Modern Identity

Scott Reed

Brain Hz Software

scott@brainhzsoftware.com

(760) 845-3320

Security in the Wild

- **Detection and Prevention**
  - **Authentication**
  - **Authorization**
  - **Auditing**

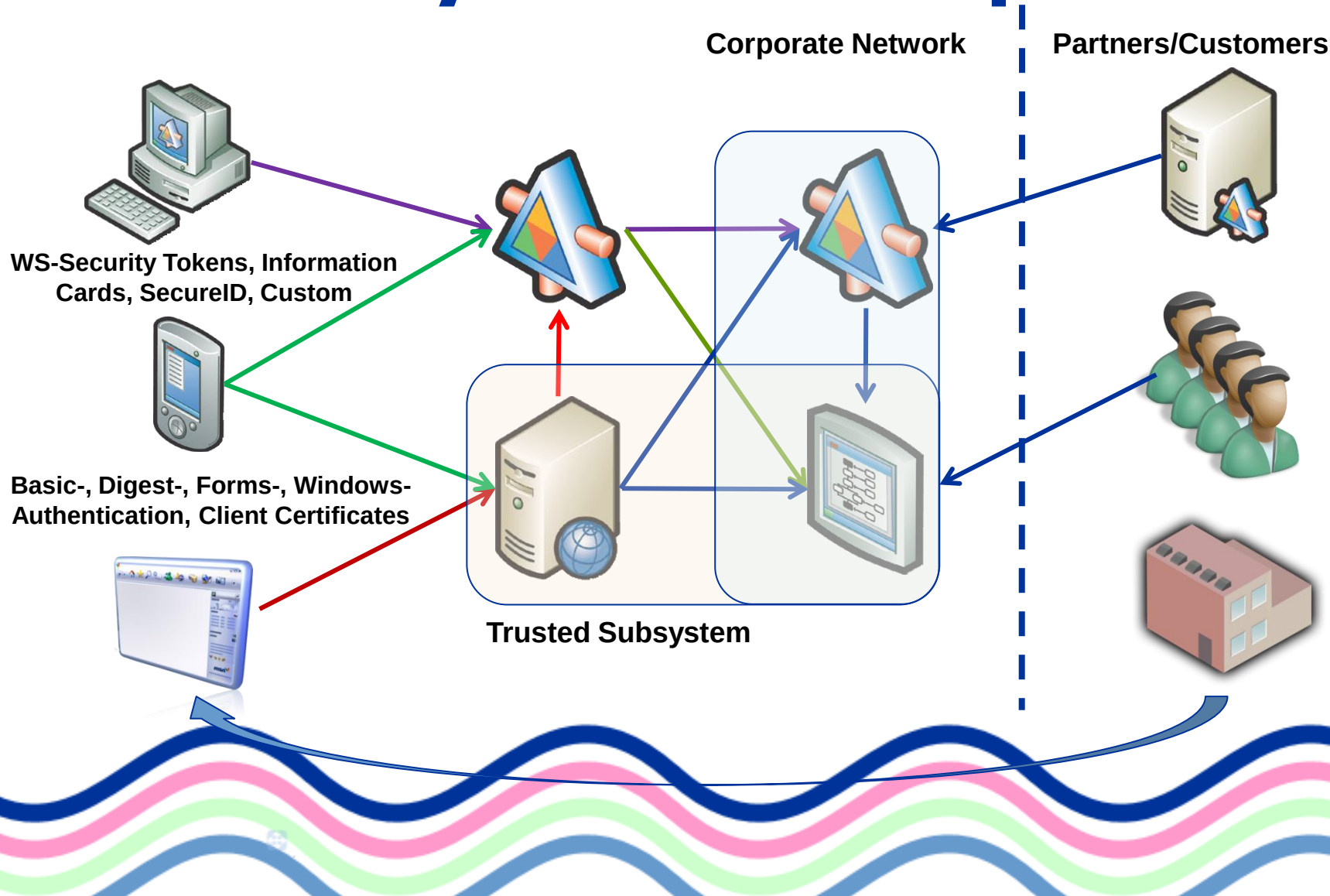
Security on the Wire

- **Confidentiality**
- **Integrity**
- **Authentication**

Authentication (the Common link)

