New and Improved!

SAML, OAUTH, and Session sharing in Domino 9

Andrew Pollack
Northern Collaborative Technologies

Andrew Pollack, Northern Collaborative Technologies

- Administrator & Developer since version 2
- Products
  - NCT Search
  - NCT Compliance Search
  - NCT Simple Sign On
  - NCT SAML SSO
- Services
  - Site Performance Reviews
  - Application Development
  - Administrative Overhaul
  - Security Review & Penetration Testing
  - Expert Witness Services
- IBM Lotus Beacon Award Winner
- Structural Firefighter – Cumberland, Maine

SSO & Shared Authentication Topics

- SSO vs. Shared Authentication
- Use Cases
  - Why not just use LTPA or Active Directory?
- Specific Concerns
  - What to consider when planning
- Creating your own simple specification
- Emerging Standards
  - SAML (Security Assertion Markup Language)
  - OpenID
  - OAuth
- Setting up Domino for SAML
- A Real World Example

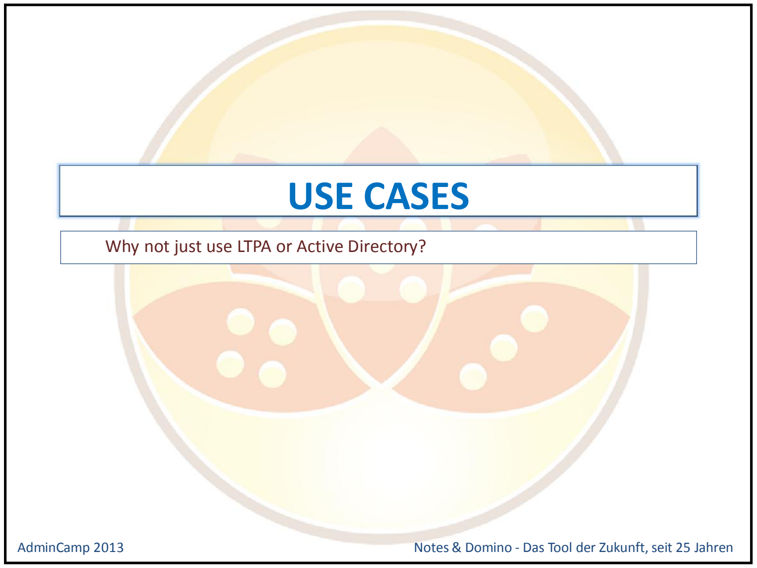
SSO vs. Shared Creds - What's the Difference?

Single Sign On

- Enter Credentials Once and you are signed in at multiple sites
- Wikipedia lists dozens of projects
  - http://bit.ly/WRaxPq

Shared Authentication

- May need to re-enter the same credentials at each site
  - LDAP
  - Domino HTTP Password Sync with Notes ID

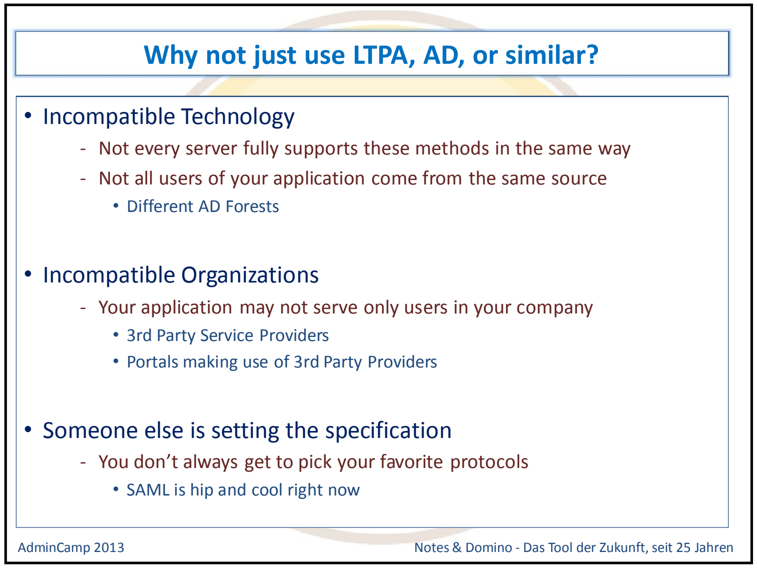


USE CASES

Why not just use LTPA or Active Directory?

AdminCamp 2013

Notes & Domino - Das Tool der Zukunft, seit 25 Jahren

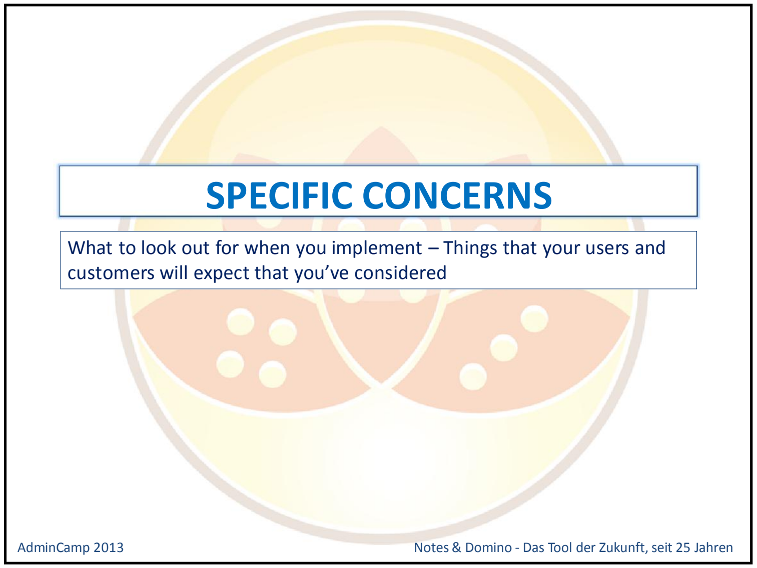


Why not just use LTPA, AD, or similar?

- Incompatible Technology
  - Not every server fully supports these methods in the same way
  - Not all users of your application come from the same source
    - Different AD Forests
- Incompatible Organizations
  - Your application may not serve only users in your company
    - 3rd Party Service Providers
    - Portals making use of 3rd Party Providers
- Someone else is setting the specification
  - You don’t always get to pick your favorite protocols
    - SAML is hip and cool right now

AdminCamp 2013

Notes & Domino - Das Tool der Zukunft, seit 25 Jahren

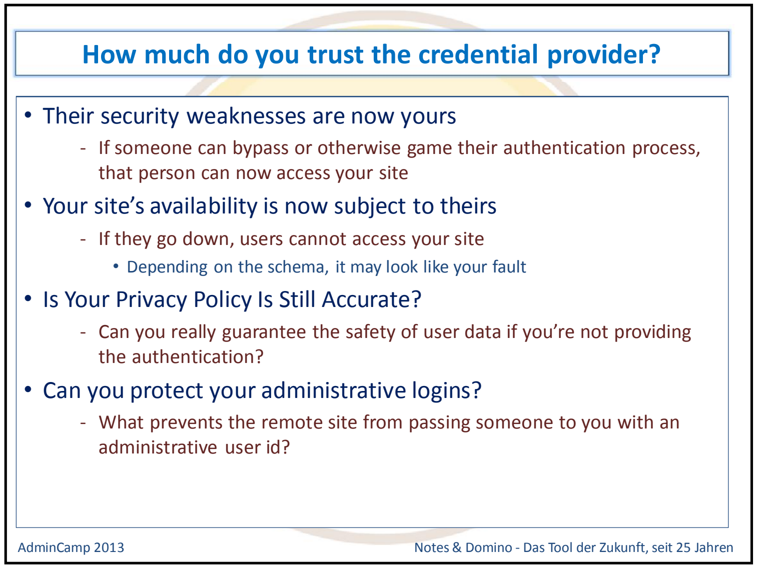


SPECIFIC CONCERNS

What to look out for when you implement – Things that your users and customers will expect that you’ve considered

AdminCamp 2013

Notes & Domino - Das Tool der Zukunft, seit 25 Jahren

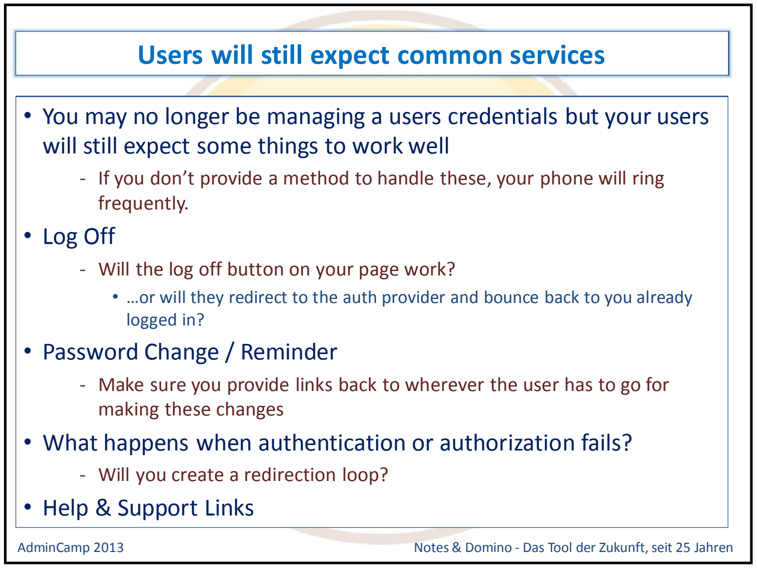


How much do you trust the credential provider?

