

Do you claim to be from the  
Azure sky?

Liam Cleary

You can teach a student a lesson for a day; but if you can teach him / her to learn by creating curiosity, they will continue the learning process as long as they live.

Clay P. Bedford



I am hoping for a different kind of Curiosity today 😊

# Security with SharePoint

- Isn't this an oxymoron? Just kidding!!



# Agenda

- SharePoint Authentication
  - What is available?
- What is claims authentication?
- SharePoint and Claims?
- Identity Providers
- Azure Control Service
  - Google, Windows Live ID, Yahoo, Facebook
  - Custom IDP
- What to choose?





SharePoint Authentication

# SharePoint Authentication

- Multiple Types of Authentication Support
  - Windows
    - NTLM
    - Kerberos
    - Basic
    - Anonymous
    - Digest
  - Forms-based Authentication
    - Lightweight Directory Access Protocol (LDAP)
    - Microsoft SQL Server
    - ASP.NET Membership and Role Providers
  - SAML Token-based Authentication
    - Active Directory Federate Services
    - 3<sup>rd</sup> Party Identity Providers
    - Lightweight Directory Access Protocol (LDAP)

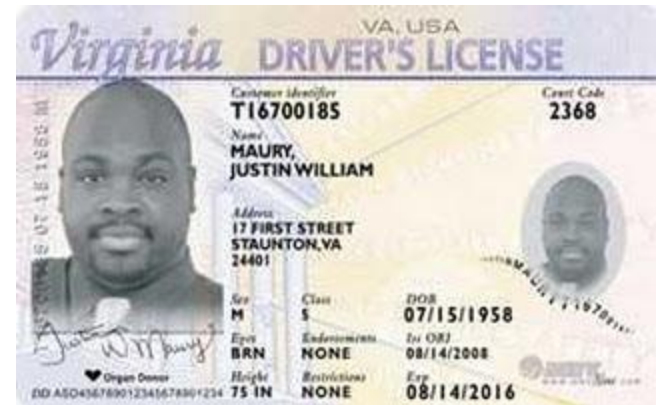
# Authentication – Claims

## Why introduce Claims Authentication?

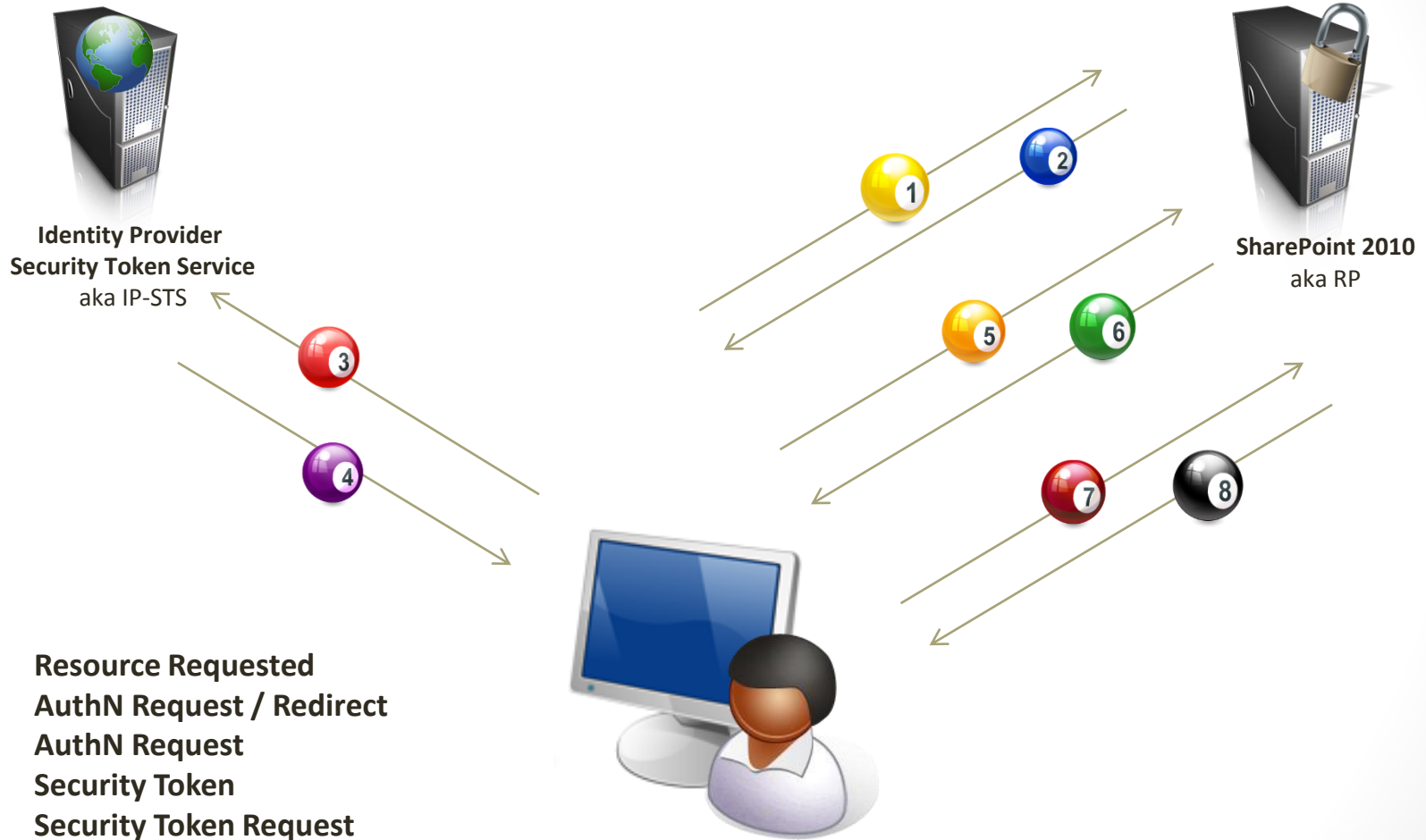
- Wide Support
- Standards Based
  - WS-Federation 1.1
  - WS-Trust 1.4
  - SAML Token 1.1 AuthN
- Single Sign On
- Federation
  - Already many providers
- Microsoft standard approach
- Fed up custom coding everything, every time
- Gets round (some) Office Integration problems
- Easy to configure with little effort
  - Multiple Web Config changes, Web Application Changes and then of course the actual configuration of your identity provider

