Information Card Support

What is an Information Card?

See INTRODUCING INFOCARD, which Kim Cameron describes as "An excellent introduction to InfoCard technology by David Chappell".

The technical description of the Information Card profiles is currently controlled by Microsoft, and can be found here.

Broadly speaking, there are two kinds of cards: managed and unmanaged. Managed cards represent an identity that is mediated by an IdP, and involves authentication to that IdP. Unmanaged cards represent an identity that is mediated locally by the client and is self-asserted, but the process involves a signature using locally controlled private keys, making it somewhat ssh-like.

1. Planned Functionality for Version 1

1. Extend the IdP to support Information Card profiles using SAML assertions as security tokens
2. Extend the SP to support authentication via managed card
3. Extend the SP to support authentication via unmanaged card
4. Extend SAML metadata via a profile to capture basic Information Card requirements

This support will be based on the Identity Selector Interoperability Profile V1.5 (August, 2008). If interoperability requires additional profiling, that work will be submitted to an appropriate OASIS TC.

There are no immediate plans to natively support authentication **to** the IdP using the Information Card profile. However, deployers can wrap the Shibboleth SP around the IdP's REMOTE_USER login handler, turning the IdP into a gateway between the Information Card and SAML protocols.

1.1 Extend the IdP to support Information Card profiles using SAML assertions as security tokens

- The browser user will be able to go to a new endpoint at the IdP, authenticate, and obtain an Information Card with a set of SAML attributes, as configured by the administrator. The IdP extension will likely include a mechanism and templates for managing this. A deployment could choose to make multiple endpoints available, each one creating a card with different sets of attributes.
- The SAML attributes will map to claims that Information Card RPs can request, enabling the client-side selection of appropriate cards in the standard fashion.
- The extension will integrate fully with the existing IdP policy controls over attribute release, utilizing SAML metadata, along with possibly other policy dialects, to identify relying parties and filter attributes. The combination of administrative and user control over release will be similar to that achieved with the SWITCH ARPViewer for browser SSO.
- Support for non-audited SSO will be disabled by default, because of its insecurity.
- Initially, the IdP extension will support only the username/password authentication mechanism defined by the Information Card profile.
- Both SAML 1.1 and 2.0 assertions will be usable as security tokens. A profile for their content will be documented and submitted to an appropriate OASIS TC, and we will work with vendors as much as possible to ensure consistency in the meantime.

1.2 Extend the SP to support authentication via managed card

- An SP extension library will be developed to add a SessionInitiator and AssertionConsumerService handler to trigger an identity selector and validate a supplied bearer assertion respectively.
- SAML 1.1 and SAML 2.0 assertions (encrypted and plaintext) will be supported.
- Attributes and assertion content will be processed in the usual fashion and made available to applications.
- Additional hooks to support any Information Card WS-SecurityPolicy requirements will be developed as needed.

1.3 Extend the SP to support authentication via unmanaged card

- The same extensions that handle managed security tokens will be extended to optionally recognize and accept unmanaged tokens.
- No identity mapping or validation will be performed by the SP; the public key information will be made available to applications in some form, and they will be responsible for any account linking requirements.
- Microsoft has a document available from MSDN that covers some of this space: Patterns for Supporting Information Cards at Web Sites: Personal Cards for Sign-up and Sign-In

1.4 Extend SAML metadata via a profile to capture basic Information Card requirements

- As with the ADFS / WS-Federation extension, SAML metadata will be used to capture and communicate critical information about endpoints and trust information, using a profile that allows the information to co-exist alongside the existing SAML support.
- There is no intent to duplicate or replace the use of WS-SecurityPolicy within the Information Card profiles, but merely supplement it so that the existing trust models supported by Shibboleth can be applied.

2. Possible steps toward providing a testbed

- Add Infocard support to the TestShib SP; sites could install Infocard support into their IdPs, and test via TestShib.
- Add Infocard support to the spaces wiki. Sites would have to offer a "managed card service", and federations would need to support the appropriate metadata profile, in order to use this.

3. Possible Functionality in Future Versions

Kerberos Support

The Shibboleth 2.2 IdP may provide support for SP-NEGO authentication. This may allow the Information Card support to be subsequently extended to allow for authentication to the IdP via Kerberos. The technical details are different, but some of the back-end requirements will be similar.