- Their security weaknesses are now yours
  - If someone can bypass or otherwise game their authentication process, that person can now access your site
- Your site’s availability is now subject to theirs
  - If they go down, users cannot access your site
    - Depending on the schema, it may look like your fault
- Is Your Privacy Policy Is Still Accurate?
  - Can you really guarantee the safety of user data if you’re not providing the authentication?
- Can you protect your administrative logins?
  - What prevents the remote site from passing someone to you with an administrative user id?

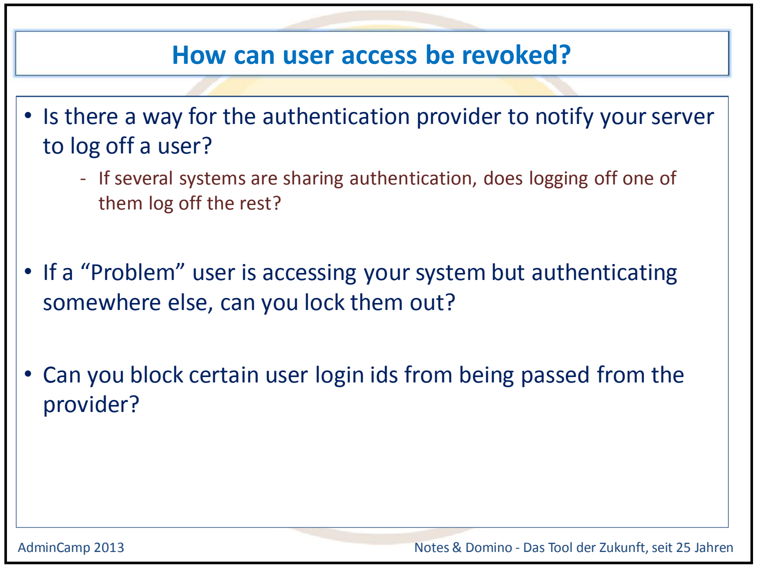
AdminCamp 2013

Notes & Domino - Das Tool der Zukunft, seit 25 Jahren



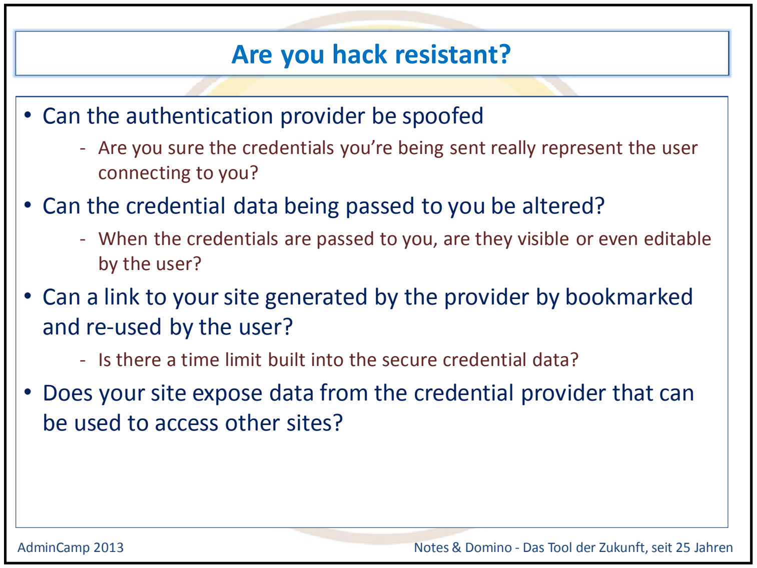
Users will still expect common services

- You may no longer be managing a users credentials but your users will still expect some things to work well
  - If you don’t provide a method to handle these, your phone will ring frequently.
- Log Off
  - Will the log off button on your page work?
    - …or will they redirect to the auth provider and bounce back to you already logged in?
- Password Change / Reminder
  - Make sure you provide links back to wherever the user has to go for making these changes
- What happens when authentication or authorization fails?
  - Will you create a redirection loop?
- Help & Support Links



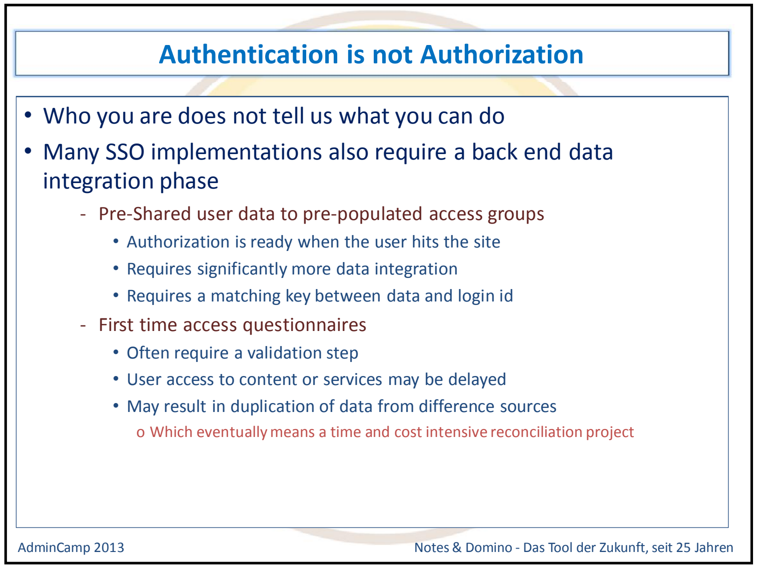
How can user access be revoked?

- Is there a way for the authentication provider to notify your server to log off a user?
  - If several systems are sharing authentication, does logging off one of them log off the rest?
- If a “Problem” user is accessing your system but authenticating somewhere else, can you lock them out?
- Can you block certain user login ids from being passed from the provider?



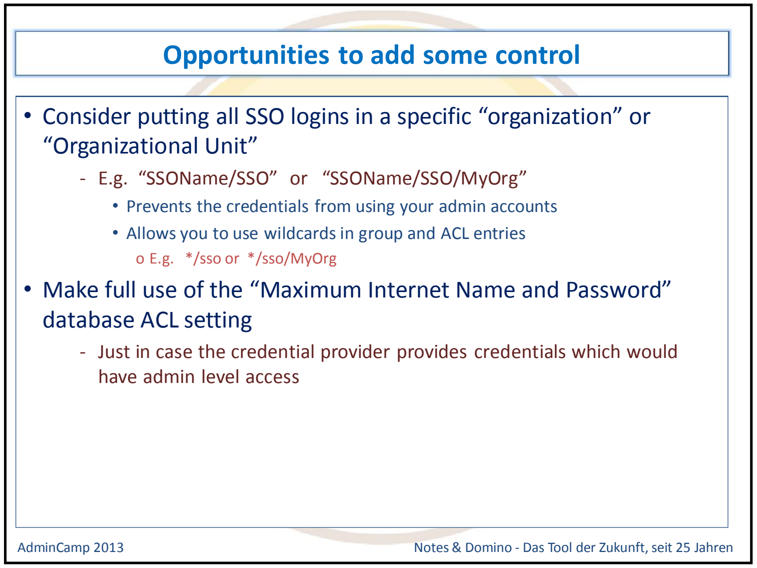
Are you hack resistant?