- To establish identity:
  - What do you have?
    - Certificate, Token
  - What do you know?
    - Password
  - What are you made of?
    - Fingerprint, retinal scan
  - Multifaceted
    - Smart card (cert and pin)
  - Client, Server, or Mutual

Identity in the Enterprise



Problems with Enterprise Identity

- Need richer identity information
- Want to support single sign-on
- Enable third party authentication
- Support identity delegation
- Roles are not flexible enough
- Need to be able to federate identities

Problems with Internet Identity

- Has no identity system built-in
- SSL, Forms based, creating identity silos
- Phishing and pharming becoming more prevalent
- Violating the Laws of identity

Problems with token formats

- **Username/Password**
  - **Least secure, least information**
- **X.509**
  - **Thumbprint, Common name not enough**
- **Kerberos**
  - **Name and groups**

Digital Identities and Claims

- **Digital Identities**
  - ***a set of claims made by one digital subject about itself or another digital subject***
- **Claim**
  - **An assertion of the truth of something, typically *one which is disputed or in doubt.***

Example Claims

- **Identifiers such as Student number = 490-525, or Windows name = BRAINHZ\sreed**
- **Assert that a subject knows a given key**
- **Personally identifying information like email, address, date of birth, citizenship**
- **Part of a certain group like People over 21, or Premium member.**
- **Capability to place orders up to a certain limit or modify a given file.**

Where do Claims come from?

- Shredded from other token types
- Transformed locally
  - Like GenericIdentity
- Sent from third party

Active Demo

Claims Transformation Demo

Where do claims come from?

- Security Token Service (STS)
- WS-Trust is the contract
  - Issue, Renew, Cancel, and Validate
- Tokens are claims based and extensible
  - Security Assertion Markup Language (SAML) most likely
- Signed and then encrypted for target service

How/where do I get an STS?

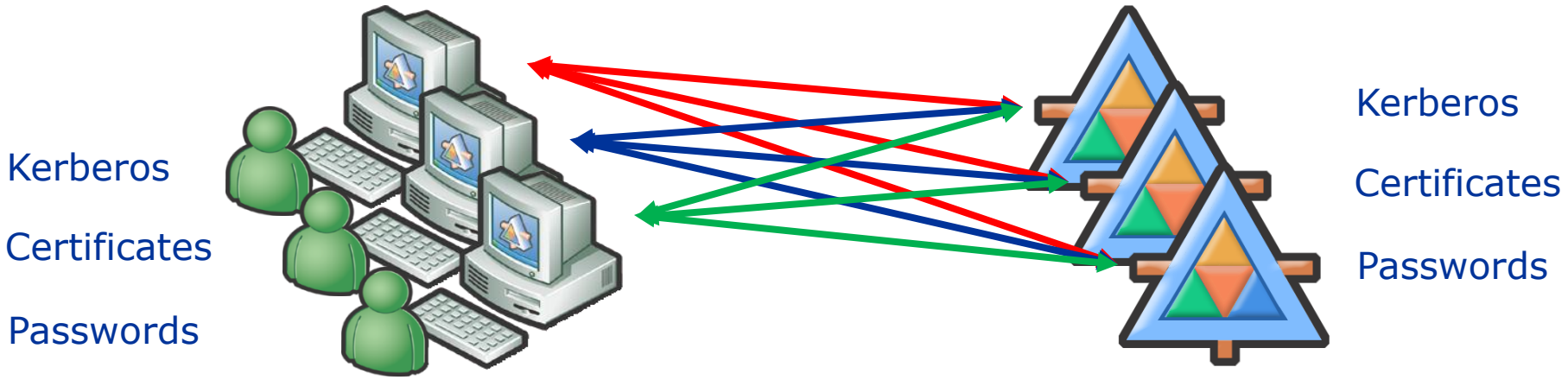
- STS products
  - Microsoft ADFS / "Geneva" Server
  - comparable offerings by IBM, CA, Oracle, SUN…
  - usually tightly coupled with a specific user directory
- STS as a service
  - .NET Services Access Control Service
  - Resource STS in the cloud
- Write your own STS
  - full flexibility, generally discouraged
  - made easier by the Geneva framework

