

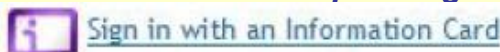
Client-based CardSpace-OpenID Interoperation

1. Abstract

We present a novel scheme to provide interoperability between two of the most widely discussed identity management systems, namely CardSpace and OpenID. The scheme, based on a browser plugin, enables CardSpace users to obtain an assertion token from an OpenID provider (OP), the contents of which can be processed by a CardSpace-enabled relying party (RP).

2. User Experience

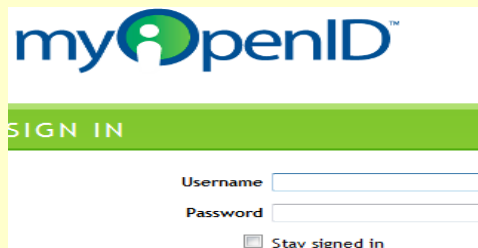
A. User clicks CardSpace logo



B. User selects OpenIDCard



C. User signs on to OP



D. User accesses CardSpace RP

WELCOME

4. Protocol (2/4)

- The user clicks the CardSpace logo, invoking the CardSpace selector, and submits an OpenIDCard.
- The plugin intercepts the RSTR, and uses its contents to build an OpenID authentication request, and redirects the user to the OP.

5. Protocol (3/4)

- The OP authenticates and redirects the user back to the RP with an OpenID token.
- The plugin verifies the MAC-protected OpenID token by interacting with the OP using the 'check_authentication' mode via a TLS/SSL channel.

6. Protocol (4/4)

- The plugin constructs a CardSpace-compatible SAML token (using the RSTR & OpenID tokens), and forwards it to the RP.
- The RP verifies the SAML token (including verifying the RSTR signature, PPID, nonce, time-stamps, etc.), and, if satisfied, grants access.

7. Features & Conclusions

- Benefits from CardSpace security features (e.g. it defeats phishing attacks).
- Transparent to OPs and identity selectors.
- Supports exchange of user attributes.
- Stronger user authentication (the user must authenticate via CardSpace and OpenID).

3. Protocol (1/4)

- A user navigates to an RP webpage containing CardSpace tags, in which the RP policy is embedded.
- The browser plugin:
 - examines the RP policy to check whether the use of personal cards is acceptable; and
 - keeps a local copy of any RP-requested claims.