- Can the authentication provider be spoofed
  - Are you sure the credentials you’re being sent really represent the user connecting to you?
- Can the credential data being passed to you be altered?
  - When the credentials are passed to you, are they visible or even editable by the user?
- Can a link to your site generated by the provider by bookmarked and re-used by the user?
  - Is there a time limit built into the secure credential data?
- Does your site expose data from the credential provider that can be used to access other sites?



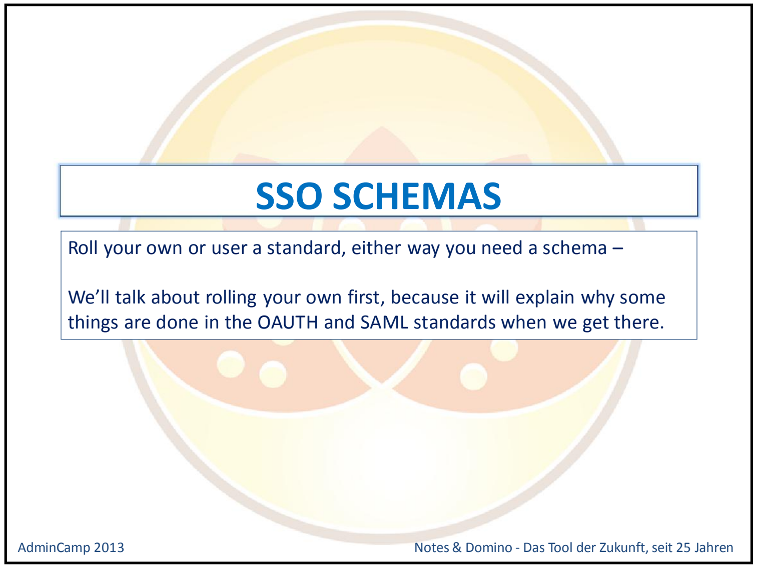
Authentication is not Authorization

- Who you are does not tell us what you can do
- Many SSO implementations also require a back end data integration phase
  - Pre-Shared user data to pre-populated access groups
    - Authorization is ready when the user hits the site
    - Requires significantly more data integration
    - Requires a matching key between data and login id
  - First time access questionnaires
    - Often require a validation step
    - User access to content or services may be delayed
    - May result in duplication of data from difference sources
      - o Which eventually means a time and cost intensive reconciliation project



Opportunities to add some control

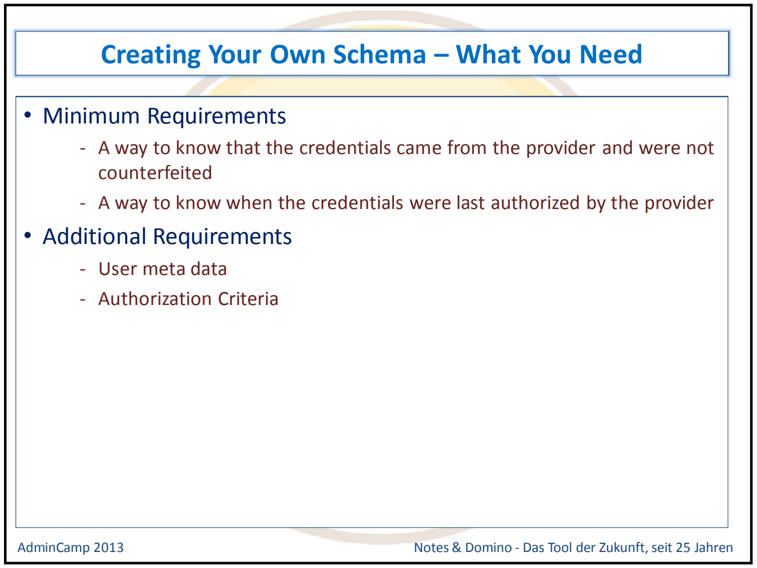
- Consider putting all SSO logins in a specific “organization” or “Organizational Unit”
  - E.g. “SSOName/SSO” or “SSOName/SSO/MyOrg”
    - Prevents the credentials from using your admin accounts
    - Allows you to use wildcards in group and ACL entries
      - o E.g. */sso or */sso/MyOrg
- Make full use of the “Maximum Internet Name and Password” database ACL setting
  - Just in case the credential provider provides credentials which would have admin level access



SSO SCHEMAS

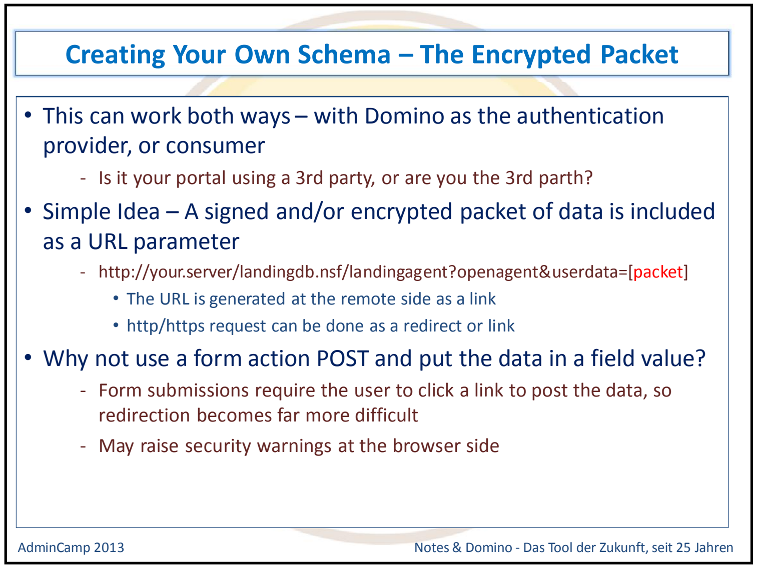
Roll your own or user a standard, either way you need a schema –

We’ll talk about rolling your own first, because it will explain why some things are done in the OAUTH and SAML standards when we get there.



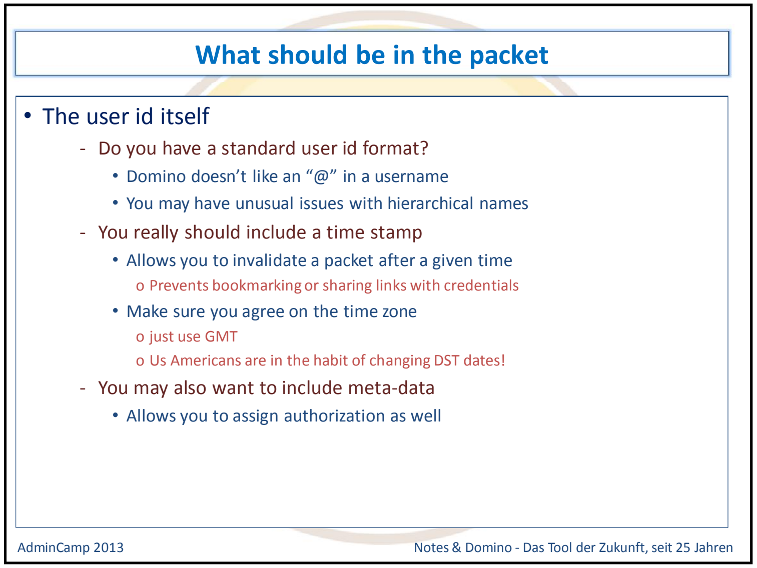
Creating Your Own Schema – What You Need

- Minimum Requirements
  - A way to know that the credentials came from the provider and were not counterfeited
  - A way to know when the credentials were last authorized by the provider
- Additional Requirements
  - User meta data
  - Authorization Criteria