ADFS

- ADFS 1.x
  - part of Windows Server 2003/2008
  - STS with AD as a backing store
  - provides applications with SAML tokens for domain users
  - allows cross organization trust with WS-Federation
- ADFS 2 (a.k.a. ”Geneva” Server)
  - all of the above plus
    - WS-Trust
    - SAML 2.0
    - Information Cards

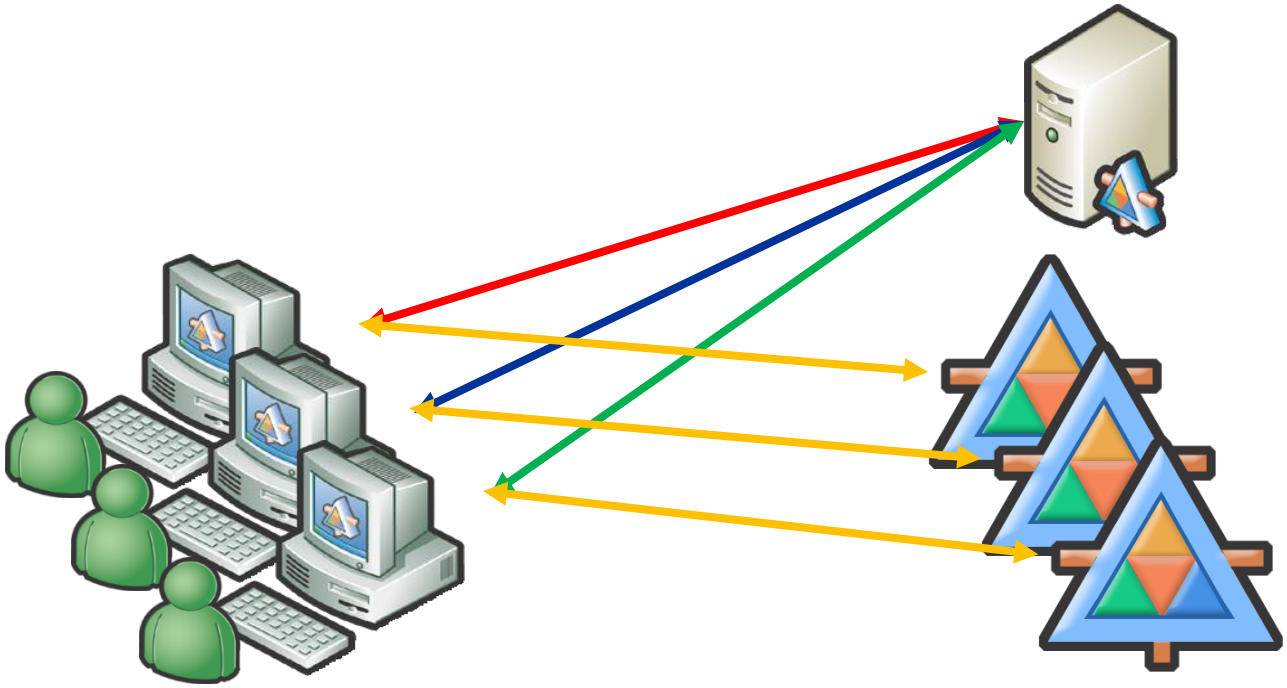
Active Clients

- **WCF Security: Choose mode, client credential type, then each side specifies their own credentials and how to authenticate the other side**



Active Client with STS

- **Designed to centralize the authentication**



Passive Client with STS

3: authentication
4: claims transformation
5: render form to post token

2: GET /sts/auth.aspx

```
<form method="POST" action="http://app/default.aspx">
  <input name="wresult" value="[token]" />
  …
  <script >
      window.setTimeout('document.forms[0].submit()', 0);
  </script>
</form>
```

