



vbug

.NET Developer Conference 2007

17th and 18th October 2007
Microsoft Campus, Reading, UK

Cardspace – Authentication Without Passwords
Barry Dorrans, MVP Visual Tools - Security
<http://idunno.org/>



.NET Developer Conference 2007

Agenda

- The Authentication Problem
- The Identity Metasystem
- What is “Information Card”?
- What is “CardSpace”?
- How do I do it?
- Picking apart the message
- Being an STS
- Things to consider
- Resources



.NET Developer Conference 2007

The authentication problem

- Patchwork of identity systems
- Criminalisation of the internet
- Identity systems can be hard, for users and coders



.NET Developer Conference 2007

Agenda

- The Authentication Problem
- The Identity Metasystem
- What is “Information Card”?
- What is “CardSpace”?
- How do I do it?
- Picking apart the message
- Being an STS
- Things to consider
- Resources



.NET Developer Conference 2007

The identity metasystem

- An abstract concept
- The laws of identity
 - User control and consent
 - Limited disclosure for contained use
 - Justifiable parties
 - Directed Identity
 - Pluralism of operators and technologies
 - Human Integration
 - Consistent experience across contexts

.NET Developer Conference 2007

The identity metasystem

- Three roles
 - Subjects
 - Identity Providers
 - Relying Parties
- Claims versus assertions
 - Assertions are for controlled systems
 - Claims need belief

.NET Developer Conference 2007

Agenda

- The Authentication Problem
- The Identity Metasystem
- What is "Information Card"?
- What is "CardSpace"?
- How do I do it?
- Picking apart the message
- Being an STS
- Things to consider
- Resources

NET Developer Conference 2007

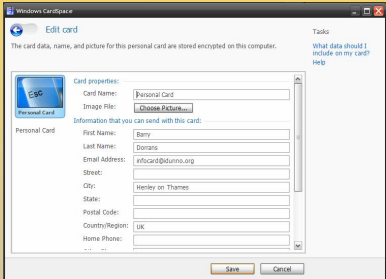
What is Information Card

- "Information Card" is not Passport.
- WSTrust, WS Secure, SAML
- Provides two types of card
 - Self Issued
 - Managed

NET Developer Conference 2007

Self Issued Cards

- User Created
- Phone Book Information




NET Developer Conference 2007

Managed Cards

- Issued by Identity Provider
- No information stored
- Not directly user editable
- Custom Claims
 - Username / Password
 - Smartcard / Certificates
 - Kerberos

NET Developer Conference 2007

Why Cards?



<http://www.microsoft.com/downloads/details.aspx?FamilyID=c99e033-39a8-4bc5-9014-60ed0b560d0e>

NET Developer Conference 2007

Agenda

- The Authentication Problem
- The Identity Metasystem
- What is "Information Card"?
- What is "CardSpace"?
- How do I do it?
- Picking apart the message
- Being an STS
- Things to consider
- Resources

NET Developer Conference 2007

What is CardSpace?

<http://cardspace.netfx3.com/>

“Windows CardSpace is a piece of client software that enables users to provide their digital identity to online services in a simple, secure and trusted way”

NET Developer Conference 2007

What is CardSpace?

- Identity Selector
- Client Software
- Vista, XP, Win2003 with .NET 3.0
- “Consistent experience across contexts”
- Alternatives exist for OS X / Linux; http://www.bandit-project.org/index.php/Digital_Me

NET Developer Conference 2007

Demonstration

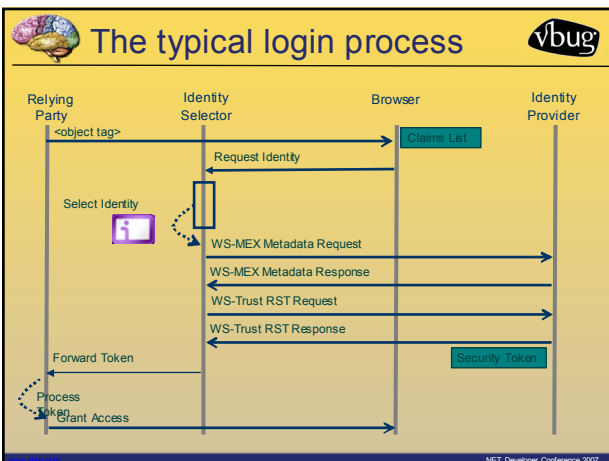
CardSpace? It's this thing

NET Developer Conference 2007

CardSpace Security


- All communications are secured
- Information encrypted in memory
- Dual ACL protection