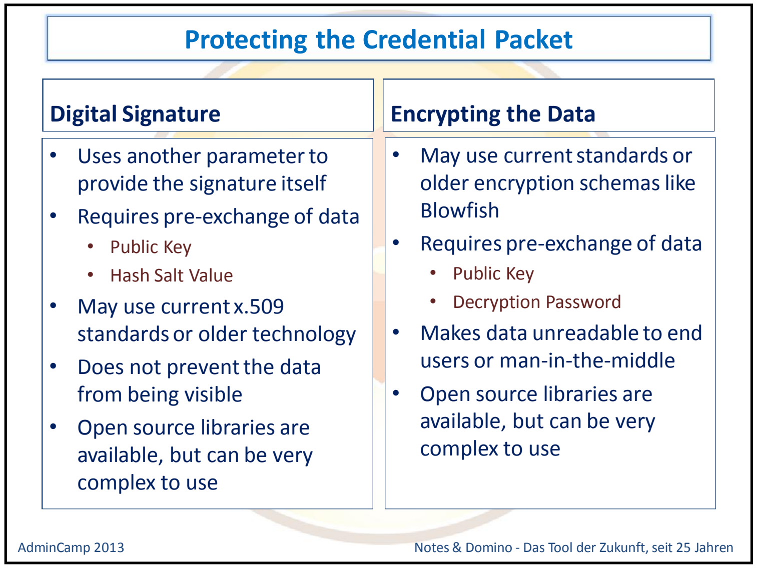
Creating Your Own Schema – The Encrypted Packet

- This can work both ways – with Domino as the authentication provider, or consumer
  - Is it your portal using a 3rd party, or are you the 3rd parth?
- Simple Idea – A signed and/or encrypted packet of data is included as a URL parameter
  - http://your.server/landingdb.nsf/landingagent?openagent&userdata=[packet]
    - The URL is generated at the remote side as a link
    - http/https request can be done as a redirect or link
- Why not use a form action POST and put the data in a field value?
  - Form submissions require the user to click a link to post the data, so redirection becomes far more difficult
  - May raise security warnings at the browser side



What should be in the packet

- The user id itself
  - Do you have a standard user id format?
    - Domino doesn't like an "@" in a username
    - You may have unusual issues with hierarchical names
  - You really should include a time stamp
    - Allows you to invalidate a packet after a given time
      - o Prevents bookmarking or sharing links with credentials
    - Make sure you agree on the time zone
      - o just use GMT
      - o Us Americans are in the habit of changing DST dates!
  - You may also want to include meta-data
    - Allows you to assign authorization as well



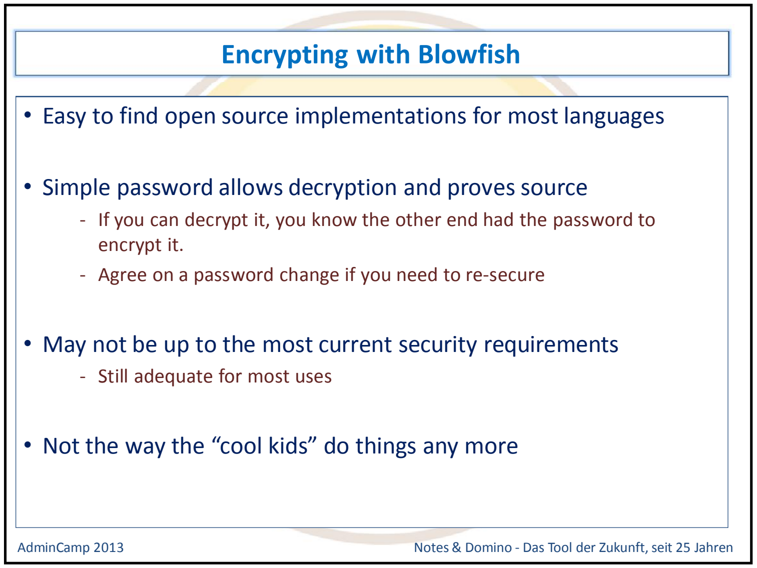
Protecting the Credential Packet

Digital Signature

- Uses another parameter to provide the signature itself
- Requires pre-exchange of data
  - Public Key
  - Hash Salt Value
- May use current x.509 standards or older technology
- Does not prevent the data from being visible
- Open source libraries are available, but can be very complex to use

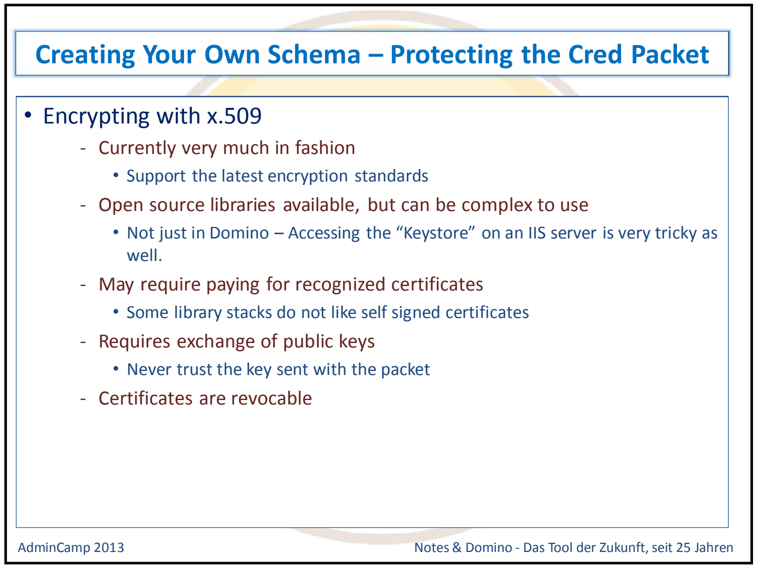
Encrypting the Data

- May use current standards or older encryption schemas like Blowfish
- Requires pre-exchange of data
  - Public Key
  - Decryption Password
- Makes data unreadable to end users or man-in-the-middle
- Open source libraries are available, but can be very complex to use



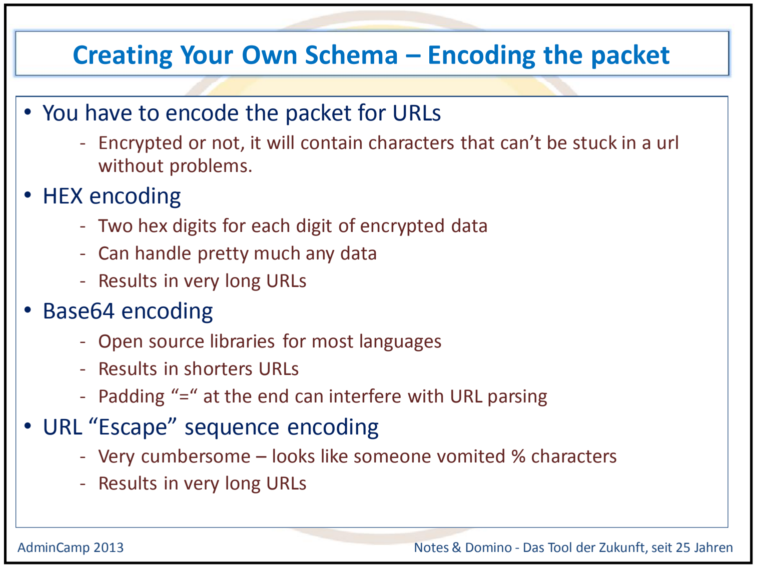
Encrypting with Blowfish

- Easy to find open source implementations for most languages
- Simple password allows decryption and proves source
  - If you can decrypt it, you know the other end had the password to encrypt it.
  - Agree on a password change if you need to re-secure
- May not be up to the most current security requirements
  - Still adequate for most uses
- Not the way the "cool kids" do things any more



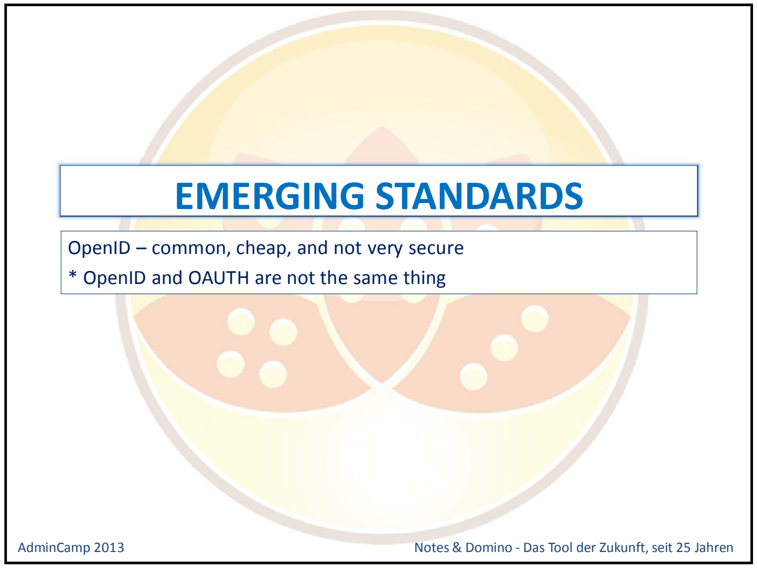
Creating Your Own Schema – Protecting the Cred Packet