1: GET /default.aspx

6: POST /default.aspx

7: turn token into cookie(s)
8: create ClaimsPrincipal

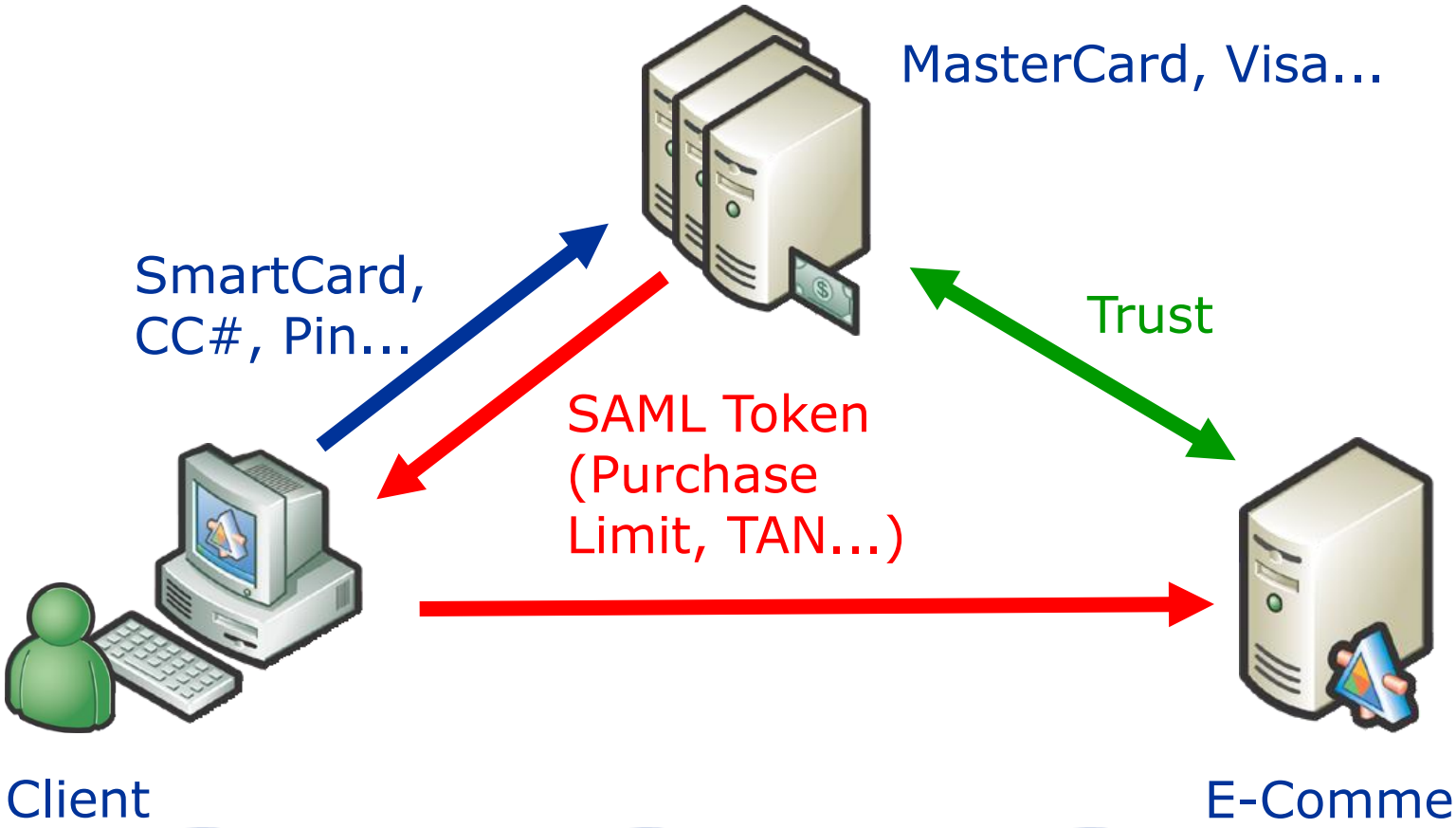
Web Single Sign On

- **WS-Federation Passive Profile**
  - **Covered on previous slide**
- **SAML Web Browser SSO Profile**
- **OpenID**
  - **Web only**
  - **Identity is in the form of a URL**
  - ***OpenID leads to Information Cards***

