Federated Identities in the Real World

Nathan Sargent – Regional Solutions Architect

Agenda

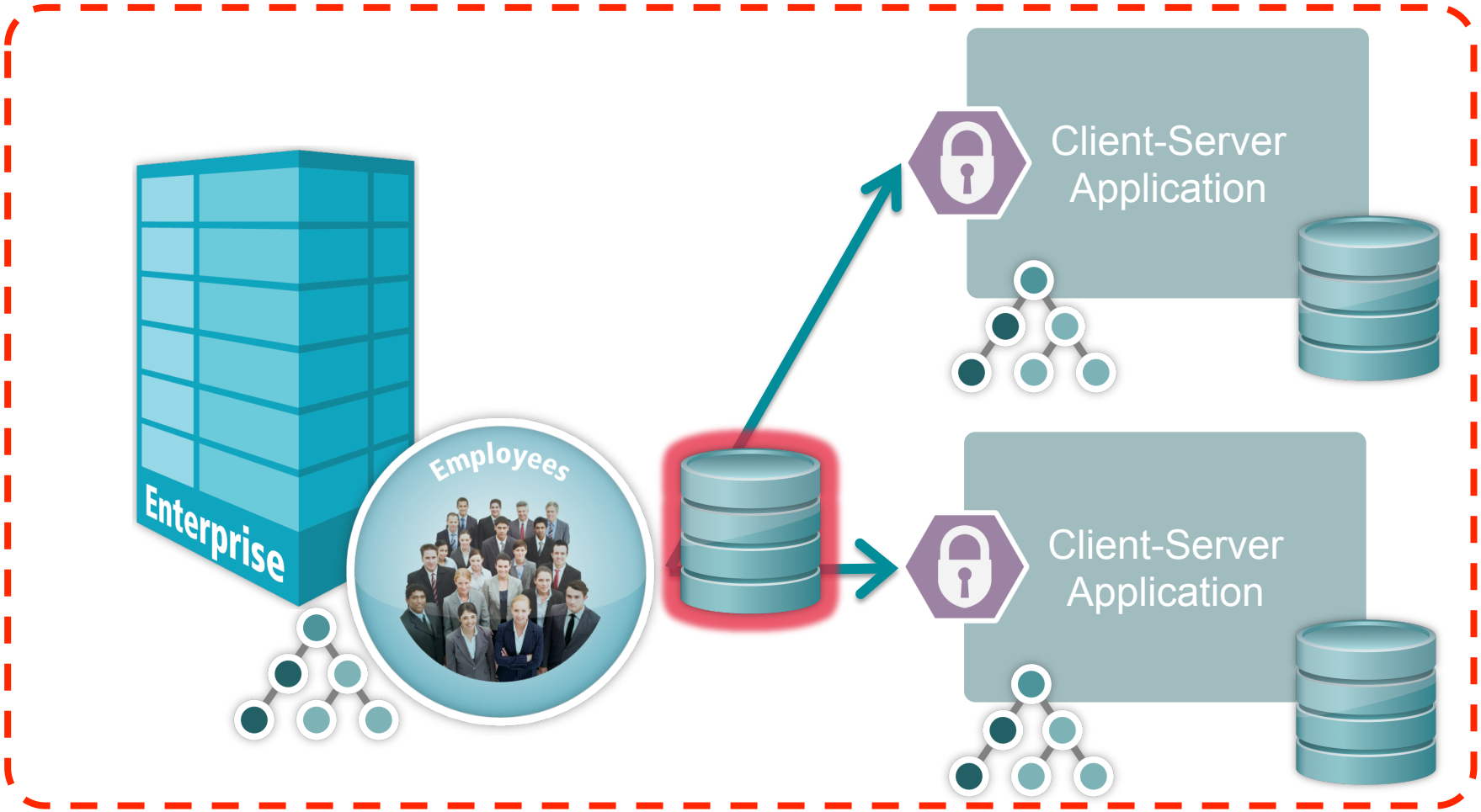
- Speaker Background
- Evolution of Federation – Client/Server
- Evolution of Federation – Move to the Cloud
- Federation History
- SAML to the Rescue!
- Use of Federated Identities in the Real World
- Practical Considerations
- Alternative Approaches
- Evolution of Federation, Part 2
- How PingIdentity Addresses these Challenges
- Question & Answer