- Encrypting with x.509
  - Currently very much in fashion
    - Support the latest encryption standards
  - Open source libraries available, but can be complex to use
    - Not just in Domino – Accessing the "Keystore" on an IIS server is very tricky as well.
  - May require paying for recognized certificates
    - Some library stacks do not like self signed certificates
  - Requires exchange of public keys
    - Never trust the key sent with the packet
  - Certificates are revocable



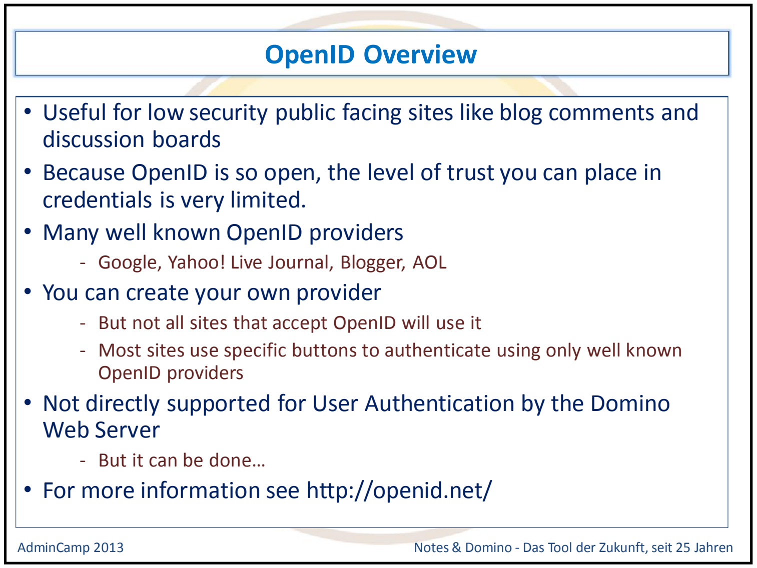
Creating Your Own Schema – Encoding the packet

- You have to encode the packet for URLs
  - Encrypted or not, it will contain characters that can't be stuck in a url without problems.
- HEX encoding
  - Two hex digits for each digit of encrypted data
  - Can handle pretty much any data
  - Results in very long URLs
- Base64 encoding
  - Open source libraries for most languages
  - Results in shorters URLs
  - Padding "=" at the end can interfere with URL parsing
- URL "Escape" sequence encoding
  - Very cumbersome – looks like someone vomited % characters
  - Results in very long URLs



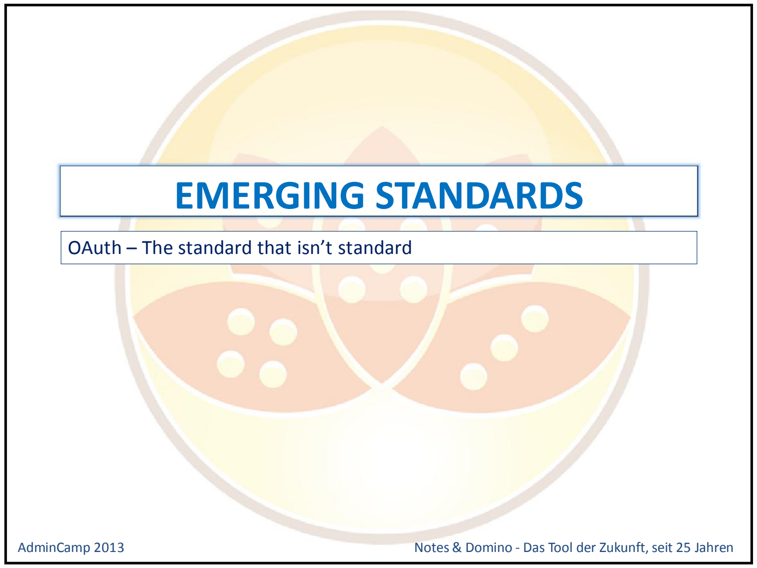
EMERGING STANDARDS

OpenID – common, cheap, and not very secure
* OpenID and OAUTH are not the same thing



OpenID Overview

- Useful for low security public facing sites like blog comments and discussion boards
- Because OpenID is so open, the level of trust you can place in credentials is very limited.
- Many well known OpenID providers
  - Google, Yahoo! Live Journal, Blogger, AOL
- You can create your own provider
  - But not all sites that accept OpenID will use it
  - Most sites use specific buttons to authenticate using only well known OpenID providers
- Not directly supported for User Authentication by the Domino Web Server
  - But it can be done…
- For more information see http://openid.net/



EMERGING STANDARDS

OAuth – The standard that isn't standard

OAuth Overview

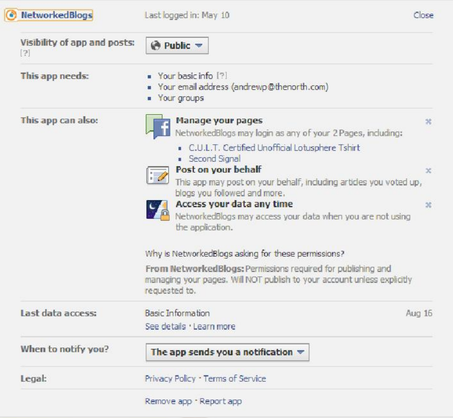
- Complementary to OpenID
- OpenID provides Authentication while OAuth provides for Authorization
- OAuth works like a “valet key”, authorizing third party applications to do things under your credentials on a site.
- Major split between version 1 and version 2
  - Original author no longer involved
  - Version 2 implementations “unlikely to be compatible” with each other.

OAUTH Acts like a “valet key”

The ‘Client’ gets its own set of credentials to access your account

You can limit what those client credentials may do on your behalf

Allows you to control or revoke access on a case by case basis.



NetworkedBlogs Last logged in: May 10 Close

Visibility of app and posts: [?] Public

This app needs:
- Your basic info [?]
- Your email address (andrewp@thenorth.com)
- Your groups

This app can also:

Manage your pages
NetworkedBlogs may login as any of your 2 Pages, including:
- C.U.L.T. Certified Unofficial Lotusphere Tshirt
- Second Signal

Post on your behalf
This app may post on your behalf, including articles you voted up, blogs you followed and more.

Access your data any time
NetworkedBlogs may access your data when you are not using the application.

Why is NetworkedBlogs asking for these permissions?

From NetworkedBlogs: Permissions required for publishing and managing your pages. Will NOT publish to your account unless explicitly requested to.

Last data access: Basic Information Aug 16
See details · Learn more

When to notify you? The app sends you a notification

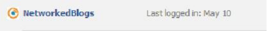
Legal: Privacy Policy · Terms of Service

Remove app · Report app

OAuth Terminology

- Resource Owner: Who’s Content Is it?

- Client: Who wants to access the content?



- Server: Where does the content live?