NET Developer Conference 2007



CardSpace versus OpenID


NET Developer Conference 2007



CardSpace versus OpenID

Identity Cards	OpenID
Clientside prompt	HTML Form
Common Experience	Experience varies
Simpler Login	Redirection / Site Bounce
Requires SSL	Doesn't require SSL


NET Developer Conference 2007



Agenda

- The Authentication Problem
- The Identity Metasystem
- What is "Information Card"?
- What is "CardSpace"?
- How do I do it?
- Picking apart the message
- Being an STS
- Things to consider
- Resources


NET Developer Conference 2007



How do I do it?

- Object tag in HTML page
- SSL Certificate
- Token processing code server side

NET Developer Conference 2007



Why SSL?

- Used to identify relying party
- Tokens encrypted against it
- Revocation lists checked, hard to use self issued certs

NET Developer Conference 2007





In HTML

```

<object type="application/x-informationcard" name="xmlToken">
  <param name="tokenType"
    value="urn:oasis:names:tc:SAML:1.0:assertion" />
  <param name="requiredClaims" value="
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/givenname
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/surname
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/emailaddress"
  />
</object>

```

NET Developer Conference 2007


Demonstration

The HTML Object Tag

NET Developer Conference 2007




SAML




- <http://www.oasis-open.org/>
- Assertion based.
- CardSpace is a SAML 2.0 "Enhanced Client Proxy".

NET Developer Conference 2007




The conversation




- Query MEX EndPoint; get authentication requirements
- Build Asymmetric Keys
- Send RST
- Receive and forward RSTR

NET Developer Conference 2007





The conversation



- Query MEX EndPoint; get authentication requirements
- Build Asymmetric Keys
- Send RST
- Receive and forward RSTR


NET Developer Conference 2007




Demonstration

The token and what it's made of.

NET Developer Conference 2007



Agenda



- The Authentication Problem
- The Identity Metasystem
- What is "Information Card"?
- What is "CardSpace"?
- How do I do it?
- Picking apart the message
- Being an STS
- Things to consider
- Resources

NET Developer Conference 2007



What's in the token



```
<enc:EncryptionMethod
  Algorithm="http://www.w3.org/2001/04/xmlenc#aes256-cbc" />
```

- Shows the token has been encrypted with AES256 CBC
- Symmetric Algorithm
- Both originator and recipient share the key

NET Developer Conference 2007




What's in the token

```
<enc:EncryptionMethod
  Algorithm="http://www.w3.org/2001/04/
  xmlenc#aes256-cbc" />
```

- Shows the token has been encrypted with AES256 CBC
- Symmetric Algorithm
- Both originator and recipient share the key

NET Developer Conference 2007



Where's the token?

```
enc:CipherData>
<enc:CipherValue>
77Ybo3C523ckPMD+1xm9t7KxfgjMTRoJczrDs0i HsxJ306i 3B04RAGr0ivLFqM YzYP41ZxsM2.1F8c Us
aV0TY9Kqs Jjp0Bwyk37n9tw7pv6E3SXkHtKx92x1 5AqmjPeBdDl/syr1Jge1bpb n5sXSPnNoOmAbVS2
Wv12o5ABIqvtoMv1bp16Ns1ImSgxuB074kmAvAUx b/LXPXq1Gwc22YtyaHMYSLV zzzYRuDH9qu0R6748
B/C11F4HeXHUgMPY aEQ+dhuzoU0Muy7/kQVPSckb B0asH5qI.1Jp5B4ve cBe /aGQ09AYNEwPv4xABSc vr
PBE64TcttSlyJknZLcdwNzqmVq1evGMxawwUPgxe D2w==
</enc:CipherValue>
</enc:CipherData>
```

