Claims based Authentication in SharePoint 2010

DD109

Spencer Harbar
Enterprise Architect
harbar.net

About Spencer

Microsoft CERTIFIED Master

MVP Microsoft Most Valuable Professional

- www.harbar.net | spence@harbar.net | @harbars
  - General SharePoint Dogsbody
  - Microsoft Certified Master | SharePoint 2007
  - Microsoft Certified Master | SharePoint Instructor & Author
  - Most Valuable Professional | SharePoint Server
  - SharePoint Patterns & Practices Advisory Board Member
  - 16 years in Enterprise IT
  - ISPA Vice President
  - Enterprise Architect working with Microsoft's largest customers deploying SharePoint Server.
  - Works with SharePoint Product Group on 2010 Readiness
  - Author for MSDN & TechNet

Agenda

- Why Claims?
- Claims Identity Primer
- Authentication (Sign In)
- Forms Based Authentication
- Services

- Scare tactics!

SHAREPOINT 2010 IS THE FIRST MICROSOFT PRODUCT TO IMPLEMENT THE WINDOWS IDENTITY FRAMEWORK

Why Claims?

- Support existing Identity infrastructure
  - Active Directory
  - LDAP, SQL
  - Federation Gateways
  - Web “SSO” and Identity Management systems
- Enable automatic, secure identity delegation
- Support “no credential” connections to external web services
- Consistent API to develop SharePoint solutions
  - Across the product SKUs / Project / Office Web Apps etc
  - For ISVs / third party developers

- SharePoint Server 2010

BUT FIRST, A QUICK PRIMER

Claims-based identity

- Is all around us every day
- Analogy: Air travel (avoiding volcano ash)
  - You Check In (Authentication)
    - Presenting credentials (Passport)
    - Credentials are validated
  - You Receive a boarding pass (Signed Claims)
    - Seat, Frequent Flyer, Gate etc
    - Encoded issue

Note: At Heathrow T5 you now have to authenticate about 20 times!

Identity

- What is Identity?
  - Set of attributes to describe a user such as name, e-mail, age, group membership, etc.
- What is a Claim?
  - Some authority that claims to have the attribute and its value

User Identity is a set of claims

- Why do we say “claim” and not “attribute”?
  - MySpace & the DVLA both have the age attribute
  - MySpace claims that I am 18, while DVLA claims I am 36.
  - In order to make authorization decisions with age, your app needs to decide which “claim” you will **trust**.
- **Trust** depends on scenario not on technical capability

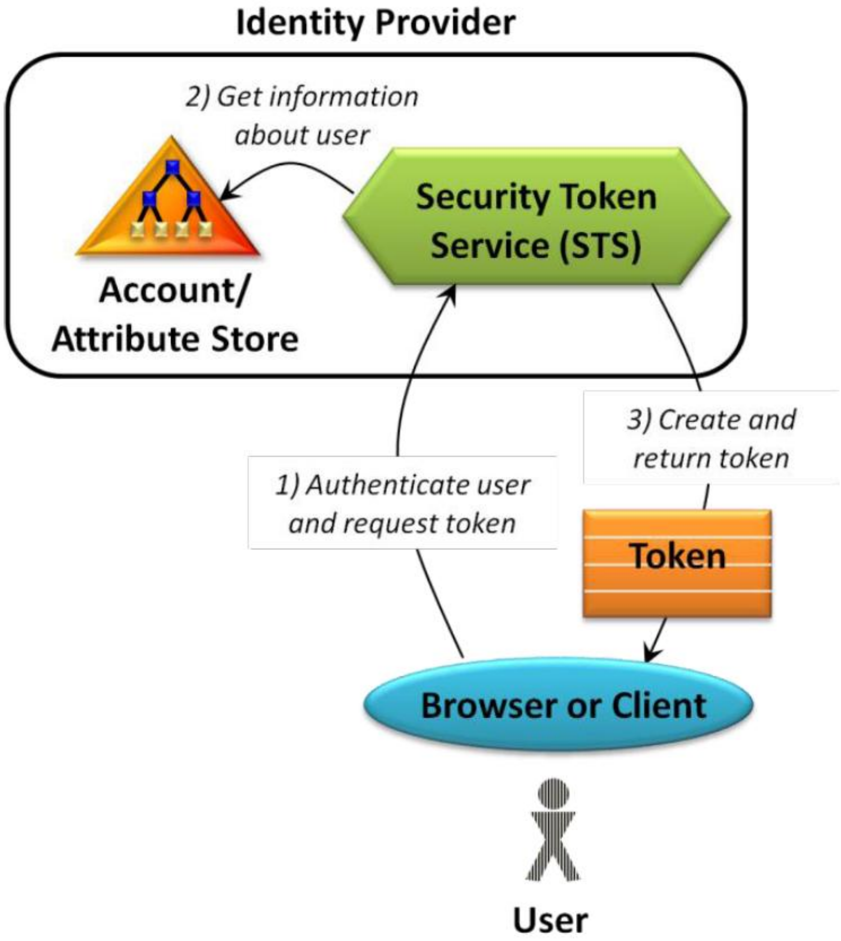
More than Federation

- Federation between Organisations was the original driver
- Over time, Claims turned out to be useful for more than just Federation
- Cleanly factoring out the Identity Provider from the application is invaluable
  - SharePoint is Identity Provider neutral

Security Token Service (STS)