OAuth Credential Types

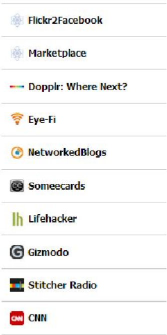
- Client Credentials
  - Typically the user’s server login
- Temporary Credentials
  - May be used to track the authorization request between the client and the server
- Token Credentials
  - Issued by the server to the client as a stand-in for the client credentials without giving those away
  - Can usually be revoked at the server by the resource owner (e.g. Remove this application’s authorization)

OAuth Request Types

- Two Legged Request
  - Where the Client and the Resource Owner are the same
- Three Legged Request
  - Where the Client is a third party acting with authorization from the Resource Owner
- N-Legged Request
  - Used when “re-delegation” is allowed (works like a three legged request)

OAuth Use Cases

- Third party web site apps
  - E.g. Facebook Games
- RSS Feed Aggregators
- Third Party Client Software
  - E.g. Twitter Applications
- Notes 9
  - Integration with Connections



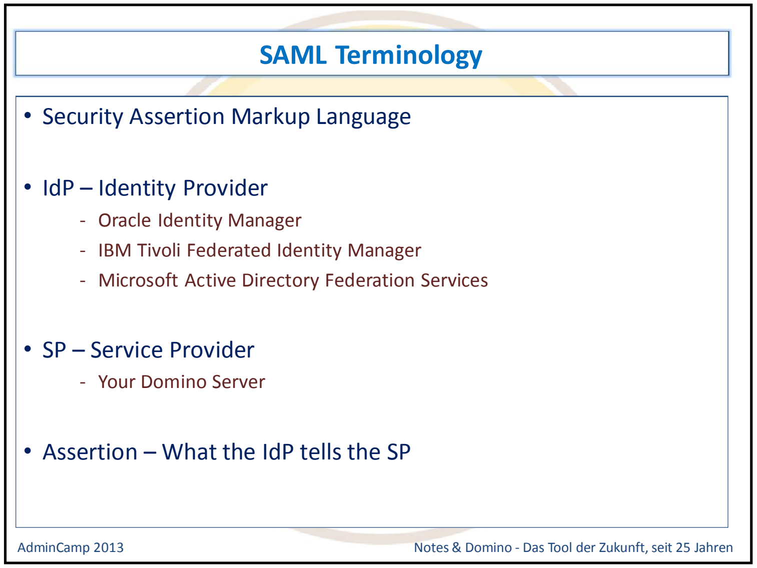
Flickr2Facebook
Marketplace
Dopplr: Where Next?
Eye-Fi
NetworkedBlogs
Someecards
Lifehacker
Gizmodo
Stitcher Radio
CNN

EMERGING STANDARDS

SAML – All the cool kids are using this one

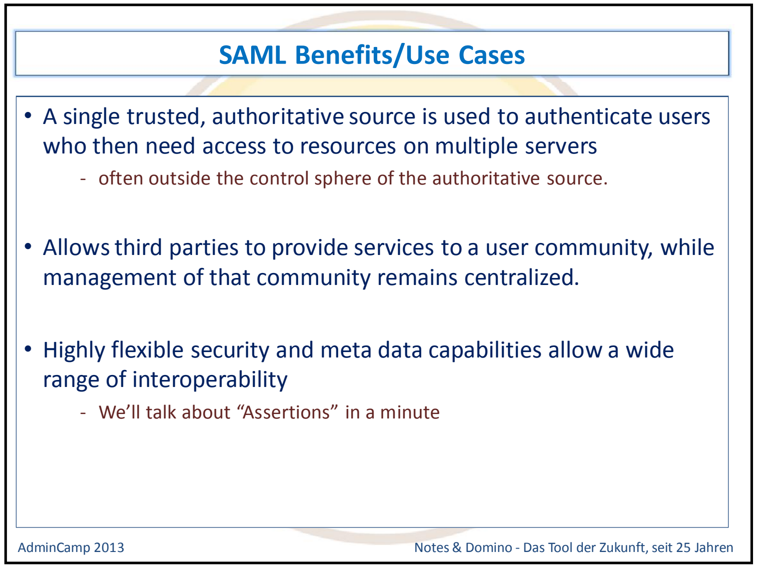
SAML Overview

- SAML is a very rich and detailed specification which provides for passing identity along with meta data between an Identity Provider and one or more Service Providers
- Data is passed in XML packages
  - Generally using http protocols, but not necessary always. The XML can be passed almost any way.
- Packaged XML can be signed, encrypted, both, or neither
- Communication can be made directly between the SP and the IdP or the XML packages can be passed by the requesting client.
  - Usually, the packets are passed by the requesting client as part of the http GET or POST data



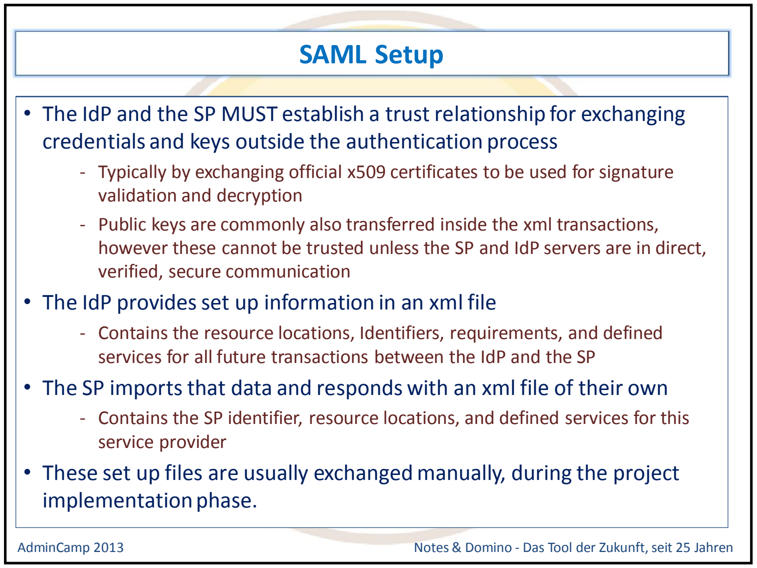
SAML Terminology

- Security Assertion Markup Language
- IdP – Identity Provider
  - Oracle Identity Manager
  - IBM Tivoli Federated Identity Manager
  - Microsoft Active Directory Federation Services
- SP – Service Provider
  - Your Domino Server
- Assertion – What the IdP tells the SP



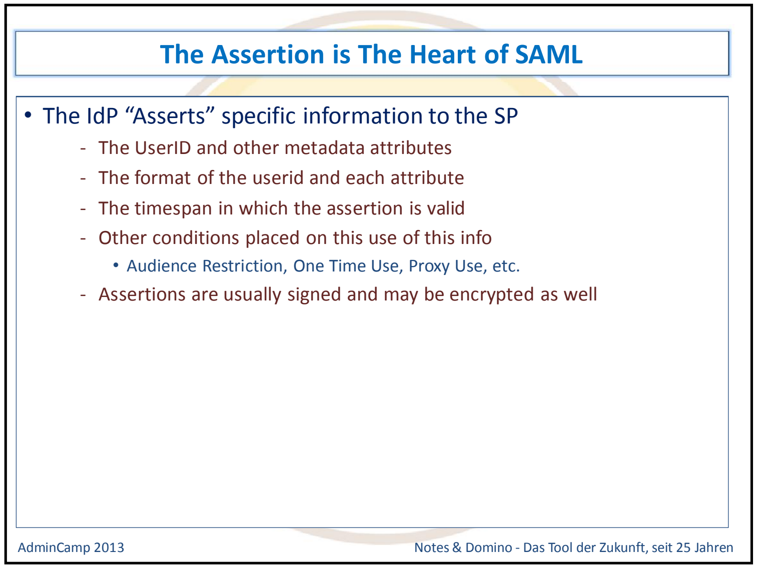
SAML Benefits/Use Cases

- A single trusted, authoritative source is used to authenticate users who then need access to resources on multiple servers
  - often outside the control sphere of the authoritative source.
- Allows third parties to provide services to a user community, while management of that community remains centralized.
- Highly flexible security and meta data capabilities allow a wide range of interoperability
  - We'll talk about "Assertions" in a minute



SAML Setup

- The IdP and the SP MUST establish a trust relationship for exchanging credentials and keys outside the authentication process
  - Typically by exchanging official x509 certificates to be used for signature validation and decryption
  - Public keys are commonly also transferred inside the xml transactions, however these cannot be trusted unless the SP and IdP servers are in direct, verified, secure communication
- The IdP provides set up information in an xml file
  - Contains the resource locations, Identifiers, requirements, and defined services for all future transactions between the IdP and the SP
- The SP imports that data and responds with an xml file of their own
  - Contains the SP identifier, resource locations, and defined services for this service provider
- These set up files are usually exchanged manually, during the project implementation phase.

