IdP API

Eric Rescorla

ekr@rtfm.com

Default Browser Behavior

- Request identity assertion if browser configured with IdP
  - Automatically inserted into offer/answer
- Validate identity assertion if received in offer/answer
  - Display results in browser UI
- DTLS fingerprints exch
- No JS application intervention required
- But we want APIs to allow customization

New API points

- Control identity generation
- Set the desired IdP and identity
- Pre-generate an assertion (performance)
- Interrogate a validated assertion

Constraints for Identity

- `RequestIdentity` constraint
  - `yes` – always generate an identity assertion
  - `no` – never generate an identity assertion
  - `ifconfigured` – generate an assertion user has configured an identity provider or if `setIdentityProvider()` has been called

Set desired IdP and identity

```
void setIdentityProvider (
                          DOMString Provider,
                          optional DOMString protocol,
                          optional DOMSTring username
                         );
```

`provider` – domain name of the provider

`protocol` – the protocol name (locally meaningful)

`username` – the desired user name

- Overrides user configuration settings
  - Is this the right priority?
  - Should we prescribe a priority?

Pre-Generate Assertions

```
void getIdentityAssertion ();
```

- Idea here is to generate identity assertion ahead of time
  - Same reason as we want to start ICE gathering early
  - Otherwise assertion happens at offer/answer generation
- This works because we only need DTLS fingerprint
- Should we have a success/failure callback?

Interrogate a valid assertion

```
readonly attribute RTCIdentityAssertion peeridentity;

interface IdentityAssertion {
  attribute DOMString idp;  // The identity provider
  attribute DOMString name; // The peer identity (rfc822-style)

};
```

- If identity was not used, this attribute is null

Detecting Identity Verification

- `onidentityresult` event
- Called when an identity verificat succeeds or fails
  - Should this have an argument or do you just check `peeridentity`?