Non-browser Use Cases

There was some discussion about the need to support more than just web-based use of the profile; it was noted that Bandit has begun to think about this use case. The browser version of the profile has been engineered and profiled by Microsoft to literally disallow proof keys. Some people feel that the security benefits of tokens with proof keys (non-bearer tokens) should be available to applications that want to take advantage of them.

We agreed to think about including support for proof keys (via the symmetric and asymmetric bindings) in possible future versions of the Information Card support. Additionally, IdP support for holder-of-key models likely supplies code that may be useful to other SAML and non-SAML profiles.

Authentication to the IdP via Unmanaged Cards

Supporting authentication with unmanaged cards includes more than deploying an SP to handle the authentication itself; as an "application", the IdP is also required to support registration of a user's PPID claim and key against their authenticated identity, and then mapping to that identity at runtime. We agreed that it would be sufficient to provide a working example (e.g. using JDBC).

4. Discussion Items and Concerns

4.1 Attributes and Policy

There are some major differences between the models that Shibboleth versions through v2.1 and Infocard use to manage the release of attributes to Relying Parties. Shibboleth imagines that a site administrator creates Attribute Filter Policies that govern the release of attributes and specific values to various SPs. Some Shibboleth extensions provide additional control models, but the basic model is that the site manages a set of policies. Infocard, on the other hand, imagines that the browser user trusts the RP based on its certificate, and wants certain attributes delivered to the RP. The common use case is the consumer case, where the IdP has essentially no organizational policy but is just serving the user's interests.

While there is relatively little in the basic Infocard profile suggesting who is supposed to trust whom for what purpose, the profile is definitely written to strongly communicate a model in which the IdP is not a vehicle for controlling what the user does or where they do it. We may run into limitations or impedance mismatches in developing a hybrid model in which both the organization and the user mutually control the release policy, or limit card use at the IdP with particular RPs.

Infocard expects a user to have a few cards, from different issuers. We're thinking about a model where a user might have a few cards from the same issuer (the different cards would release different attributes). Because of the way the claims model works, it is likely going to be impractical to pursue the multiple card model as a way to control release from the user's end unless the set of claims involved is distinct. As an example, it's certainly usable if all the cards were distinct in terms of claims and only a single card lit up for an SP. That's exactly how it should work. But, a site could certainly configure their IdP to issue a set of cards that cause significant user confusion.

Shibboleth attribute policy is designed to allow the filtering of specific attribute values. InfoCard doesn't provide for such filtering. A card might support "eduPersonEntitlement" -- in this case, policy-based filtering would still have to be done by the IdP administrator. Supporting user control over the release of individual values will be very difficult if not impossible.

It was agreed that the Shibboleth project would pursue a "hybrid" model in which the filtering engine remains involved in the attribute release process. The filtering engine does know the protocol that's being used (enabling different default release policies for different protocols -- if SAML, release nothing, if Infocard, allow the user to drive the decision).

4.2 RP Identity

Infocard doesn't have metadata in the same sense that SAML uses it; the client is assumed to be the agent that trusts the RP. The client usually just tells the IdP where the data will be sent, to enable bearer restrictions in the assertion and questionable methods for obtaining an encryption key.

That makes it difficult for a Shibboleth IdP to enforce policy based on RP identity without being able to reverse map from the location to the RP. This is exactly what Shibboleth got wrong in the pre-1.2 days. Unfortunately, we are now back to that situation. It is our sense that we need to extend the IdP's MetadataProvider interface, to allow lookup by endpoint.

5. Open Issues

- Do we support both the pre-OASIS and final versions of WS-Trust, for compatibility reasons, or is there nothing interesting to be compatible with?
- Do we use the Switch WS-Trust implementation, or one-off something for now?

6. Related Information

http://www.microsoft.com/downloads/details.aspx?DisplayLang=en&FamilyID=b94817fc-3991-4dd0-8e85-b73e626f6764

Kim Cameron's Web Site

Bandit Project's DigitalMe (Info Cards for Firefox)

Info Card Support within the Shibboleth 2.0 IdP

Info Card Support within the Shibboleth 2.0 SP