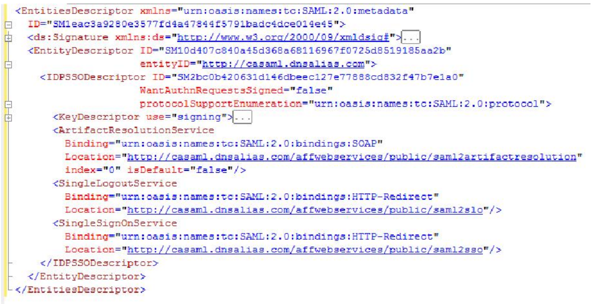


The Assertion is The Heart of SAML

- The IdP "Asserts" specific information to the SP
  - The UserID and other metadata attributes
  - The format of the userid and each attribute
  - The timespan in which the assertion is valid
  - Other conditions placed on this use of this info
    - Audience Restriction, One Time Use, Proxy Use, etc.
  - Assertions are usually signed and may be encrypted as well

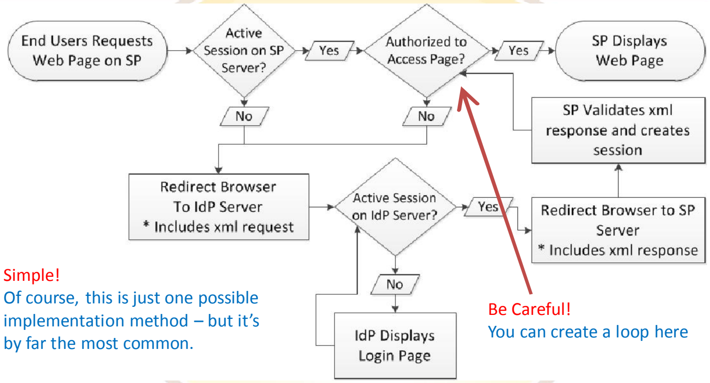
Sample IDP Metadata XML

The digital signature elements have been collapsed for this example.



```xml
<EntitiesDescriptor xmlns="urn:oasis:names:tc:SAML:2.0:metadata"
  ID="SM1eac3a9280e3577fd4a47844f5791badc4dce014e45">
  <ds:Signature xmlns:ds="http://www.w3.org/2000/09/xmldsig#">...
  <EntityDescriptor ID="SM10d407c840a45d368a68116967f0725d8519185aa2b"
                    entityID="http://casaml.dnsalias.com">
    <IDPSSODescriptor ID="SM2bc0b420631d146dbeec127e77888cd832f47b7e1a0"
                    WantAuthnRequestsSigned="false"
                    protocolSupportEnumeration="urn:oasis:names:tc:SAML:2.0:protocol">
      <KeyDescriptor use="signing">...
      <ArtifactResolutionService
        Binding="urn:oasis:names:tc:SAML:2.0:bindings:SOAP"
        Location="http://casaml.dnsalias.com/affwebservices/public/saml2artifactresolution"
        index="0" isDefault="false"/>
      <SingleLogoutService
        Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-Redirect"
        Location="http://casaml.dnsalias.com/affwebservices/public/saml2slo"/>
      <SingleSignOnService
        Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-Redirect"
        Location="http://casaml.dnsalias.com/affwebservices/public/saml2sso"/>
    </IDPSSODescriptor>
  </EntityDescriptor>
</EntitiesDescriptor>
```

Typical SAML Process Flow


End Users Requests Web Page on SP
Active Session on SP Server?
Yes
Authorized to Access Page?
Yes
SP Displays Web Page
No
No
SP Validates xml response and creates session
Redirect Browser To IdP Server
* Includes xml request
Active Session on IdP Server?
Yes
Redirect Browser to SP Server
* Includes xml response
No
IdP Displays Login Page

Simple!
Of course, this is just one possible implementation method – but it's by far the most common.

Be Careful!
You can create a loop here

SAML IN DOMINO 9

Re-check the documentation frequently – this functionality is evolving

SAML in Domino 9

- Domino acts as an SP only, not an IdP
- Currently only supports two IdP Products
  - Microsoft Active Directory
  - Tivoli Federated Identity Manager
- There are reports of it working with others
  - Most common IdP I've seen is Oracle Federated Identity
    - add on to Oracle Identity Manager
- Requires a Notes ID and Person Document for all federated Notes Client users
  - but not necessarily browser access users
- Requires the use of ID Vault if used for Notes Client federated login

Considerations

- Is your IdP supported?
  - Tivoli or Microsoft ADFS
- Is this a SAML 1.1 or 2.0 Implementation?
  - Find out from your IdP before you start (or look in the xml)

```
protocolSupportEnumeration="urn:oasis:names:tc:SAML:2.0:protocol">
```

- Is your IdP going to be using a self signed x.509 certificate?
- Your server's names.nsf template must be version 9
- If your server's ID file is password protected
  - See: "Creating a Domino metadata file if the server id is password protected" in the ADMIN help database.

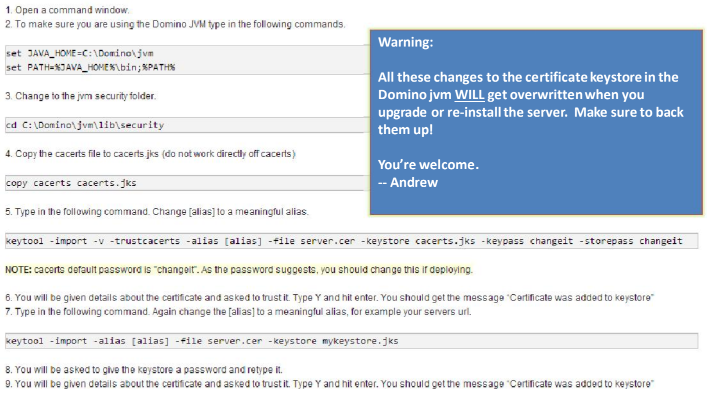
First get the metadata file & x.509 from the IdP

- Typically this is going to be "idp.xml" or "metadata.xml"
- Warning – Some IdPs will give you an invalid XML file!
  - I have experienced this repeatedly with Oracle Identity Manager
- If the XML file they give you has line feeds in it, so it formats well when you open it in a text editor, it is quite probably broken.
  - We'll talk more about this in a minute
- The x.509 public key certificate should be in .cer format
  - Typically base64 encoded text
- If the certificate is self signed, make sure you get the public key of the certificate authority as well.
  - This will require extra work on your part to trust the certificate

The Trouble with XML Signatures

- The xml signature specification used by SAML for signed content is extremely tricky to work with.
  - The signature is stored inside the area defined as "signed" along with the content.
  - A definition of what to exclude from signature checking is included in the signature header by namespace.
  - To verify signed content, the signature has to be excluded first.
- White space (line feeds, carriage returns, tabs) between elements in XML is meant to be ignored.
  - Signed XML does not ignore the whitespace between elements within the signed elements.
- By default, the methods used to export the XML DOM to a file in Java adds carriage return and line feed formatting to the output.
  - Which means the output XML given to you may already be invalid

If your IdP Has a Self-Signed x.509 Certificate



1. Open a command window.
2. To make sure you are using the Domino JVM type in the following commands.

```
set JAVA_HOME=C:\Domino\jvm
set PATH=%JAVA_HOME%\bin;%PATH%
```

3. Change to the jvm security folder.

```
cd C:\Domino\jvm\lib\security
```

4. Copy the cacerts file to cacerts.jks (do not work directly off cacerts)

```
copy cacerts cacerts.jks
```

5. Type in the following command. Change [alias] to a meaningful alias.

```
keytool -import -v -trustcacerts -alias [alias] -file server.cer -keystore cacerts.jks -keypass changeit -storepass changeit
```

NOTE: cacerts default password is "changeit". As the password suggests, you should change this if deploying.

6. You will be given details about the certificate and asked to trust it. Type Y and hit enter. You should get the message "Certificate was added to keystore"
7. Type in the following command. Again change the [alias] to a meaningful alias, for example your servers url.

```
keytool -import -alias [alias] -file server.cer -keystore mykeystore.jks
```

8. You will be asked to give the keystore a password and retype it.
9. You will be given details about the certificate and asked to trust it. Type Y and hit enter. You should get the message "Certificate was added to keystore"

Warning:

All these changes to the certificate keystore in the Domino jvm WILL get overwritten when you upgrade or re-install the server. Make sure to back them up!

You're welcome.
-- Andrew

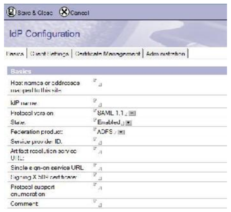
Source Article: "Connecting to a Domino server over SSL in Java, using a self signed certificate."
By Simon O'Dohert -- http://ibm.co/156IXwG

Now You're Ready to Configure Domino!