- Web Service that issues security tokens carrying claims that describe the caller
  - Supporting multiple credential types
  - Supporting Federation Scenarios
    - Users are authenticated by their domain and granted access to resources in another domain by establishing trust between each domain's STS
  - Facilitating identity delegation scenarios
    - Authenticated user granted access to downstream services
  - Facilitating claims transformation so that relevant claims area available at applications and services

Security Token Service (STS)


Identity Provider
2) Get information about user
Security Token Service (STS)
Account/ Attribute Store
3) Create and return token
1) Authenticate user and request token
Token
Browser or Client
User

Relying Party (RP-STS)

- An application that relies on claims
  - Claims aware application
  - Claims based application
- Web Applications and Web Services can both be built this way
  - e.g. A SharePoint Web Application

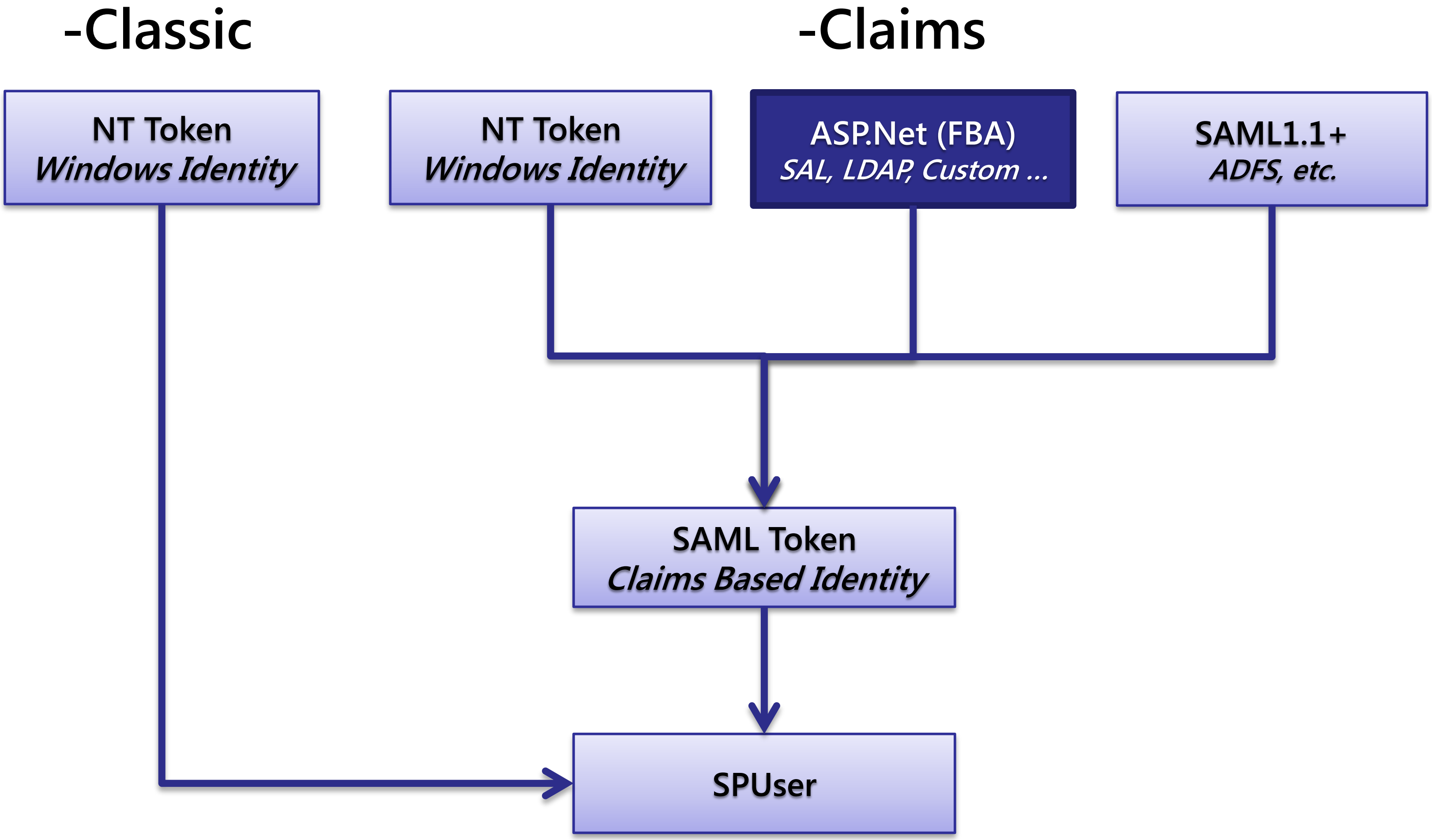
- SharePoint Server 2010

AUTHENTICATION (SIGN IN)

