Enhancing Cardspace using the Identity Capable Platform

Conor P. Cahill, Naveen Mellemmpudi
Intel Corporation
What you are about to see is a bunch of starry-eyed technological research. There is no current or future publicly announced product which includes this functionality.
The Identity Capable Platform

A protected environment
- An Identity Manager (IDMgr)
- One or more Manageable Identities (iMID)

Full lifecycle support for Manageable Identities
- Provision, update, delete
- Activate, deactivate
- Serialize/deserialize
- Portability
- Over the wire/air as well as physical provisioning

Policy controlled access and operations
- Which user can access which iMID
- What can be done with each iMID
ICP in a Nutshell

Service Provider

Identity Provider

Identity Agent

PC/Device

Protected Environment

IDManager

OS

Apps

Browser+
Cardspace (Identity Selector)
Cardspace w/ICP

PC/Device

1. Relying Party

2. Browser

3. Cardspace

4. IDManager

5. OS

6. Identity Agent

Protected Environment
Advantages of local IdP agent

- Platform becomes something the user has
  - An authentication factor
- Local Authentication
  - Increased security
  - Decreases value of stolen credentials
- Increased Privacy
  - Network IdP doesn’t need to know exactly when user went where
- Load distribution
  - Network IdP distributes authn load to the network edge
- Resiliency
  - IdP can be offline or otherwise unavailable
IdP Agent

1. WS-Trust interface for Cardspace requests/responses
2. ID-WSF Provisioned Module (PM) for administrative operations w/IDManager
3. SAML 2.0 Engine w/delegation assertion support to
4. ID-WSF ICP Svc Client to get SAML Minting assertions from Network IdP
5. Policy Engine to enforce issuing policies from IdP
6. Local Authentication interface to authenticate user as dictated by policies
SAML 2.0 Delegation

- Minted Assertion
  - SAML Assertion created by someone other than original IdP (e.g. someone who doesn’t have IdP’s private key)
- Minting Assertion
  - Delegate right to mint assertions to another party
  - Carried in <Advice> of Minted assertions
  - Has controls/policies directed at Minted assertion
    - Limited relying parties
    - Limited user identities
    - Limited timeframes
    - Etc., etc.
- Part of Liberty ID-WSF Advanced Client
  - ID-WSF IDP Service one way to obtain such tokens
  - Advanced Client Overview documents token profile
SAML 2 Minting Assertion (MING)

```xml
<saml2:Assertion xmlns:saml2="urn:oasis:names:tc:SAML:2.0:assertion" ID="sxJu9gvvLG9sAN9bKp8q0NKU"
    IssueInstant="2006-05-01T17:20:30.213Z" Version="2.0">
    <saml2:Subject>
        <saml2:SubjectConfirmation Method="urn:oasis:names:tc:SAML:2.0:cm:holder-of-key">
            <ds:KeyInfo>PublicKey info for IdP Agent</ds:KeyInfo>
        </saml2:SubjectConfirmation>
    </saml2:Subject>
        <saml2:AudienceRestriction><saml2:Audience>Provider1</saml2:Audience></saml2:AudienceRestriction>
    </saml2:Conditions>
    <saml2:AuthzDecisionStatement Resource="urn:oasis:names:tc:SAML:2.0:assertion" Decision="Permit">
</saml2:Assertion>
```
SAML2 Minted Assertion (MED)

```xml
<saml2:Assertion xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion" ID="ID_1"
    IssueInstant="2006-05-02T11:43:12.723Z" Version="2.0">
    <ds:Signature>IdP Agent's Signature</ds:Signature>
    <saml2:Subject>
        <saml2:NameID NameQualifier="SP's Provider ID" Format="urn:oasis:names:tc:SAML:2.0:nameid-format:persistent">
            Principal's NameID at SP
        </saml2:NameID>
        <saml2:SubjectConfirmation Method="urn:oasis:names:tc:SAML:2.0:cm:bearer">
            <saml2:SubjectConfirmationData InResponseTo="AuthnRequestID" />
        </saml2:SubjectConfirmation>
    </saml2:Subject>
        <saml2:AudienceRestriction>
            <saml2:Audience> SP's Provider ID </saml2:Audience>
        </saml2:AudienceRestriction>
    </saml2:Conditions>
    <saml2:Advice>
        <saml2:Assertion ...> MING assertion data here </saml2:Assertion>
    </saml2:Advice>
        Authentication information here
    </saml2:AuthnStatement>
</saml2:Assertion>
```
ACME Bank Demonstration

- IDP & Relying party are same entity (ACME Bank)
  - ACME using this to create second user auth factor
- Provisioning of IdP Agent
  - Using Liberty ID-WSF Advanced Client protocols
- Use of IdP Agent through Cardspace
  - Authenticating back to ACME Bank
  - Using stock, off-the-shelf Cardspace
- Compare to existing 2\textsuperscript{nd} factor authns
  - Stored cookie (most common)
  - User hardware token (e.g. SecurID).
Provisioning of IdP Agent

1. User browses to ACME Bank and signs up for secure token
2. ACME sends IdP Agent Provisioning handle through browser to IDManager
3. IDManager uses provisioning handle to get IdP Agent
4. IDManager instantiates IdP Agent
5. IdP Agent creates private key(s) and registers public key with ACME Bank IdP. IdP Agent would also typically request minting assertion(s) at this point.
6. IDManager registers Infocard with Cardspace
Use of provisioned IdP Agent

1. ACME Bank initiates Cardspace Autn through browser
2. Browser feeds request to Cardspace
3. User selects ACME Bank Infocard and Cardspace sends token request to IdP Agent
4. IdP Agent authenticates user (if necessary) and, upon success, generates SAML 2.0 token (using minting token issued by ACME IdP) and returns it to Cardspace
5. Cardspace encrypts token for ACME Bank and sends to browser.
6. Browser submits token to ACME Bank
Issues

• SSL currently required to IdP agent
  • CA root keys, X509 certs for each agent, etc.
  • Confidentiality probably not necessary on local cxn
  • Possibly just put IdP Agent public key in InfoCard

• Cardspace doesn’t know about ICP & IDManager
  • We had to manually stick infocard into Cardspace
  • Better if Cardspace recognized ICP platform and asked IDManager to enumerate infocard compatible IdP Agents

• Still some weak points to attack *session*
  • Cardspace or browser could be replaced by malware
  • But, would be a single session token as opposed to reusable token
  • Even if you totally protect Authn event, you then have potential hijack attacks on browser session
Standards

Provisioning & Lifecycle management
- Liberty Advanced Client
  - Provisioning Service
  - Provisioned Module Management Service

Delegated Token Generation
- SAML 2.0
- Liberty Advanced Client
  - IdP Service
  - Trusted Module (SAML 2.0 Delegation profile)

Cardspace Integration
- WS-Trust
- Infocards
- Identity Selector Protocols
More Information

Liberty:  http://www.projectliberty.org
Infocard:  http://www.informationcard.net
ICP: http://www.intel.com/technology/systems/stl/
My blog: http://conorcahill.blogspot.com
Email:  Conor.P.Cahill – at - intel.com
Questions ?