- Create "idpcat.nsf" from the "idpcat.ntf" template on your Domino 9 Server
  - Make sure to do it in lower case if you are on linux or unix, or if you ever in the figure might migrate to linux or unix (Just do it anyway)
- In the "idpcat.nsf"create a new configuration document
- Fill in the first four fields

Host Name MUST match a host name on one of your WEB SITE documents. Use an IP address if you plan to use SSL.

IdP Name is just a label for you – it can be Anything you want.



IdP Configuration

Basics | Client Settings | Certificate Management | Administration

Basics

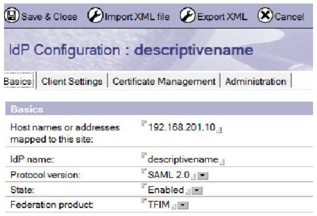
Host names or addresses mapped to this site:	
IdP name:	
Protocol version:	SAML 1.1
State:	Enabled
Federation product:	ADFS
Service provider ID:	
Artifact resolution service URL:	
Single sign-on service URL	
Signing X.509 certificate:	
Protocol support enumeration	
Comment	

Configuring the idpcat.nsf Configuration Document

- Click the "Import XML File" button to bring in the IdP metadata

  WARNING: The file will be removed from the file system. No, there is no good reason for this. Make sure you have a backup even though it gets attached to the record.

- The rest of the fields on this tab will be filled in automatically



IdP Configuration : descriptivename

Basics | Client Settings | Certificate Management | Administration

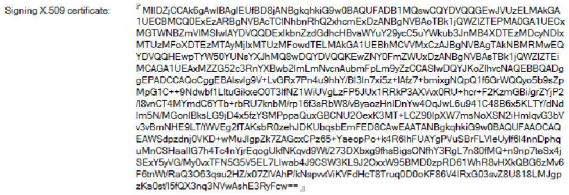
Basics

Host names or addresses mapped to this site:	192.168.201.10
IdP name:	descriptivename
Protocol version:	SAML 2.0
State:	Enabled
Federation product:	TFIM

Check your Certificates

- The certificates will be added automatically
  - Make sure they match the public key you were given
  - Make sure there are no carriage returns or line feeds in them
    - This will happen without anyone realizing it
    - If there are line feeds in this data, you will receive a meaningless error when you start the http task after configuring the system

HTTP Server: Error reading IdP configuration for server xxxxxx:Invalid arguments

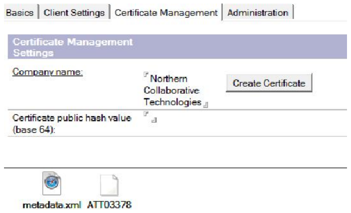


Signing X.509 certificate:

```
MIIDZjCCAk6gAwIBAgIEUfBD8jANBgkqhkiG9w0BAQUFADB1MQswCQYDVQQGEwJVUzELMAkGA
1UECBMCQ0ExEzARBgNVBAcTClNhbnRhQ2xhcmExDzANBgNVBAoTBk1jQWZlZTEPMA0GA1UECx
MGTWNBZmVlMSIwIAYDVQQDExlkbnZzdGdhcHBvaWYuY29ycC5uYWkub3JnMB4XDTEzMDcyNDIx
MTUzMFoXDTEzMTAyMjIxMTUzMFowdTELMAkGA1UEBhMCVVMxCzAJBgNVBAgTAkNBMRMwEQ
YDVQQHEwpTYW50YUNsYXJhMQ8wDQYDVQQKEwZNY0FmZWUxDzANBgNVBAsTBk1jQWZlZTEi
MCAGA1UEAxMZZG52c3RnYXBwb2ImLmNvcnAubmFpLm9yZzCCASIwDQYJKoZIhvcNAQEBBQADg
gEPADCCAQoCggEBAlsvIg9V+LvGRx7Pn4u9hhY/BI3In7xi5z+IAfz7+bmixgNQpQ1f6GrWQQyo5b9sZp
MpG1C++9Ndwbf1LltuGikxeO0T3IfNZ1WiUVgLzFP5JUx1RRkP3AXVvx0RU+hcr+F2KzmGBi/grZYjP2
/I8vnCT4MYmdC6YTb+rbRU7knbM/rp16f3sRbW8/vByaozHnIDnYw4OqJwL6u941C48B6x5KLTY/dNd
Im5N/MGonIBksLG9jD4x5fzYSMPppaQuxGBCNU2OexK3MT+LCZ90IpXW7msNoXSN2iHmlqvG3bV
v3vBmNHE9LT/tWVEg2fTAKsbR0zehJDKUbqsbEmFED8CAwEAATANBgkqhkiG9w0BAQUFAAOCAQ
EAWSdpzdnj0VKD+wMuJlgpZk7ZAGcxCPz65+YaeopPo+k4R6IhFUAYgPVuSBrFLVIeUyIf6I4nnDphq
uMnCSHaallG7h4Tc4nYjrEqogUkfNKqvd9Wt/273DXbxg9fhsBigsONfhY3RgL7n80fMQ+n9np7teSx4j
SExY5yVG/My0vxTFN5G5V5EL7LIwab4J9CSW3KL9J2OxxW95BMD0zpRD61WhR8vHXkQBG6zMv6
F6tnWt/RaQ3O63qsu2HZ/x07ZlVAhP/kNspwtViKVFdHcT8Truq0D0oKF86V4IRxG03svZ8U818LMJgp
zKa0st/I5fQX3nq3NVwAshE3RyFcw==
```

Continue Configuring the IDP Catalog Record

- The "Client Settings" tab is used ONLY if you are going to use this SAML configuration for NOTES CLIENT logon.
  - This also requires configuration with the IDVAULT
- On the "Certificate Management" tab fill in your company name
- SAVE the document then Click the "Create Certificate" button.
- Click the "Export XML" button To generate your "SP.XML" file To give back to the IdP



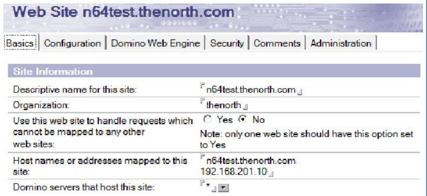
Basics | Client Settings | Certificate Management | Administration

Certificate Management Settings

Company name:	Northern Collaborative Technologies
Certificate public hash value (base 64):	

Now Configure The Website Document

- You must be using the "Internet Sites" view
  - Setting is on the server document
- You MUST say "NO" on the third question and Configure this site with A host name to match.



Web Site n64test.thenorth.com

Basics | Configuration | Domino Web Engine | Security | Comments | Administration

Site Information

Descriptive name for this site: n64test.thenorth.com

Organization: thenorth

Use this web site to handle requests which cannot be mapped to any other web sites: ○ Yes ● No

Note: only one web site should have this option set to Yes

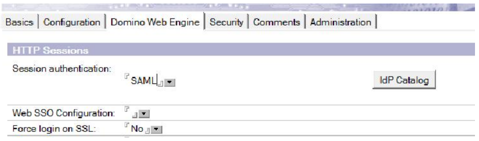
Host names or addresses mapped to this site: n64test.thenorth.com 192.168.201.10

Domino servers that host this site: *

- While not required, you SHOULD specific an IP address in the "Host Names" field so that SSL can be used.
- The values in the "Host Names" field will be used to find the correct IdP configuration in the "idpcat.nsf" file – make it match

Set Session Authentication to "SAML"

- The "IdP Catalog" button will show up once you select SAML
  - If you have properly configured the IdP catalog record and the host name match this web site document, when you click that button, the IdP configuration record will open. If it does not, you have not matched the host names.
- You can still use a multi-session LTPA Token in the "Web SSO Configuration" field. If none is specified, single server session based authentication is used (just like without SAML)



Basics | Configuration | Domino Web Engine | Security | Comments | Administration

HTTP Sessions

Session authentication: SAML

Web SSO Configuration:

Force login on SSL: No

Restart the HTTP Task

- When you restart the HTTP task on the server, if your site is not properly configured it will give you an error.
  - The error will not be helpful. You probably have line feeds in your xml.
- If all is configured, when you access a link on the domino server controlled by that website document which requires authentication, you will be redirected to the IdP to logon.

Ask a Question to Continue the Adventure!

Fill Out Your! Evaluations

Contact me:
andrewp@thenorth.com
@FireFighterGeek
http://www.thenorth.com