# Authentication – Claim Terminology

- Identity
  - Info about a Person or Object (AD, Google, Windows Live, Facebook etc.)
- Claim
  - Attributes of the Identity (User ID, Email, Age etc.)
- Token
  - Binary Representation of Identity
  - Set of Claims and the Signature
- Relying Party (aka RP)
  - Users Token
- Secure Token Service (STS)
  - Issuer of Tokens for Users



# Authentication – Sign In Process



1. Resource Requested
2. AuthN Request / Redirect
3. AuthN Request
4. Security Token
5. Security Token Request
6. Service Token
7. Resource Request w/Service Token
8. Resource Sent

# Authentication – Identity Provider

- No need for Membership and Role Provider
- Single Sign Built in
- Central Managed and Entry point for all Authentication
- Utilizes Windows Identity Framework

## **How to build an Identity Provider**

- Create new ASP.NET Security Token Web Service Web Site
- Configure Certificate Settings and Name in <AppSettings>
  - Check Issuer Name within Certificates MMC
- Create new Claims-aware ASP.NET Web Site (testing)
  - Add STS Reference to Claims-aware ASP.NET Web Site
  - Set Claims
- Test
  
- Real World will need code changes:
  - Connect to authentication system
  - Modify Claims
  - Authentication Logic

# Azure Control Service

- Microsoft ADFS Type Cloud Based Service
  - Central Point for offloading Authentication
  - Supports SAML 1.1 / SAML 2.0
  - Support
    - Facebook
    - Google
    - Windows Live ID
    - Yahoo
    - Custom IDP
    - Open ID type authentication
- Support for 3<sup>rd</sup> Party Integration
- Claim Mapping through configuration