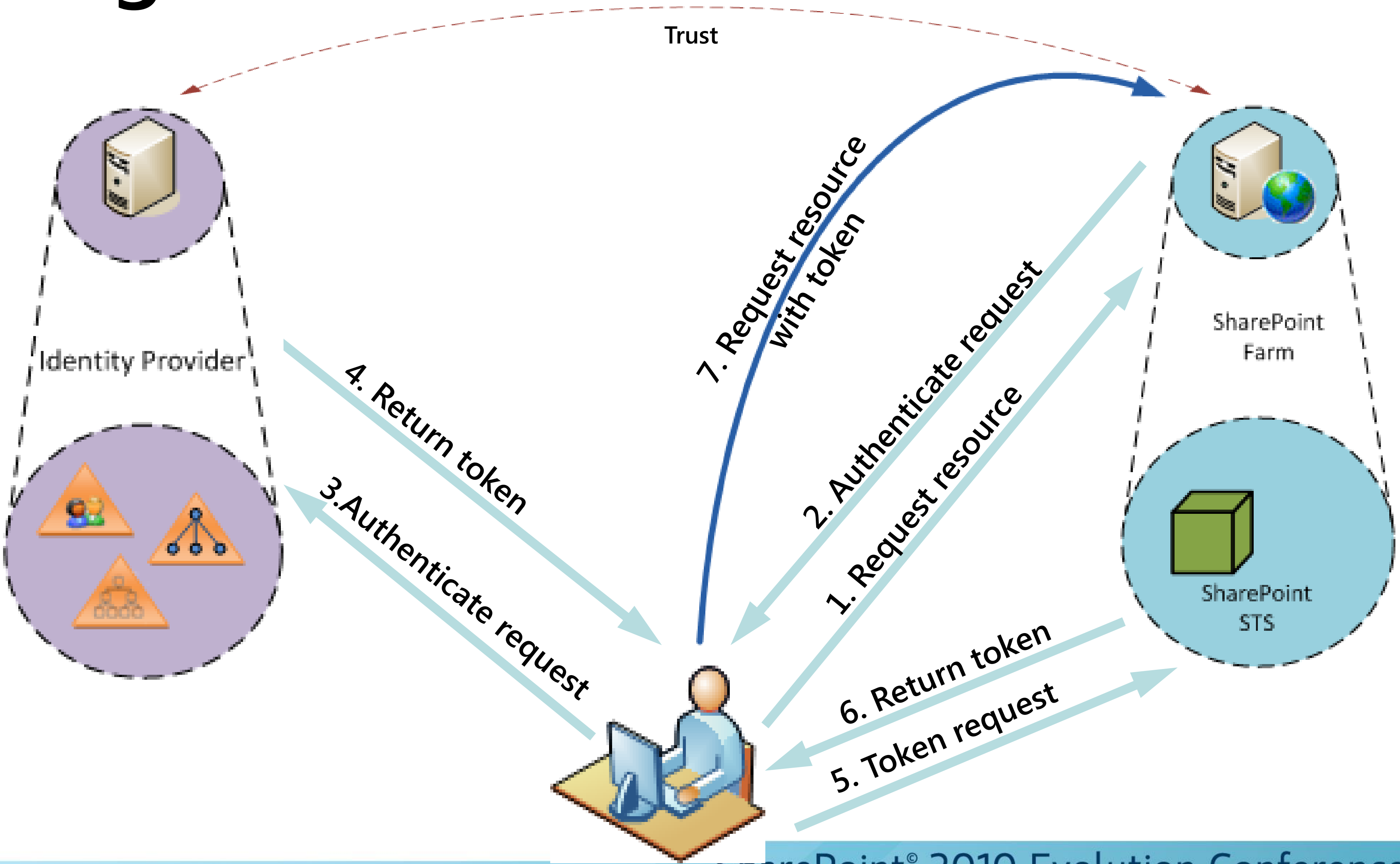
Sign-in Scenarios

- Sign-in to SharePoint with both Windows and LDAP directory Identity
- Easily configure Intranet and Extranet users for Collaboration
- Integrate with other customer identity systems (e.g. ADFS, etc.)
- Use Office Applications with non-Windows Authentication