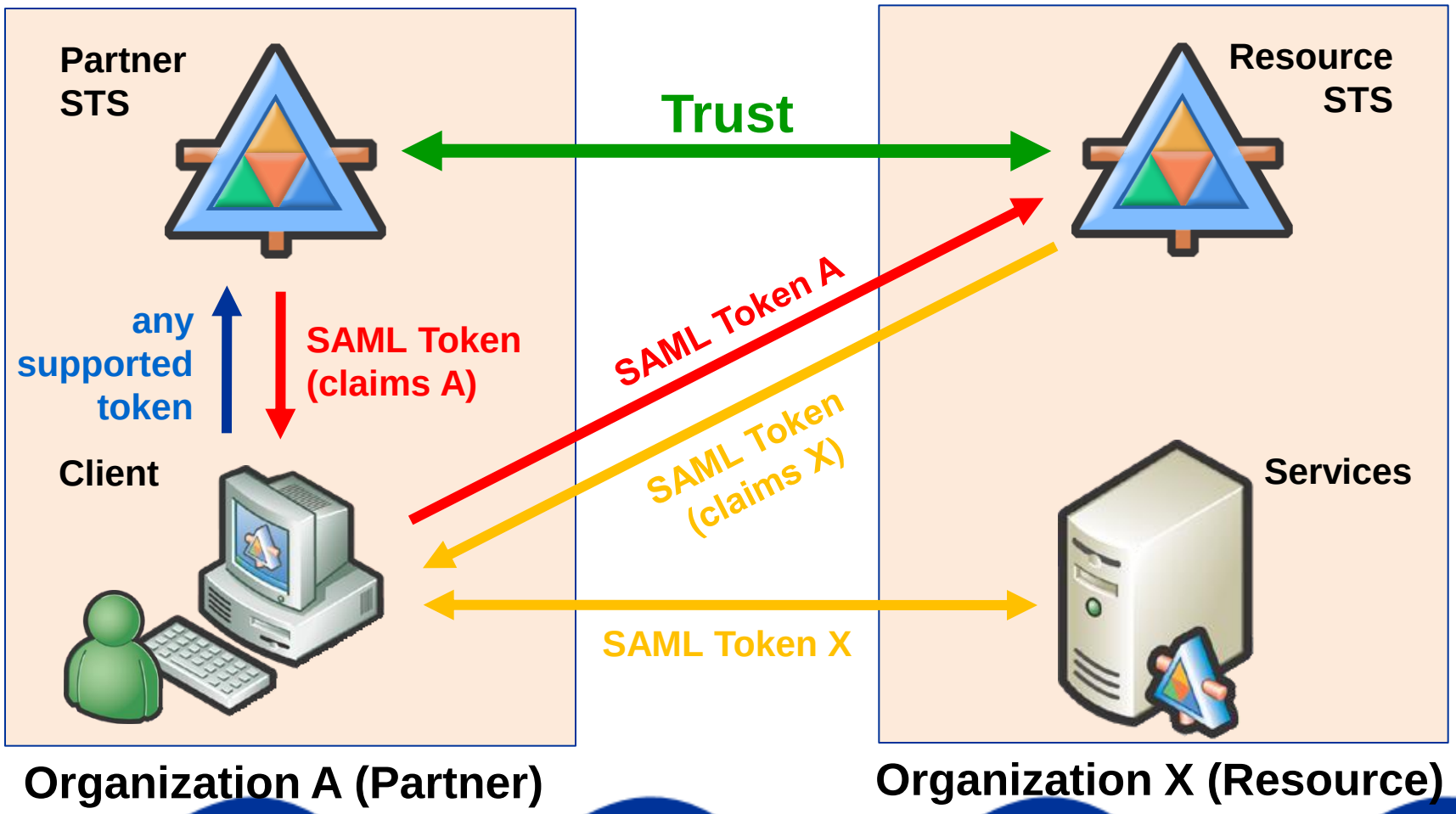
Terminology

- **May be multiple STSs**
  - ***Identity provider* issues first token/claims**
  - ***Resource STS* does token transformation**
