implement a Single SignOn (“SSO”) experience for users - especially useful when the workstation and/or server operating systems have a Kerberos implementation available and multiple vendors operating systems are used;
- Take advantage of the credential delegation/forwarding capability in the Kerberos protocol to pass credentials securely from middle tier to back-end tier application and infrastructure components;
- Provide a secure approach for passing a SAML Assertion to an application that is Kerberos enabled.
<xml version='1.0' encoding='UTF-8' ?>
<!-- Schema for DCE PAC -->

<x:schema xmlns:xs="http://www.w3.org/2001/XMLSchema"

targetNamespace="sstc-saml-schema-dce-pac-2.0-cs.xsd">

<x:element name="ForeignGroup">
   <xs:complexType>
      <xs:sequence>
         <xs:element name="Realm" type="string" minOccurs="1" maxOccurs="1"/>
         <xs:element name="GroupName" type="string" minOccurs="1" maxOccurs="unbounded"/>
      </xs:sequence>
   </xs:complexType>
</x:element>

</x:schema>
Nameldentifier Syntax?

1) 
<saml:Subject>
    <saml:NameIdentifier
        NameQualifier="http://www.cybersafe.ltd.uk/
        Format="urn:oasis:names:tc:SAML:2.0:nameid-format:kerberos">
        talsop@CYBERSAFE.LTD.UK
    </saml:NameIdentifier>
</saml:Subject>

2) 
<saml:Subject>
    <saml:NameIdentifier
        Format="urn:oasis:names:tc:SAML:2.0:nameid-format:DCE"
        NameQualifier="MyRealm">
        jhughes
    </saml:NameIdentifier>
</saml:Subject>
Outstanding:

- Microsoft Kerberos PAC authorisation data mapping
- Binding Kerberos credentials to SAML Assertion – how/why?
- More details on Kerberos/GSS-API bindings
- Take advantage of any existing Liberty, WSS, Microsoft Passport Kerberos related standards/drafts

Future

- Site to Site (e.g. cross realm) trust
- Other …