Identity Normalization



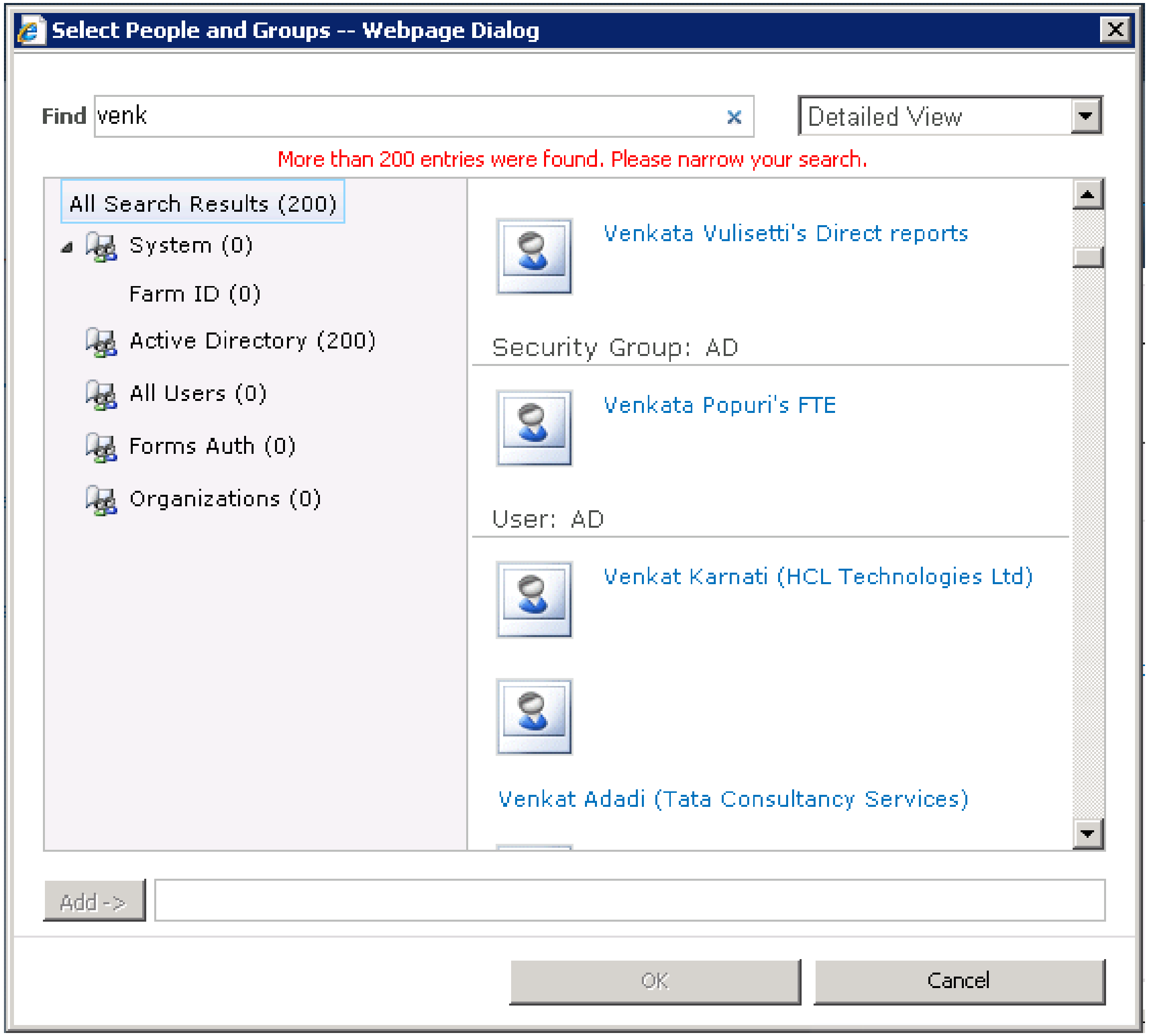
Sign In


Trust
Identity Provider
SharePoint Farm
SharePoint STS
1. Request resource
2. Authenticate request
3.Authenticate request
4. Return token
5. Token request
6. Return token
7. Request resource with token

Claim Providers

- Augmentation of Claims
  - Used to add application specific claims
  - SharePoint will authorize over these claims
- Search and Resolve Claims
  - Provides a way to enumerate and select claims
  - SharePoint will present the claims in the User Experience

Claims Picker



Find venk

Detailed View

More than 200 entries were found. Please narrow your search.

- All Search Results (200)
- System (0)
- Farm ID (0)
- Active Directory (200)
- All Users (0)
- Forms Auth (0)
- Organizations (0)

Venkata Vulisetti's Direct reports

Security Group: AD

Venkata Popuri's FTE

User: AD

Venkat Karnati (HCL Technologies Ltd)

Venkat Adadi (Tata Consultancy Services)

