The CardSpace Identity Management Framework

Chris Mitchell
Royal Holloway, University of London
http://www.isg.rhul.ac.uk/~cjm
c.mitchell@rhul.ac.uk

Structure of talk

a. Introduction to CardSpace
b. Underlying philosophy
c. The CardSpace architecture
d. Secure interactions
e. Security and privacy issues
f. Possible solutions

Structure of talk

a. Introduction to CardSpace
b. Underlying philosophy
c. The CardSpace architecture
d. Secure interactions
e. Security and privacy issues
f. Possible solutions

CardSpace

- CardSpace is a Microsoft architecture for identity management.
- It has a number of component parts:
  - A distributed architecture for identity management;
  - A set of defined Web Services interfaces between entities in the architecture;
  - A set of software is available for both Vista and XP which will enable users to manage their identities in a Windows environment;
  - Development support to enable applications to use CardSpace managed identities.

Identity Metasystem

- Microsoft refers to this collection of components as an Identity Metasystem.
- The idea is to provide a unified way for (Windows) users to use many different underlying identity management systems.
- Key ideas here are:
  - provide a simple user model for identity;
  - enable users to control which identity is used for what purpose.

What about Passport?

- Microsoft's experience with Passport has been rather painful.
- They tried to solve the problem of identity management by becoming ***the*** global identity provider.
- This idea failed abysmally – the main lesson is that there will never be such a global identity provider.
- This has led to CardSpace, as a means of supporting an identity ecosystem with multiple providers …

Structure of talk

a. Introduction to CardSpace
b. Underlying philosophy
c. The CardSpace architecture
d. Secure interactions
e. Security and privacy issues
f. Possible solutions

The Laws of Identity

- In 2004/05 Microsoft (Kim Cameron) started a blog on identity.
- The purpose was to test Microsoft's evolving ideas about identity and the management of identities.
- This in turn has affected the development of things such as CardSpace.
- Cameron also developed a set of principles called the *Laws of Identity*.

The identity problem

- The Internet has arisen without any unified notion of user identity.
- As a result, there are many different solutions in place for managing identities.
- Almost every website has a different way of managing login, and collecting various bits and pieces of personal information.
- As a result, various solutions for identity management (notably SSO schemes) have emerged.

Criminality and identity

- Serious threats to identity have emerged, notably phishing and pharming attacks.
- Problems arise because users do not know who their PC is talking to.
- Users are tricked into revealing credentials and/or installing malicious software.
- In parallel, businesses holding multiple user identities are attacked, and identity data (e.g. credit card numbers) is compromised.
- Better ways of managing identities needed …

Identity management is tough

- Currently, the only successful ID management schemes are those for particular domains, e.g.:
  - Kerberos within companies;
  - Special-purpose PKIs for company use, and for specific systems (e.g. EMV);
  - Passport for MSN/Microsoft.
- No global schemes – no universal PKI.
- Identity is context-specific, which makes a universal global identity provider very unlikely.

Some identity definitions

- *Digital identity*: a set of claims made by one digital subject about itself or another digital subject.
- *Digital subject*: a person or thing, represented or existing in the digital realm.
- *Claim*: an assertion of the truth of something.

Comments I

- The Microsoft definition of digital identity is a very general one, and does not distinguish between two concepts which are often treated separately:
  - identifiers or labels (e.g. email address, National Insurance Number, passport number, …);
  - attributes (e.g. the identity holder is an employee of company X, a silver card holder for airline Y, a season ticket holder for train route Z, …)

Comments II

- There are two main justifications for the Microsoft 'claims' approach:
  - it enables protocol interactions to be simplified – a single protocol can be used to transfer claims;
  - some types of claim are difficult to categorise – a credit card number may be viewed as both an identifier and an attribute.
- However, on the down side, human beings by and large understand the distinction between the two types of claim – this means that it may be a useful distinction.

The Laws of Identity

- Microsoft has devised a set of seven *Laws of Identity*, which capture the philosophy behind CardSpace.
- In fact, if adhered to, these laws appear to have quite general repercussions for privacy in information systems.
- Rather grand claims are made for the general truth of these ‘laws’.

Law 1. User Control and Consent

Technical identity systems must only reveal information identifying a user with the user’s consent.

- Success of a system requires user trust, and giving users control will build trust.
- The law permits implementations where the metasystem allows the users to decide to automatically use identity information in a specific context.