- ***Relying party* is the service or site using the identity**
- ***Identity selector* is the client side piece that helps users choose which tokens and STSs to use**

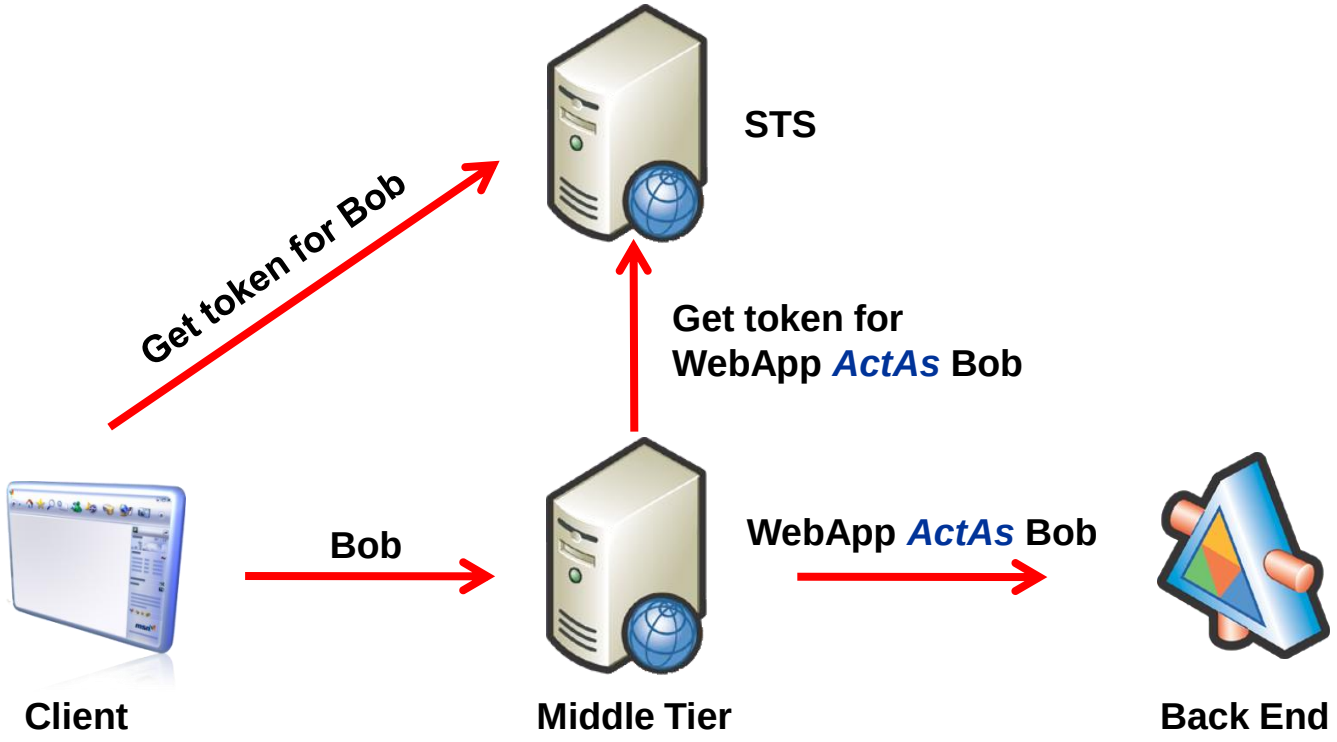
What else can an STS do?