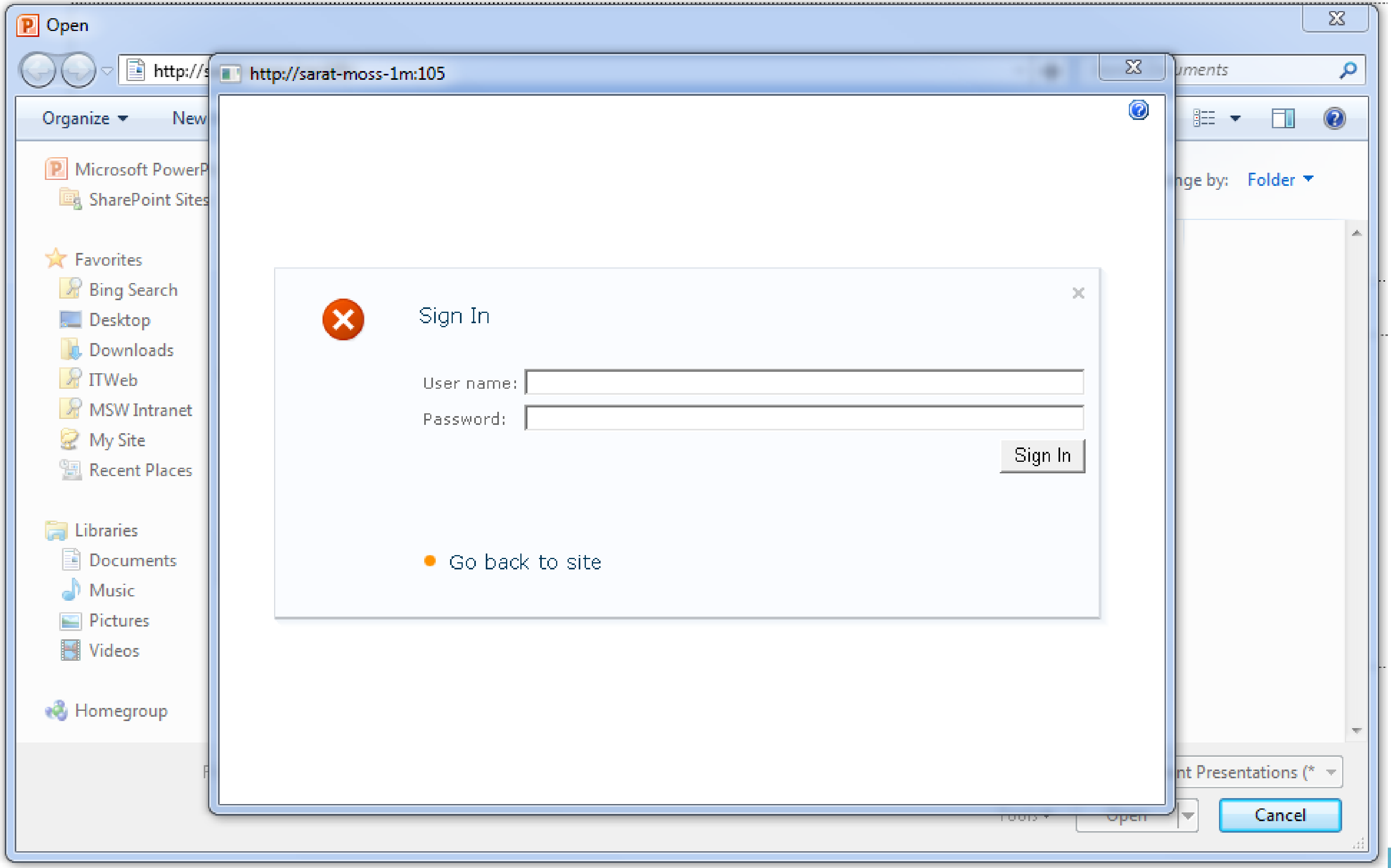
SharePoint Authentication Model

- Two Authentication Modes
  - "Classic" and Claims
- There are no other SharePoint Authentication Providers!
- Classic Mode is more or less the same as SharePoint 2007
  - A few minor details: www.harbar.net
- SharePoint uses claims "internally" regardless
  - Identity normalisation

Office Application support

- Office Client applications support non-Windows Integrated Authentication
- Office 2010 on
  - Windows XP + IE8
  - Windows Vista SP2 or IE8
  - Windows 7
- Office 2007 SP2 on
  - Windows XP + IE8
  - Windows Vista SP2 or IE8
  - Windows 7

Office non-Windows sign-in



Sign In

User name:

Password:

Sign In

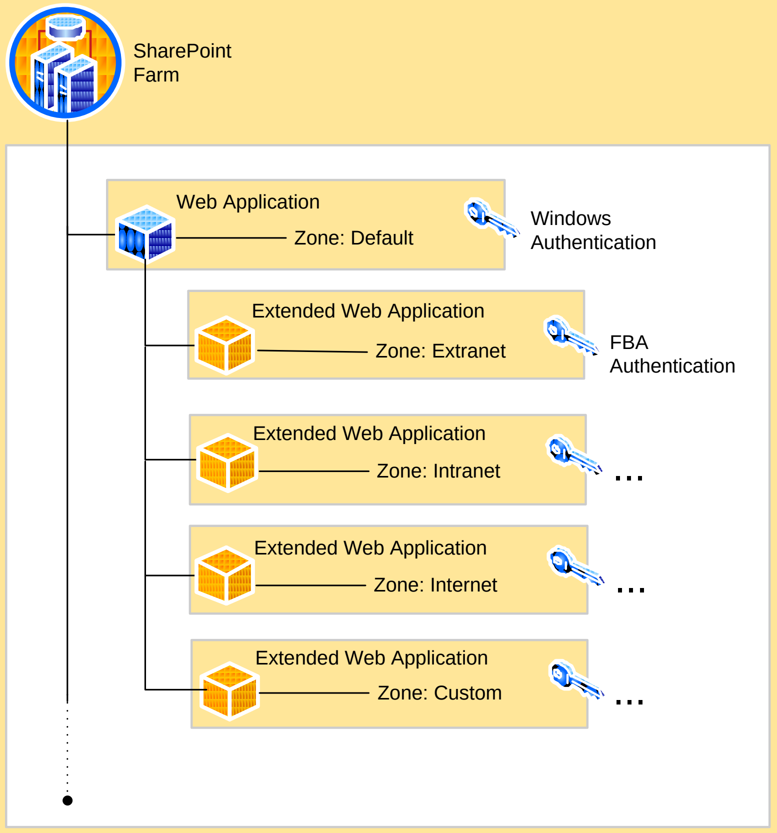
● Go back to site

Supported Modes

- Windows-Classic
- FBA-Claims
- Anonymous
- FBA-Claims + Anonymous
- Windows-Claims
- SAML-Claims
- Windows-Claims + FBA-Claims