Speaker Background

Nathan Sargent, Regional Solutions Architect, SSCP/CISSP/CIFI

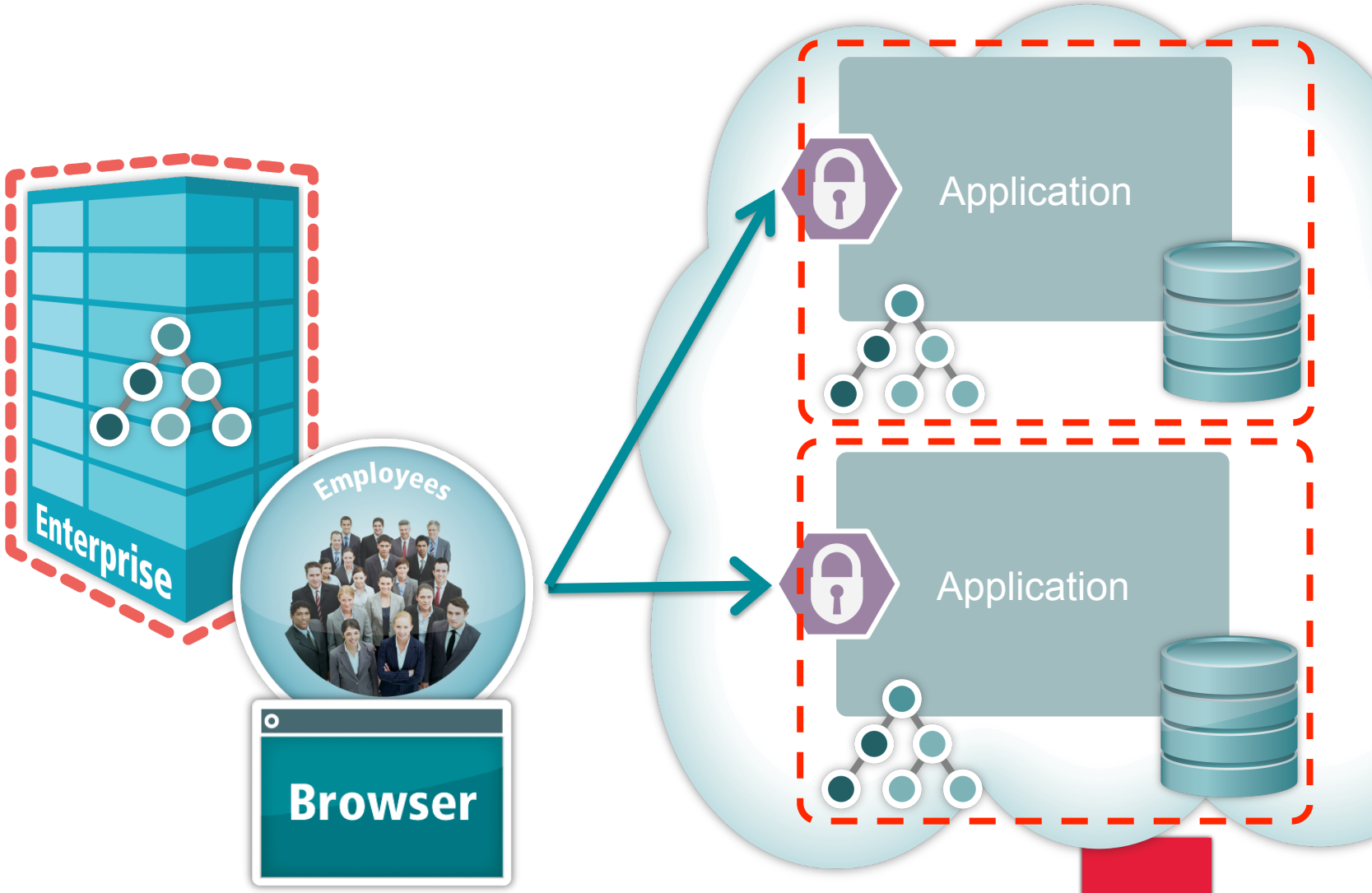
Mr. Sargent has over 20 years of industry experience in information security and technology that include network design, security operation center management and extensive consulting experience with security best practices and procedures. Specialties include secure network design, secure policies and procedures, business continuity planning, enterprise security management, identity management, federation, and computer information forensics.