Federation


Partner STS
Trust
Resource STS
any supported token
SAML Token (claims A)
SAML Token A
SAML Token (claims X)
Client
Services
SAML Token X
Organization A (Partner)
Organization X (Resource)

Identity Delegation



Information Cards

- Graphical representation of
  - Claim requirements
  - WS-Trust, WS-Federation details
- Two types of cards
  - self issued
  - Managed
- Reduces password memorization
- More robust against phishing

Identity Selectors

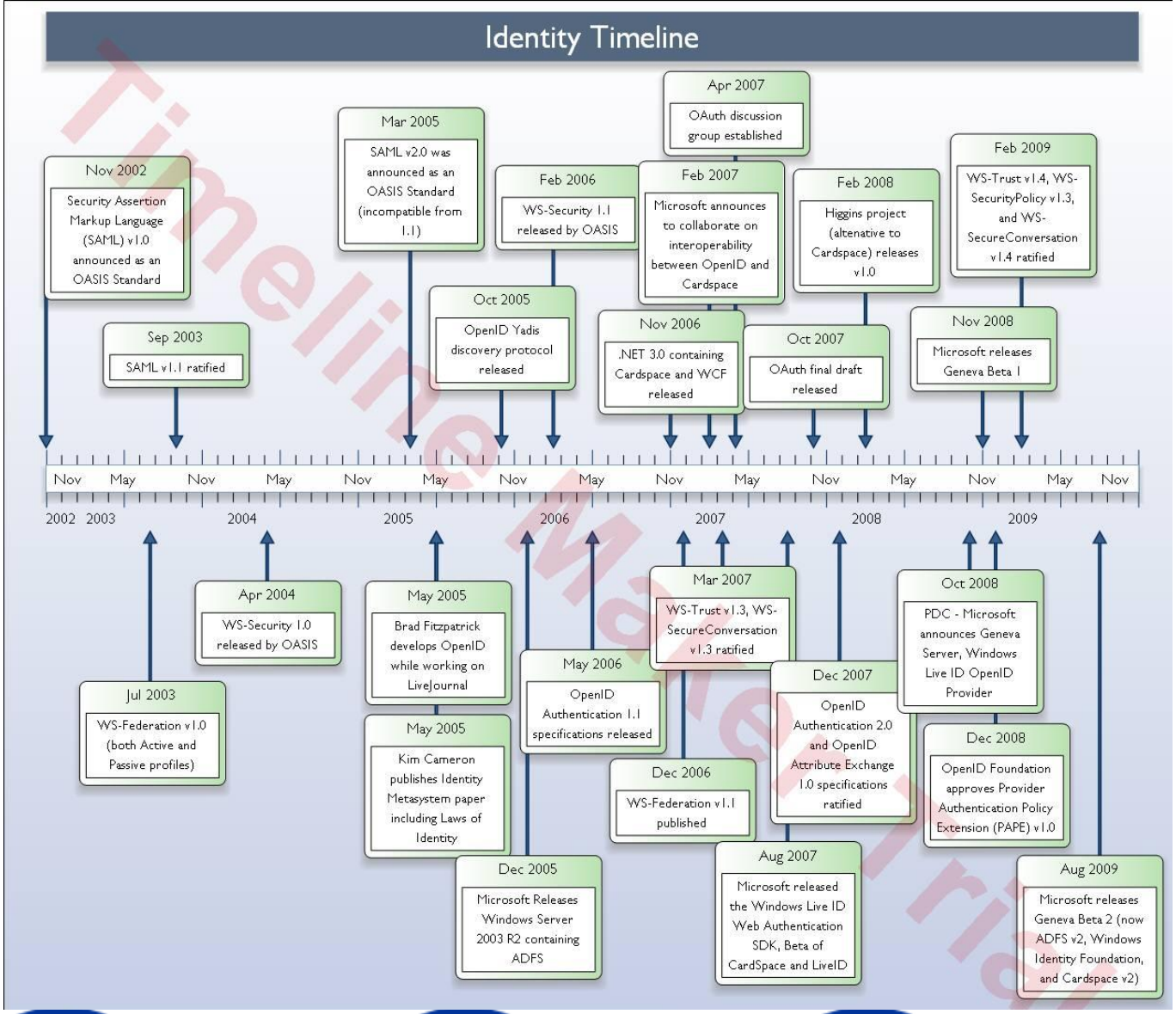
- Cardspace
  - Ships with .NET 3.0 and Vista and later
  - New version shipping with Geneva
- Digital Me (Bandit)
  - Developed by Novell for Mac/Linux
- Higgins project
  - First released Feb 2008