Mixed vs Multi-Authentication

Mixed Authentication



SharePoint Farm

Web Application
Zone: Default
Windows Authentication

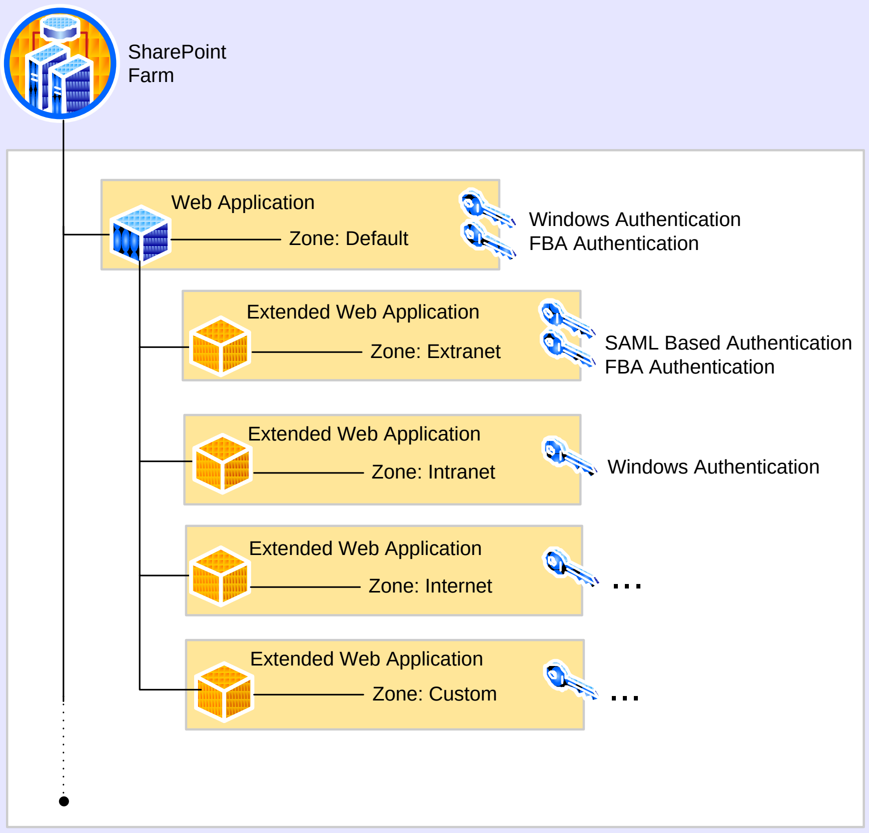
Extended Web Application
Zone: Extranet
FBA Authentication

Extended Web Application
Zone: Intranet
…

Extended Web Application
Zone: Internet
…

Extended Web Application
Zone: Custom
…

Multi-Authentication



SharePoint Farm

Web Application
Zone: Default
Windows Authentication
FBA Authentication

Extended Web Application
Zone: Extranet
SAML Based Authentication
FBA Authentication

Extended Web Application
Zone: Intranet
Windows Authentication

Extended Web Application
Zone: Internet
…

Extended Web Application
Zone: Custom
…

- SharePoint Server 2010

FORMS BASED AUTHENTICATION (FBA)

What changed in FBA

- FBA Users are Claims Identities
  - Claims identity is created instead of ASP.Net Generic identity
  - STS calls membership provider to validate user and issues a claims token
  - ValidateUser() must be implemented by membership providers
  - Roles are converted to claims
- Mixed mode environments
  - All principals are available in all zones

Forms Based Authentication

- Requires Claims Mode
- Implemented as a Claims Provider
- Upgrade from SharePoint 2007
  - In Place: ACLs updated, web.config not
  - DB Attach: ACLs updated, no need to update config.
- Provider Neutral
  - e.g. SQL, LDAP, etc

Configuring FBA

- Create Authentication Provider
- Create or Configure existing Web App to use that Authentication Provider
- Add membership/role provider entries to web.confg for:
  - Central Administration
  - Content Web Application
  - STS

Why three places?

- Central Administration
  - Needs the references of all providers to enable picking of principles from any provider
- STS
  - Authenticate User
  - Get Roles of User (converted to Claims)
- FBA Web Application
  - Needs “system” claims provider (automatically configured)
  - Custom provider enables people picker