Law 2. Minimal Disclosure

The solution that discloses the least amount of identifying information and best limits its use is the most stable long-term solution.

- This approach minimises risk by using the 'need to know' principle.
- It also reduces risk of attack.
- This also means minimising use of global identifiers (as opposed to local identifiers).

Law 3. Justifiable Parties

Digital identity systems must be designed so [that] the disclosure of identifying information is limited to parties having a necessary and justifiable place in a given identity relationship.

- The user must be aware of who he/she is sharing information with.
- This law is seen to explain the failure of Passport – Microsoft was not seen as a 'necessary and justifiable' general purpose identity provider.

Law 4. Directed Identity

A universal identity system must support both 'omni-directional' identifiers for use by public entities, and 'uni-directional' identifiers for use by private entities, thus facilitating discovery while preventing unnecessary release of correlation handles.

- A uni-directional identifier is essentially a pseudonym.
- In general, pseudonyms should be used unless there is a good reason not to.

Law 5. Pluralism of Operators and Technologies

A universal identity system must channel and enable the inter-working of multiple identity technologies run by multiple identity providers.

- This is self-evident – we all use a multiplicity of different identities, with the choice of identity depending on the context – this is not going to change.
- A universal metasystem must clearly support all these types of identity.

Law 6. Human Integration

The universal identity metasystem must define the human user to be a component of the distributed system integrated through unambiguous human-machine communication mechanisms offering protection against identity attacks.

- The human user is a key component – the lack of human understanding of the PC interface (and the identities it displays) leads to phishing and pharming.

Law 7. Consistent Experience Across Contexts

The unifying identity metasystem must guarantee its users a simple, consistent experience while enabling separation of contexts through multiple operators and technologies.

- To support the previous law, users need a consistent view of identity across multiple applications.
- This consistency should be supported by the identity metasystem, and more generally by the user experience across applications.

Structure of talk

a. Introduction to CardSpace
b. Underlying philosophy
c. The CardSpace architecture
d. Secure interactions
e. Security and privacy issues
f. Possible solutions

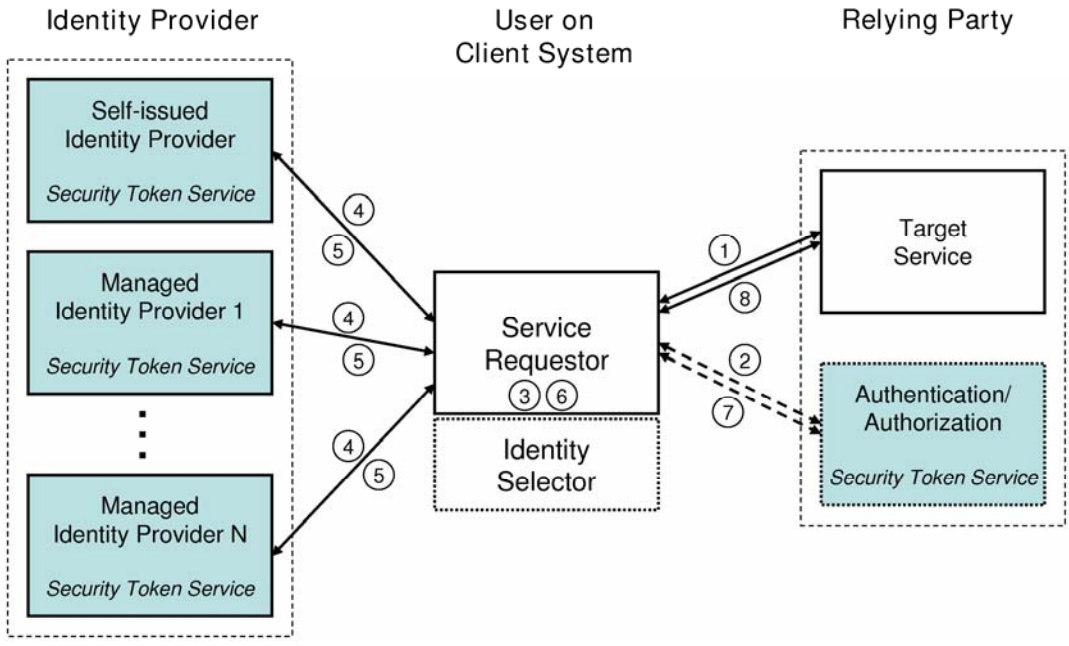
Entities

- CardSpace defines three types of entity:
  - *Users/Clients*, i.e. the entities (digital subjects) for whom identities are managed;
  - *Relying Parties*, i.e. entities who wish to have some assurance regarding an identity for a user;
  - *Identity Providers (IPs)*, i.e. entities issuing identities and providing assurance regarding identities to Relying Parties.

