

RETS Security Working Group Report (partial)

Peter Williams

## *What We'll Cover:*



## ***What We'll Cover:***

- .NET support for RETS  
programmers  
implementing the security tokens
- Extending .NET platform ...  
for “MLS” Federations with Title and Mortgage
- What is this “SAML” stuff in  
RETS2.....  
for .NET systems?

## *What We'll Cover (2)*

- How do vendors compete when adding-value... using RETS2 extensions?
  - “Vendor-defined” web services for provisioning security systems (e.g. Microsoft .NET SAML, .NET2 Roles, .NET2 Members, COM+ RBAC)
  - “Vendor-Right” to “add” wsdl, and “specify” xsd types for payloads?
  - Secure Payloads, with Distributed Data Management (DRM) e.g. OASIS XrML wrappers for payloads, from Microsoft Rights Management libraries?

# Which security tokens?

1. Username – password
2. Digital Certificates
3. SAML Tokens
  1. For application SSO
  2. For Federated SSO
  3. For Sessions



# ■ Certificate Signing!

- Do you! use them? For signing emails, and logging on to websites?
- How many of you PGP encrypt your files, or your entire desktop file system?
- So why is this token in our standard?
  - “For the future”? (12 years on PKI, and still counting...)
  - “Because its there?”
- But, at least we understand
  - The “little” transaction gets “rather bigger”, with 11k certs chains, EACH TIME!
  - The whole transaction is “signed” (using RSA) and keys

# ■ UserName/Passwords

- Two issues came up
  - 1. Is the user/password token sent each time (unlike a RETS1 login session?)
  - 2. does the token “sign” the transaction, using a hash?
  
  - .NET1.1 WS-\* toolkits (WSE1) doesn't support RETS security standards
  - The WSEv2 (SP2) seems to do (simple) RETS: we can send a username/password, now !!
  
  - So, huge transactions, come back down to small size streams.
  - But, we lose integrity, and signing. Are we assuming SSL?

Then there this the issue of sessions! (which gets back to signing!)

## ■ UserName/Passwords

- In Web services, client proxies can store HTTP cookies
  - Do web services just use HTTP1.1 keep-alive and cookies!!?
  - If cookies, then can we just use traditional SSO cookies?
  - But isnt web services stateless!!
- Reality of products, vs spec.
  - Real products have (client) state.
  - Traditional ASP.NET proxies have cookie-container support
  - Webservices products may be CO-RESIDENT with web apps (e.g. RETS + Rapattoni Data Manager).
- Real Microsoft proxies (with WSE3) used special SAML tokens
  - WS-SecureConversation creates a “session key” after initial login.
  - Subsequent transactions are “signed” using those keys – security context
  - Basically, SSL at the XML layer. Rather than SSL sessions...WS-SC sessions!
- Hmm. .... Passwords ....related now to SAML... and back to signing.

# ■ UserName/Passwords - Roles

- Role-based Access Control is a new feature
- Playing with .NET <-> Java toolkits, we experimented (on Windows)
- 1. Java Class, wrapped as a .NET components, in a TCP/IP listener
  - Soap listener, but not RETS compliant – uses SOAP-RPC encoding.
- 2. Java Class, under Microsoft SOAP toolkit in Component Services App Services
  - Added full role-based access control, per method, per interface
  - Full pooled class loaders, for data center engineering
  - But, still not complying
- 3. Component Services app services now hosted by IIS and ASP.NET
  - Nicely WS-I compatible, for same Java Class!
  - Also, ASP.NET hosts the WSE pipeline, which adds the WS-Security support mentioned earlier
- So...we have a Java compiled classes implement RETSs, with .NET Web Services support.

# ■ SAML

- We built a Microsoft Quickstart sample
  - Using WS-Trust request/responses, issue a SAML token
  - Full source code provided, in MS style
  - Doesn't use RSA or OpenSAML libraries
- For single sign on to applications and federations:
  - We deployed Windows 2003 RC2
    - Installed Microsoft Active Directory Federation Service (using an LDAP directory)
    - Played with IIS plugin, that uses ADFS to do SSO using SAML
  - We deployed Shibboleth IdP and RdP from Internet2 project
    - Another SSO scheme, aligned with SAML1.1 and the Liberty ID-FF profile of SAML
  - We rebuilt Shibolleth with the “interworking module” for ADFS!
    - i.e. ADFS could operate in “non-Microsoft” mode
  - We deployed the Ping Federation Server – another ADFS extension

## ■ Servlets and J2EE

- Avoided J2EE, limited work to servlet containers, to avoid platform-specific security models (Beans, Java Queuing, etc)
- Succeeded to deploy the Apache WS-Security libraries
- Deployed .wars and .jsp web services onto the FIPS 140-1 level 3 secure server from Rainbow,
  - with full cryptographic hardware acceleration
  - Highly locked down servlet engine, suitable for VERY sensitive signing, e.g. WS-Trust STS
  - Can run any .war application, e.g. RSA servers, but cannot deploy additional Linux packages, or use file system
- Deployed opensaml libraries
  - Simple ant-build
  - SAML 1.1 and SAML2? token formats
  - Contrasted this class library with MS SAML classes, and MS Quickstart
- Went through the RETS1.5 sample code (finally) for MySQL
- Rebuilt the Rapattoni Secure Logon web services (tokencode validation) as a servlets, for the Rainbow Crypto box, with full KSD-64 arming

# ■ RSA OTPS community standards

- More than tokens....doing password generation
- OTPS series of standards, targeting all RSA (n,000) business partners
  - Provisioning the tokens with keys, in the field
  - OTPS-PKCS#11 – crypto middleware for accessing “connected tokens” – e.g. GSA smartcards and DoD COTS medium assurance office systems
  - OTP-PEAP – yet another EAP extension for L2TP and IPSec stacks
  
  - OTP-WSS-Token
    - Perhaps don't use the standard UserNameToken for one time passwords, use RSA's token?
    - Issue of patents (beware weasel words)
    - Issue of open source
    - Issue of licensing fees for toolkits
    - Status in OASIS, since 2005?

# *Conclusions*

- **Spec well aligned with various toolkits**
  - Major SUN, IBM, Microsoft support
  - Open source Apache libraries
  - Internet2 opensaml and Shibboleth
  - Microsoft pipelined WSE libraries, for http.sys-based servers (and IIS)
  - Microsoft ADFS and WS-Secure Conversation sessions
  - RSA servers “ClearTrust and FIM” in XML router hardware from third-parties, for data centers
  
- Good evidence for viability of Security Roadmap
  
- **Spec is very incomplete security model, re industry expectations for Data Management – industry need to control the repurposing of data.**