Demo

SharePoint 2010

FBA & MULTI MODE AUTHENTICATION

SERVICES

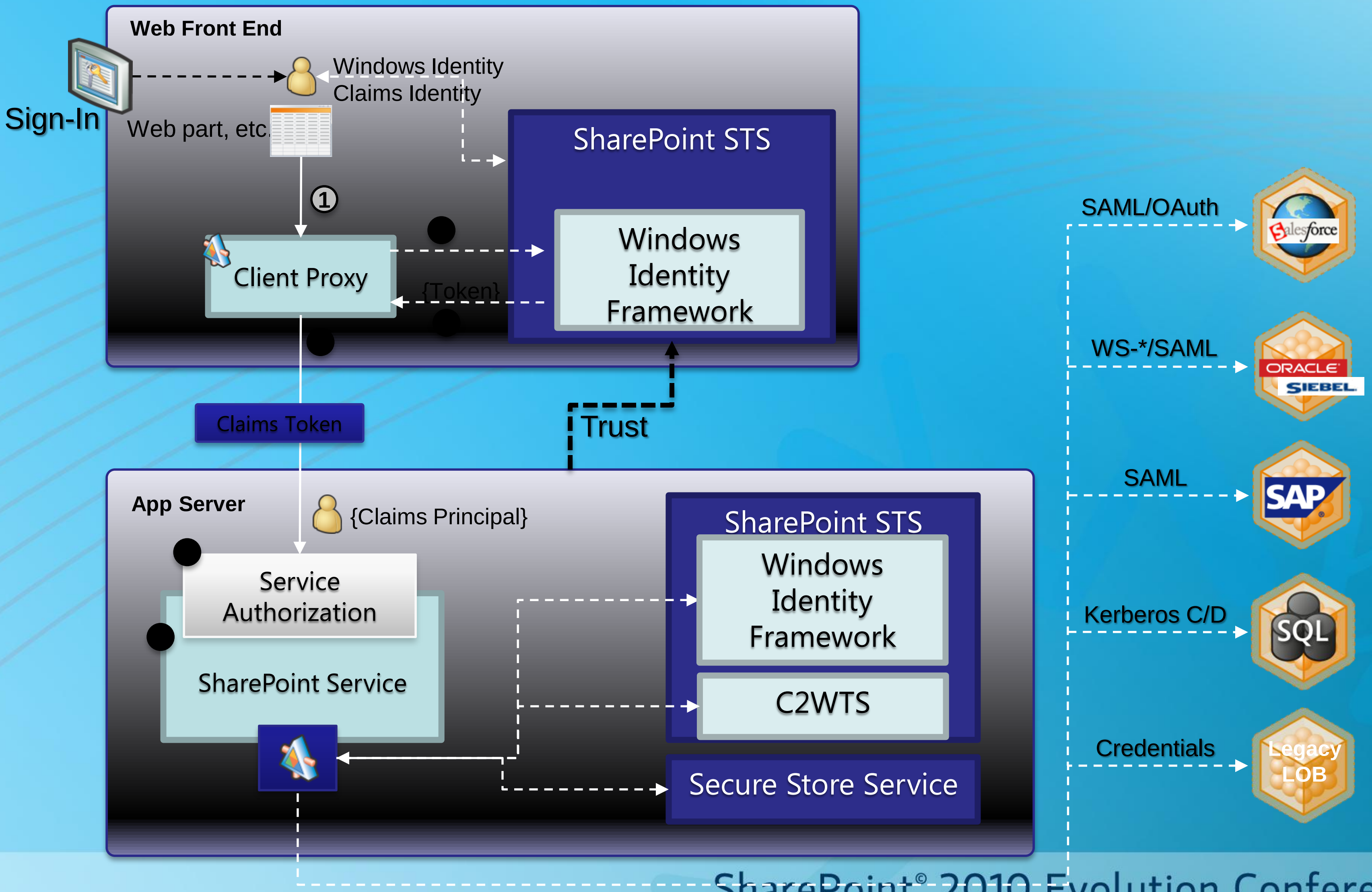
Claims in SharePoint Features

- SharePoint Foundation
- Search (Security Trimming)
- FAST for SharePoint
- Business Connectivity Services
- Virtual Lists
- Excel Calculations Services, InfoPath
- Inter-Farm Trusts
- Basically everything that can consume data from a data connection

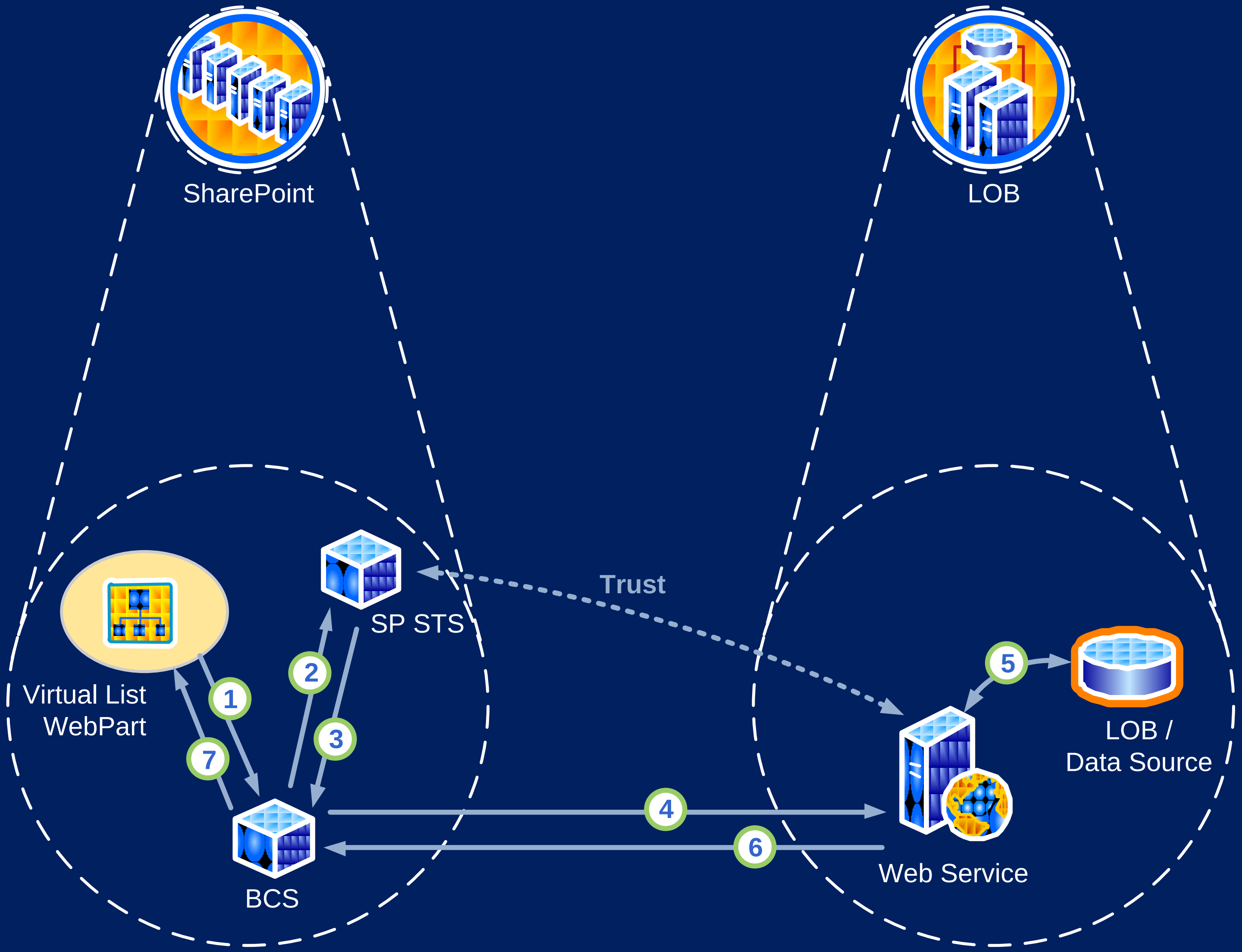
Services Scenarios

- Show user’s PayStub in LOB data without credentials (intranet)
- Show real-time order status from supplier inside the enterprise Portal (extranet or internet)
- Securely deploy SharePoint farm(s) for user identity delegation