Credit Card Security

- No “good” solution, yet
- 3-D Secure
  - Verified by Visa
  - Mastercard SecureCode
  - JCB J/Secure
- Ideal would be to use a managed information card

OAuth

- OAuth
  - Not an authentication protocol
  - An Authorization delegation protocol
  - Used when a user wants to share resources from one web site to another


Identity Timeline
Nov 2002
Security Assertion Markup Language (SAML) v1.0 announced as an OASIS Standard
Sep 2003
SAML v1.1 ratified
Mar 2005
SAML v2.0 was announced as an OASIS Standard (incompatible from 1.1)
Oct 2005
OpenID Yadis discovery protocol released
Feb 2006
WS-Security 1.1 released by OASIS
Apr 2007
OAuth discussion group established
Feb 2007
Microsoft announces to collaborate on interoperability between OpenID and Cardspace
Nov 2006
.NET 3.0 containing Cardspace and WCF released
Oct 2007
OAuth final draft released
Feb 2008
Higgins project (altenative to Cardspace) releases v1.0
Feb 2009
WS-Trust v1.4, WS-SecurityPolicy v1.3, and WS-SecureConversation v1.4 ratified
Nov 2008
Microsoft releases Geneva Beta 1
Nov May Nov May Nov May Nov May Nov May Nov May Nov May Nov May Nov
2002 2003 2004 2005 2006 2007 2008 2009
Jul 2003
WS-Federation v1.0 (both Active and Passive profiles)
Apr 2004
WS-Security 1.0 released by OASIS
May 2005
Brad Fitzpatrick develops OpenID while working on LiveJournal
May 2005
Kim Cameron publishes Identity Metasystem paper including Laws of Identity
Dec 2005
Microsoft Releases Windows Server 2003 R2 containing ADFS
May 2006
OpenID Authentication 1.1 specifications released
Dec 2006
WS-Federation v1.1 published
Mar 2007
WS-Trust v1.3, WS-SecureConversation v1.3 ratified
Aug 2007
Microsoft released the Windows Live ID Web Authentication SDK, Beta of CardSpace and LiveID
Dec 2007
OpenID Authentication 2.0 and OpenID Attribute Exchange 1.0 specifications ratified
Oct 2008
PDC - Microsoft announces Geneva Server, Windows Live ID OpenID Provider
Dec 2008
OpenID Foundation approves Provider Authentication Policy Extension (PAPE) v1.0
Aug 2009
Microsoft releases Geneva Beta 2 (now ADFS v2, Windows Identity Foundation, and Cardspace v2)

Alphabet Soup (Quiz)

- Token Format
- Framework
- Protocol
- Identity Selector
- Identity Provider
- Resource STS
- .NET ACS
- ADFS
- Cardspace
- DigitalMe
- Geneva
- Higgins project
- Kerberos
- LiveID
- OpenID
- OAuth
- SAML
- STS
- WS-Security
- WS-Trust
- WS-Federation
- X.509

Call to action

- Enterprise
  - Support single sign on
  - Allow partners to access your sites/services
- Internet
  - Don’t store passwords
    - Instead support third party authentication
  - Don‘t store credit card information
    - Instead support information cards or 3D secure

Resources

- http://identity-des.com/
- http://www.identityblog.com/
  - In particular the video: “Why OpenID leads to Information Cards”
- http://www.leastprivilege.com/
- Others
  - http://www.identity20.com/media/OSCON2005/

Thank You

Scott Reed

Brain Hz Software

scott@brainhzsoftware.com

(760) 845-3320