Use of cryptography

- Like Liberty, CardSpace is based on the use of cryptography.
- The main interactions between principals are cryptographically protected.
- Of course, the human user may authenticate to an Identity Provider using non-cryptographic means, e.g. user name/password.

CardSpace interaction model



Model operation I

- The *service requester* is a client application running on the client (user) system.
- The *relying party* is the target service the user wishes to access via the service requester.
- One or more *identity providers* can issue security tokens (to support client authentication).
- The target service may optionally delegate authentication/validation of user identity to an *Authentication/Authorisation Security Token Service*.

Model operation II

- The user, interacting with the service requester via the *identity selector*, may have identities issued by one or more IPs.
- Each identity is represented by an *InfoCard* held by the identity selector, and this InfoCard is the means by which the user interacts with the identity selector to choose which identity to use.
- Each IP runs a Security Token Service (STS), to generate security tokens.
- A *Self-issued Identity Provider* may be provided by a client platform to allow use of self-issued tokens.

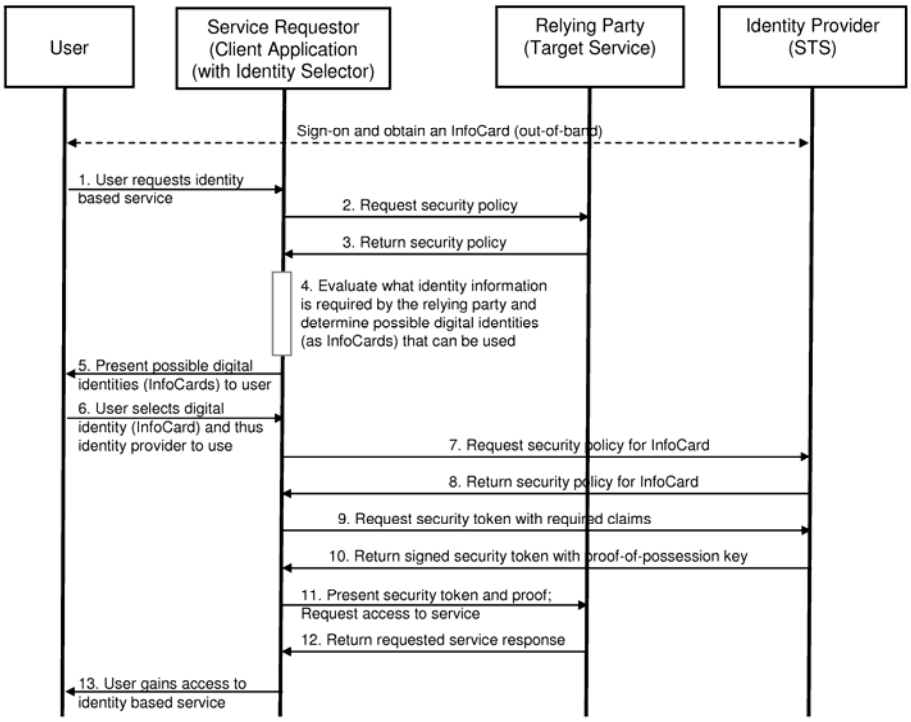
Model operation (numbered steps I)

1. Service requester gets the security policy of the target service. We suppose that the policy requires the requester to get a token issued by an IP's STS.
2. (optional) The service requester gets the policy of the authentication/authorisation STS (to determine properties of required token).
3. The requester asks the identity selector to provide a security token meeting the policy of the target service.
4. The identity selector first gets the user to choose an InfoCard capable of meeting the target service requirements, and then gets the policy of the selected IP's STS.

Model operation (numbered steps II)

5. The InfoCard indicates the method to be used to authenticate the user to the IP STS; the user sends an appropriate credential to the IP STS, and the identity selector gets back a token.
6. The token is given to the service requester.
7. (optional) The service requester presents the token to the STS, which generates a token for the target service.
8. The service requester presents the token to the target service to get access.