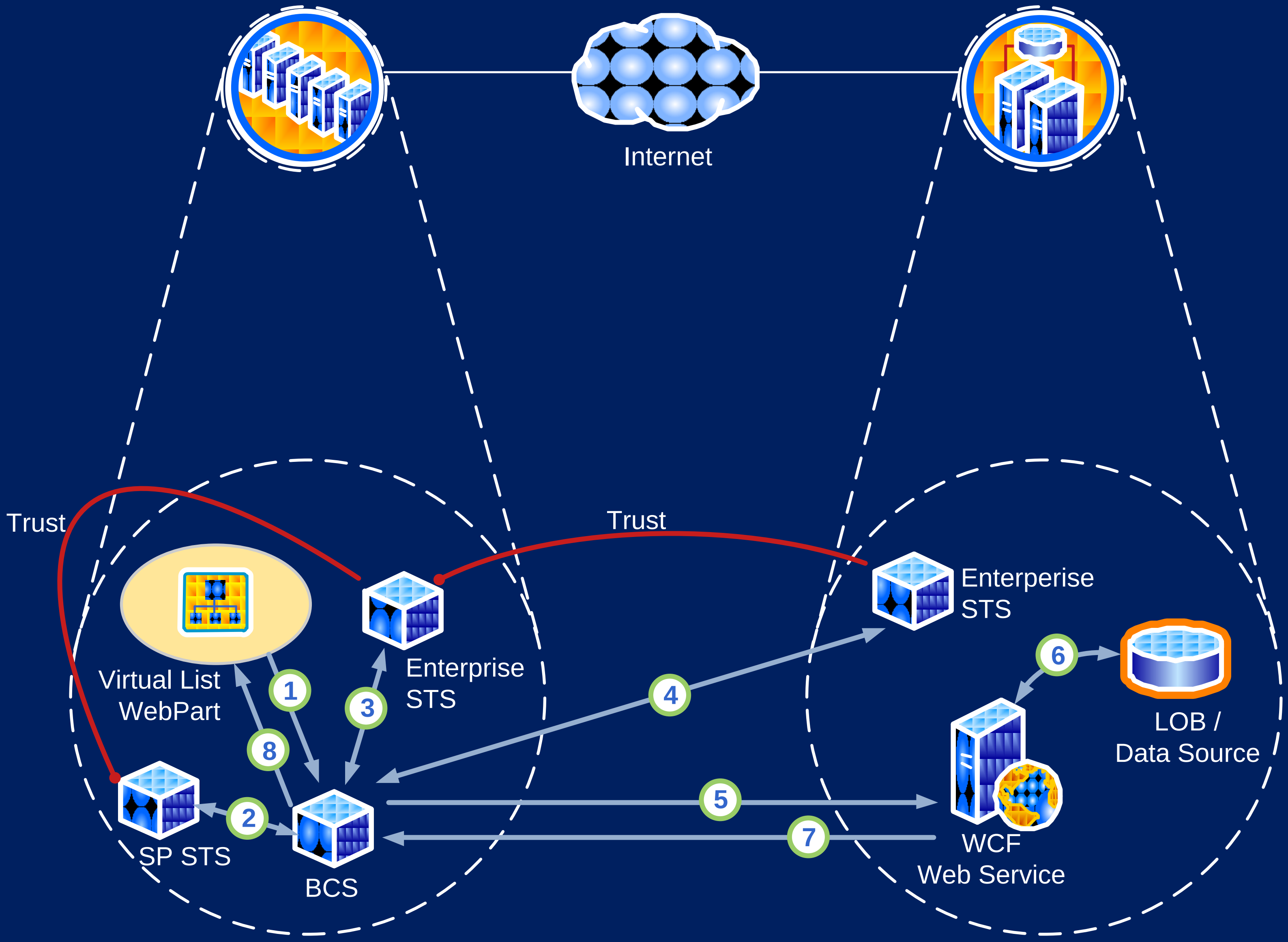
INTEROPERATING W/ SERVICES



Simple Virtual List



X-Boundary Services



Connecting to External Systems

- SharePoint will issue Security Tokens
    - User's identity is included (called ActAs token)
    - Other information about the Farm can included as well
- Many choices to invoke web services
    - Declaratively through Business Connectivity Services
        - Using ActAs token
        - Using Service Delegate token
    - Do-it-yourself with WCF
    - Do-it-yourself with SOAP
    - Use Secure Store for credentials
- Use claims to authorize inside your own service

Standards

- WS-Federation 1.1
  - Provides the architecture for a clean separation between trust mechanisms, security tokens formats and the protocols for obtaining tokens
- WS-Trust 1.4
  - How to request and receive security tokens
- SAML Token 1.1
  - XML vocabulary used to represent claims in an interoperable way

Key Takeaways

- NEW way of Identity in SharePoint
  - FBA works slightly differently from 2007
- Built on Standards for interoperability
- Enabler for Service Applications
- Office Client support for non-Windows Authentication

Thank you for attending!

Patrick, we miss you