Evolution of Federation – Client/Server



Ping Identity

Evolution of Federation – Move to the Cloud



Ping Identity®

Stormy Outlook!

Applications in the Cloud!

Passwords at Risk!

Manual On-boarding Process!

How to Remove Access?

Customized Security Solutions?

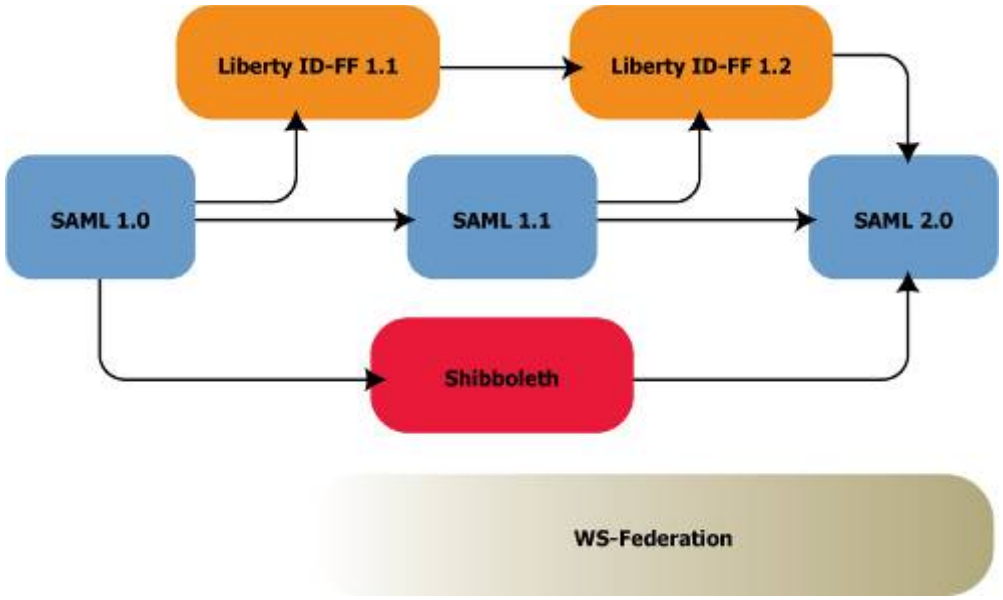
Re-write Applications?

How to Scale Business/Federation Relationships?

More Questions than Answers?

History: Federation pre-2005

Until March 2005, identity federation suffered from an unusual problem: too many standards. Companies that deployed federation prior to 2005 were forced to deal with five incompatible protocols: OASIS SAML 1.0 and 1.1, Liberty Alliance ID-FF 1.1 and 1.2, and Shibboleth. WS-Federation was isolated (ok, it still is!)



SAML 2.0 to the Rescue!

- OASIS, the Liberty Alliance and Shibboleth joined forces to create an uber-standard that eclipsed all previous standards. March 2005
- Tried and True – 7 years of adoption! SAML is everywhere, even Microsoft supports it!
- Provides a method to encapsulate identity data (NOT credentials).
- Requires web servers embrace trust model (change of AuthN model @ application)
- Just-in-Time Provisioning at Service Providers
- No de-provisioning needed by Service Providers

Ping Identity®

Common Questions

What is SAML? What does it really look like? Is there a structure to it?

How does a user get a SAML assertion?

How does my application create or consume a SAML assertion?

If my company receives a SAML assertion, what do I do with it and how to I get the user to my application?

What about Microsoft's WS-Federation "Claims" or ADFS?

Why not use PKI and shared certificates or other obscuration scheme?

What about client-side software and/or server agents?