Message flow for CardSpace



Use of WS-security

- The interactions between principals are all web services based.
- They use mechanisms from:
  - *WS-Trust* (Web Services Trust Language);
  - *WS-SecurityPolicy* (Web Services Security Policy Language);
  - *WS-MetadataExchange* (Web Services Metadata Exchange).

CardSpace-Liberty differences

- Clearly there are differences in *scope*. Notably, CardSpace addresses user identity management.
- However, there are clear overlaps and also clear inconsistencies.
- Liberty provides profiles which work in the absence of identity management software on the client.
- CardSpace, by contrast, is built round client software.
- The existing Liberty profiles for the SSO and Federation Protocol are not consistent with CardSpace.

User interface issues

- A key component of the CardSpace architecture is the way that identities are presented to users.
- The objective is to provide a unified and simple way to manage multiple user identities.
- This applies even when the identities rely on vastly different technologies.

Structure of talk

a. Introduction to CardSpace
b. Underlying philosophy
c. The CardSpace architecture
d. Secure interactions
e. Security and privacy issues
f. Possible solutions

Interactions

- We now look in a little more detail at the interactions between the main entities in the CardSpace architecture.
- These interactions are WS based.
- Note that the form of security tokens is not constrained by CardSpace – because of the goal of supporting arbitrary identity schemes.
- Hence the messages are primarily about shipping arbitrary data structures between the parties.

Requirements – Relying Party

- A CardSpace Relying Party will need to support:
  - authentication of itself using an X.509 certificate including a logo (to assist user recognition);
  - use of *WS-SecurityPolicy* to express security requirements of the services it provides;
  - retrieval of its service metadata, including WSDL and policy, using *WS-MetadataExchange*;
  - submission of security tokens bound to application messages by service requester using *WS-SecurityPolicy* mechanisms.

Requirements – Identity Provider

- A CardSpace IP will need to support:
  - issue of InfoCards to users;
  - use of *WS-Trust* mechanisms, notably the *RequestSecurityToken* and *RequestSecurityTokenResponse* messages to issue security tokens based on an InfoCard;
  - extensions of/restrictions to *WS-Trust* required by CardSpace;
  - expression of security requirements of its STS using *WS-SecurityPolicy*;
  - one or more of the CardSpace authentication mechanisms to allows users to authenticate to its STS.

Relying Party Interactions

- We consider the means used by a Relying Party (RP) to convey to a service requester both:
  - its requirements for security tokens, and
  - its own identity.
- Security policy mechanisms as specified in *WS-SecurityPolicy* are used to indicate the RP token requirements and how messages should be secured.

Identifying the RP – requirements

- When an RP requests verification of a user identity in the form a security token containing claims, the user needs to first reliably identify the RP to make the trust decision.
- This requires conveying RP identity to service requester in a human-friendly ***and*** verifiable manner.

Identifying the RP – recommendations

- CardSpace recommends use of an X.509 v3 certificate for an organisation including:
  - unique subject identifier;
  - logo for organisation.
- Inclusion of a logo (strictly a logotype) helps to simplify human interpretation of certificate content.
- Security tokens sent by the identity selector to the organisation will be encrypted using the public key from the organisation certificate.

Expressing token reqs. of RP

- An RP expresses its token requirements as part of its security policy, using primitives and assertions specified in *WS-SecurityPolicy*.
- The default for an IP is to provide a token generated using symmetric cryptography.
- However, CardSpace recommends use of asymmetric cryptography for tokens.
- This is because it enables the IP to generate a signed token without knowing who the RP is, hence enhancing user privacy.

InfoCards

- An InfoCard represents a single digital identity for a user issued by an IP.
- Multiple identities for the same user (from same IP) would give separate InfoCards.
- The InfoCard is not a security token used to carry identity claims – it simply represents the relationship with the IP.

InfoCard contents

- An InfoCard carries the IP's issuing policy for tokens, including:
  - token types it supports;
  - claim types it handles;
  - the credential to use for user authentication.
- It must contain enough information about the IP's capabilities to allow the identity selector to match it with the RP's token requirements.
- The user can then select a suitable InfoCard from amongst those available.

InfoCard format

- InfoCards are XML documents; can be stored on any user device.
- An InfoCard is not particularly security-sensitive (except that it reveals a relationship between a user and an IP).
- The security-sensitive processes are:
  - user authentication to an IP (using a method specified in CardSpace);
  - generation of tokens by IP and transfer to RP;
  - verification of tokens by RP.