Sign-In Process with Azure ACS & SharePoint 2010

## DEMO

## Edit Claim Rule

Specify how one or more input claims can be transformed into an output claim delivered to your relying party application. [Learn more about claim rules.](#)

If

### Input claim issuer

Select the input claim issuer that this rule applies to. Select Identity Provider to process claims from various identity providers, or select Access Control Service to process input claims from a service identity or another claim rule. [Learn more](#)

- Identity Provider:
- Access Control Service

### Input claim type

Select or enter an input claim type. The available claim types will change based on the identity provider specified above. A claim type can be a string or a URI, and is case-sensitive. [Learn more](#)

- Any
- Select from...

Name ^	Date	Status
AddTrustExternalCARoot.crt	5/30/	
ComodoRoot.cer	11/30	
ComodoUTNSGCCA.crt	12/1/	
EssentialCA.cer	11/30	
EssentialSSLCA_2.crt	12/1/	
Helloitsliam-ST5.pfx	11/30	
sharepointcloudsts_helloitsliam_com.cer	11/30	
sharepointcloudsts_helloitsliam_com.cer	11/30	
UTNAddTrustSGCCA.crt	6/7/2- 11/28/2012	Valid (Primary)
	X.509 Certificate	11/30/2011 - 11/28/2012  Valid (Primary)

encryption in this ACS namespace. [Learn more](#)

## Rule Groups

## Certificates and Keys

Add or manage the certificates and keys [about certificates and keys.](#)

[Add](#) | [Delete](#)

### Token Signing

Used For

[Service Namespace](#)

[Service Namespace](#)

Ready

Mar

Dev

App

### Output claim value

The first input claim value can be passed through or replaced with a custom value. [Learn more](#)

- Pass through first input claim value
- Enter value:

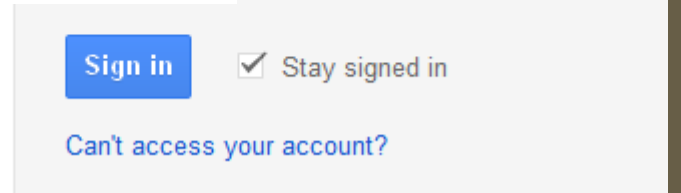
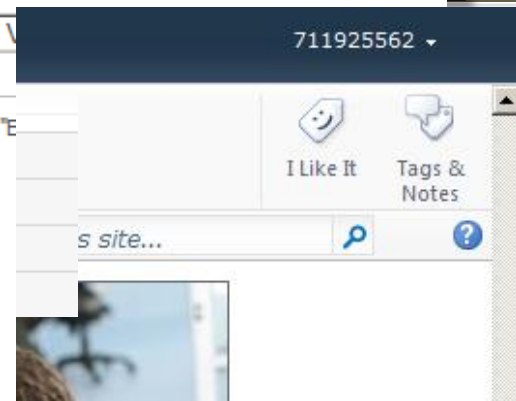
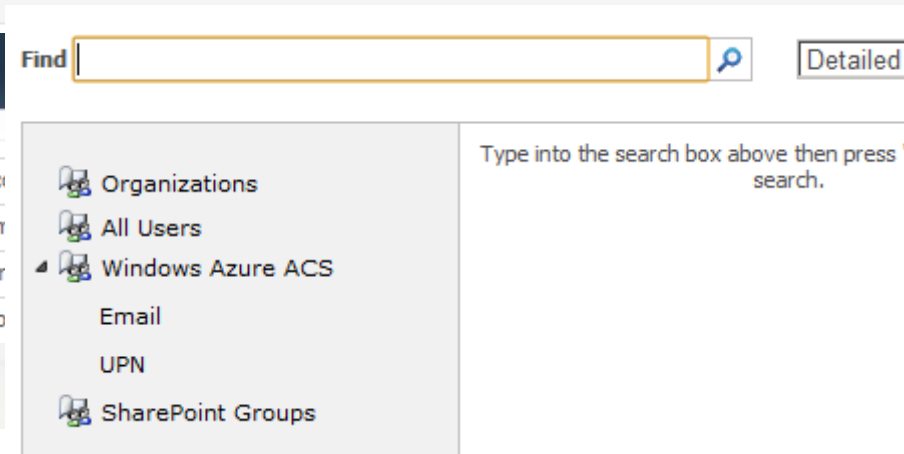
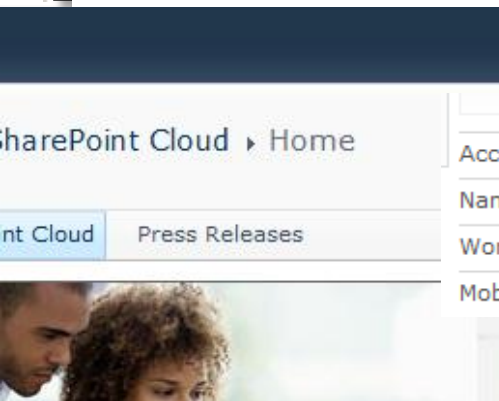
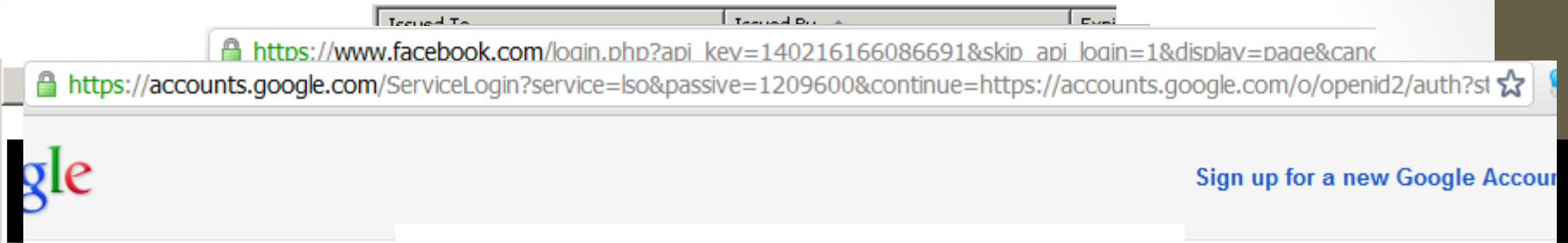
### Rule Information

#### Description (optional)

Enter a description for this claim rule.

Passthrough "nameidentifier" claim from Windows Live ID as "nameidentifier"

# Azure Control Service - SharePoint



Thawte Timestamping CA	Thawte Timestamping CA	12/3
UTN - DATACorp SGC	UTN - DATACorp SGC	6/24
COMODO Certification Authority	UTN - DATACorp SGC	5/30
UTN-USERFirst-Object	UTN-USERFirst-Object	7/9/
VeriSign Class 3 Public Primary Cer...	VeriSign Class 3 Public Primary Certifi...	7/16
VeriSign Trust Network	VeriSign Trust Network	5/18
VeriSign Trust Network	VeriSign Trust Network	8/1/



DEMO

# What to else to know?

- Given the choice
  - Microsoft ADFS
  - Custom Identity provider
  - Azure ACS
    - Multiple Providers
- Custom Claims Provider will be needed
- If Augmentation of claims is needed from LOB, Custom IDP
- All users will experience the “**nothing**” redirect
  - Redirect, Redirect and Redirect 😊
- SharePoint does not support SAML 2.0 Assertions
- For internal LOB for Auth to ACS – maybe overkill
  - Expose Internal LOB Auth to ACS through provider

# SHAREPOINT SATURDAY



Utah

## Thanks to our sponsors!



# Thank you & Questions

Email: [liamc@susqtech.com](mailto:liamc@susqtech.com)

Work: <http://www.susqtech.com>

Twitter: @helloitsliam

Blog: <http://blog.helloitsliam.com>