- And that's your SAML token

NET Developer Conference 2007




Token contents

```
<saml:Conditions
  NotBefore="2007-02-01T10:50:06.468Z" NotOnOrAfter="2007-02-01T11:50:06.468Z">
  <saml:AudienceRestrictionCondition>
    <saml:Audience>
      https://www.fabrikam.com/Demos/Reading/signin4.html
    </saml:Audience>
  </saml:AudienceRestrictionCondition>
</saml:Conditions>
```

```
<saml:Attribute AttributeName="givenname"
  AttributeNamespace="http://schemas.xmlsoap.org/ws/2005/05/identity/claims">
  <saml:AttributeValue>Barry</saml:AttributeValue>
</saml:Attribute>
<saml:Attribute AttributeName="privatepersonalidentifier"
  AttributeNamespace="http://schemas.xmlsoap.org/ws/2005/05/identity/claims">
  <saml:AttributeValue>wL6X15ZSuXQn5u40mRbklj5cUkVf02HyASCo8uceNK</saml:AttributeValue>
</saml:Attribute>
```


NET Developer Conference 2007



Standard SAML Claims

Anonymous, Authentication, AuthorizationDecision, Country, DateOfBirth, Dns, Email, Gender, GivenName, Hash, HomePhone, Locality, MobilePhone, Name, NameIdentifier, OtherPhone, PostalCode, PPID, RSA, SID, SPN, StateOrProvince, StreetAddress, Surname, System, Thumbprint, Upn, URI, WebPage, X500DistinguishedName


NET Developer Conference 2007



Uniquely Identifying a Card

- PPID for self issued cards
- Identity Provider Public Key & Unique claim for managed cards

NET Developer Conference 2007



Uniquely Identifying a Card

- PPID for self issued cards
- Identity Provider Public Key & Unique claim for managed cards

NET Developer Conference 2007



Agenda



- The Authentication Problem
- The Identity Metasystem
- What is "Information Card"?
- What is "CardSpace"?
- How do I do it?
- Picking apart the message
- Being an STS
- Things to consider
- Resources

NET Developer Conference 2007



Being a STS



- EV SSL Certificate
- WS-Trust Service
- Card Delivery Mechanism
- Auditing / Non-auditing
- Realms and PPIDs

NET Developer Conference 2007



Agenda



- The Authentication Problem
- The Identity Metasystem
- What is "Information Card"?
- What is "CardSpace"?
- How do I do it?
- Picking apart the message
- Being an STS
- Things to consider
- Resources

NET Developer Conference 2007



Things to consider



- Validation of claims
- How much do you trust a card issuer?

NET Developer Conference 2007



Agenda



- The Authentication Problem
- The Identity Metasystem
- What is "Information Card"?
- What is "CardSpace"?
- How do I do it?
- Picking apart the message
- Being an STS
- Things to consider
- Resources

NET Developer Conference 2007



Resources



- Microsoft provide
 - Client Side Kit
 - ASP.NET Kit
- ASP.NET Kit
<http://go.microsoft.com/fwlink/?LinkId=89183>
- ASP.NET Control
<http://www.leastprivilege.com>
- Ruby
<http://www.codeplex.com/informationcardruby>
- Java
<http://www.codeplex.com/informationcardjava>

NET Developer Conference 2007



Blogs



- Kim Cameron
<http://identityblog.com>
- Vittorio Bertocci
<http://blogs.msdn.com/vbertocci>
- Garrett Serack
<http://fearthecowboy.com>
- CardSpace Team Blog
<http://blogs.msdn.com/card/>

NET Developer Conference 2007



Identity Providers



- OpenID & Information Cards
<http://www.signon.com/>
- Live Labs Beta STS
<https://sts.labs.live.com/gettingstarted.aspx>
- Verisign
<https://pip.verisignlabs.com/>

NET Developer Conference 2007



Agenda



- The Authentication Problem
- The Identity Metasystem
- What is "Information Card"?
- What is "CardSpace"?
- How do I do it?
- Picking apart the message
- Being an STS
- Things to consider
- Resources

NET Developer Conference 2007



Questions



"Now, with the debut of the Info-Card identity management system, Microsoft is leading a network-wide effort to address the issue. To those of us long skeptical of the technology giant's intentions, the plan seems too good to be true. Yet the solution is not only right, it could be the most important contribution to Internet security since cryptography."

Lawrence Lessig, Wired Magazine, March 2006.

NET Developer Conference 2007