InfoCard example

```
<InfoCard
    xmlns="http://schemas.microsoft.com/ws/2005/05/identity"
    xmlns:wsa="http://schemas.xmlsoap.org/ws/2004/08/addressing"
    xmlns:wsp="http://schemas.xmlsoap.org/ws/2002/12/policy"
    xml:lang="en-us">
  <InfoCardReference>
    <CardId>http://xyz.com/CardId/d795621fa01d454285f9</CardId>
  </InfoCardReference>
  <CardName>XYZ membership card</CardName>
  <CardImage MimeType="image/gif"> ... </CardImage>
  <IssuerName>XYZ Authority</IssuerName>
  <TimeIssued>2003-08-24T00:30:05Z</TimeIssued>
  <TokenServiceReference>
    <TokenService>
      <wsa:EndpointReference>
        <wsa:Address>http://xyz.org/sts</wsa:Address>
        <wsid:Identity>
          <ds:KeyInfo>
            <ds:X509Data>
              <ds:X509Certificate>...</ds:X509Certificate>
            </ds:X509Data>
          </ds:KeyInfo>
        </wsid:Identity>
      </wsa:EndpointReference>
      <UserNamePasswordAuthenticate>
          <Username>Zoe</Username>
      </UserNamePasswordAuthenticate>
    </TokenService>
  </TokenServiceReference>
  <ic:InfoCardPolicy>
    <SupportedTokenTypes>
      <TokenType URI="urn:oasis:names:tc:SAML:1.0:assertion"/>
    </SupportedTokenTypes>
    <SupportedClaims>
      <SupportedClaim URI="http://.../ws/2005/05/identity/claims/givenname">
        <DisplayTag>Given Name</DisplayTag>
      </SupportedClaim>
      <SupportedClaim URI="http://.../ws/2005/05/identity/claims/surname">
        <DisplayTag>Last Name</DisplayTag>
      </SupportedClaim>
    </SupportedClaims>
    <RequireAppliesTo />
  </ic:InfoCardPolicy>
</InfoCard>
```

InfoCard issue

- Issue of InfoCards can use any convenient 'out of band' mechanism, e.g.
  - via HTTP;
  - via email.
- To give user assurance of validity of InfoCard, the InfoCard should be sent with an XML signature generated by the IP.
- X.509 certificates including a logo are recommended to support this signature.

Token requests

- When user selects an InfoCard for use with an RP, the identity selector requests a security token from the IP STS.
- Tokens are requested using the *RequestSecurityToken* message specified in *WS-Trust*.
- The request message includes:
  - unique identifier of InfoCard;
  - (optionally) set of claims to be authenticated;
  - either opaque reference to RP (or actual RP identity if symmetric cryptography being used);
  - (optionally) request for display token to be shown to user;
  - (optionally) type of token.

Token responses

- Tokens are sent back using the *RequestSecurityTokenResponse* message specified in *WS-Trust*.
- The response message is always sent via a confidentiality-protected channel.
- It includes:
  - (optionally) a display token;
  - key management material, e.g. a certificate;
  - the token itself!

Authenticating to the IP

- The InfoCard specifies the type of credential that must be used to authenticate the user to the IP.
- This must take place before any tokens are issued.
- A number of credential types are supported by CardSpace – we look at a few.
- User authentication messages are protected using XML encryption and XML signature.

Username–password authentication

- The IP can require the user to provide a username and password.
- The following credential format for the InfoCard is defined:

```
<ic:UserNamePasswordAuthenticate>
  <ic:Username>xs:string</ic:Username> ?
</ic:UserNamePasswordAuthenticate>
```

- For user convenience the username can be included in the InfoCard, but not the password.

Kerberos-based authentication

- The IP can require the submission of a Kerberos v5 ‘service ticket’.
- The following credential format for the InfoCard is defined:

```
<ic:KerberosV5Authenticate>
  <ic:UserPrincipalName>xs:string</ic:UserPrincipalName> ?
</ic:KerberosV5Authenticate>
```

- The *service principal name* for the IP must be included in the InfoCard, to enable the service requester to get an appropriate Kerberos ticket.

X.509 certificate based authentication

- The IP can require the provision of an X.509 v3 certificate for the user, where the certificate and keys are stored in software.
- The following credential format for the InfoCard is defined:

```
<ic:X509V3Authenticate>
  <ds:X509Data>
    <wsse:KeyIdentifier ValueType="http://docs.oasis-open.org/wss/2004/xx/
oasis-2004xx-wss-soap-message-security-1.1#ThumbprintSHA1">
       xs:base64binary
    </wsse:KeyIdentifier>
  </ds:X509Data>
</ic:X509V3Authenticate>
```

- A key identifier for the certificate is provided, based on a SHA-1 hash of the entire certificate.

Structure of talk

a. Introduction to CardSpace
b. Underlying philosophy
c. The CardSpace architecture
d. Secure interactions
e. Security and privacy issues
f. Possible solutions

Implementing CardSpace

- Identity management is a rapidly developing area.
- CardSpace, if it succeeds, could significantly improve identity security and privacy.
- However, it requires:
  - IPs and RPs to support web service based interactions;
  - user adoption of CardSpace interface, including registering with appropriate IPs.

Sessions in CardSpace

- It is not clear whether a ‘session’ can be established between a user and an IP, to allow multiple tokens to be generated without re-authenticating the user every time (or re-use of a ‘cached’ token).
- Of course, this could work if the identity selector cached user credentials.

A privacy issue

- When using CardSpace, the RP receives potentially sensitive personal information about the user.
- This is because CardSpace permits IPs to make assertions about a range of user attributes, not just identifiers.
- That is, CardSpace covers both identification issues and attribute management.

A user judgement

- Thus, when deciding to go ahead with a CardSpace interaction with an RP, a user is making an important judgement.
- This is based on the user authentication of the RP.
- This is typically based on a public key certificate (however, there may not be any authentication at all).

Problems with user perceptions

- It is a well-known problem that, when using SSL/TLS sessions, many users have no idea of who is being authenticated, and how to check this (i.e. to look at the address bar).
- This could mean that users are easily misled into revealing sensitive personal information to bogus RPs.

Improving browser interfaces

- Microsoft is making major efforts to improve the user experience in Internet Explorer to make matters clearer to users.
- This includes use of ‘high assurance’ certificates and green address bars.
- However, even this is not guaranteed to be effective (recent experimental results support this); moreover, it will be some time before all RPs have high assurance certificates.

A security issue

- The means by which a user authenticates to an IP is not restricted by CardSpace.
- It could be just password based.
- If so, and if the password is compromised, then the consequences could be very serious (it might be possible to impersonate the user to many RPs).

Structure of talk

a. Introduction to CardSpace
b. Underlying philosophy
c. The CardSpace architecture
d. Secure interactions
e. Security and privacy issues
f. Possible solutions

Privacy protection I

- One way in which privacy could be improved would be if the IP's assertions about a user could only be interpreted by an RP which already knew what information about the user is being asserted.
- If the user reveals its relevant attributes to an RP at registration time (a one-off process when the user is likely to be more careful), then the process of making assertions to an RP could be made less privacy-sensitive.

Privacy protection II

- A solution of this type using 'Secured from Identity Theft' (SIT) attributes has recently been proposed.
- Essentially, this means that the RP asserts attributes of a user to an RP in such a way that the RP can only interpret the assertion if it already knows the attributes.
- This reduces the privacy threat.

Reinforcing user authentication I

- The same ‘SIT’ approach can also be used to enhance user authentication.
- The user can only prove the assertion to the RP if it possesses a copy of the attributes being asserted.
- Knowledge of such attributes indirectly authenticates the user.

Reinforcing user authentication II

- It is also possible to build additional user authentication on top of CardSpace ‘proof keys’.
- These proof keys are used to prevent ‘theft’ of assertions.
- That is, the assertion made by an IP will contain an encrypted secret (proof key), and, at the same time, the user will be given a copy of this secret by the IP.
- This secret can be used to prove ownership of an assertion.
- The secret could be partly made up of a long term secret key shared by the user and the IP, providing additional user authentication.

Scope for research

- CardSpace is clearly of very great potential significance, because it is being supported by Microsoft (and the WS interactions are also being used by other parties).
- Hence addressing security and privacy issues remains of very great importance.

Acknowledgements

- The illustrations used in the description of CardSpace have been taken from Microsoft documents.
- The security and privacy issues in CardSpace were identified by Waleed Alrodhan, and are discussed further in:

  W. Alrodhan and C. J. Mitchell, 'Addressing privacy issues in CardSpace', to be presented at: *IAS '07, Third International Symposium on Information Assurance and Security, Manchester, UK, August 2007*.