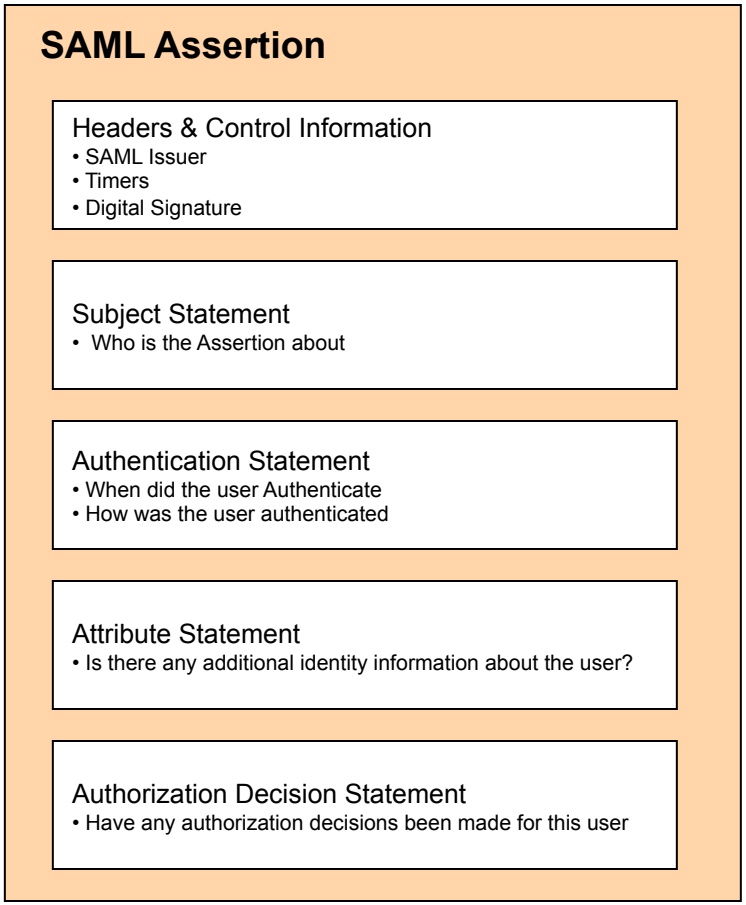
Ping Identity®

Welcome to SAML!


```
XML: <samlp:Response Destination="https://localhost:9031/sp/ACS.saml2" IssueInstant="2012-05-31T16:16:12.109Z" ID="fHY7MMJ--bue60oX3e0U.B.XetG" Version="2.0" xmlns:samlp="urn:oasis:names:tc:SAML:2.0:protocol">
 <saml:Issuer xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion">localhost:default:entityId</saml:Issuer>
 <ds:Signature xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
  <ds:SignedInfo>
   <ds:CanonicalizationMethod Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#"/>
   <ds:SignatureMethod Algorithm="http://www.w3.org/2000/09/xmldsig#rsa-sha1"/>
   <ds:Reference URI="#fHY7MMJ--bue60oX3e0U.B.XetG">
    <ds:Transforms>
     <ds:Transform Algorithm="http://www.w3.org/2000/09/xmldsig#enveloped-signature"/>
     <ds:Transform Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#"/>
    </ds:Transforms>
    <ds:DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"/>
    <ds:DigestValue>v4KAARypSiXa4oieEjLYwVDQXlY=</ds:DigestValue>
   </ds:Reference>
  </ds:SignedInfo>
  <ds:SignatureValue>Nl/rBF2Mi6O7ET59dUhnkcCIFuKHRCrmvKfcDJ44hwVqbHlf4H/qKpn6vfSwfbV4+3e3gPSMlv4DeMDOFJb3s8EFEd1DcDNtala1DL1UInOMt2l3BSuLsHe/CCW2ps+vxkrlLGs6kJKqMQwH9gNMeLMXTkFD/K7tpMQ6osnzce4=</ds:SignatureValue>
 </ds:Signature>
 <samlp:Status>
  <samlp:StatusCode Value="urn:oasis:names:tc:SAML:2.0:status:Success"/>
 </samlp:Status>
 <saml:Assertion Version="2.0" IssueInstant="2012-05-31T16:16:12.147Z" ID="RcTzLA2ql9BtZC7aBx0aQkaj5Kh" xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion">
  <saml:Issuer>localhost:default:entityId</saml:Issuer>
  <saml:Subject>
   <saml:NameID Format="urn:oasis:names:tc:SAML:1.1:nameid-format:unspecified">joe</saml:NameID>
   <saml:SubjectConfirmation Method="urn:oasis:names:tc:SAML:2.0:cm:bearer">
    <saml:SubjectConfirmationData NotOnOrAfter="2012-05-31T16:21:12.150Z" Recipient="https://localhost:9031/sp/ACS.saml2"/>
   </saml:SubjectConfirmation>
  </saml:Subject>
  <saml:Conditions NotOnOrAfter="2012-05-31T16:21:12.150Z" NotBefore="2012-05-31T16:11:12.150Z">
   <saml:AudienceRestriction>
```


YOURWALLPAPER.COM

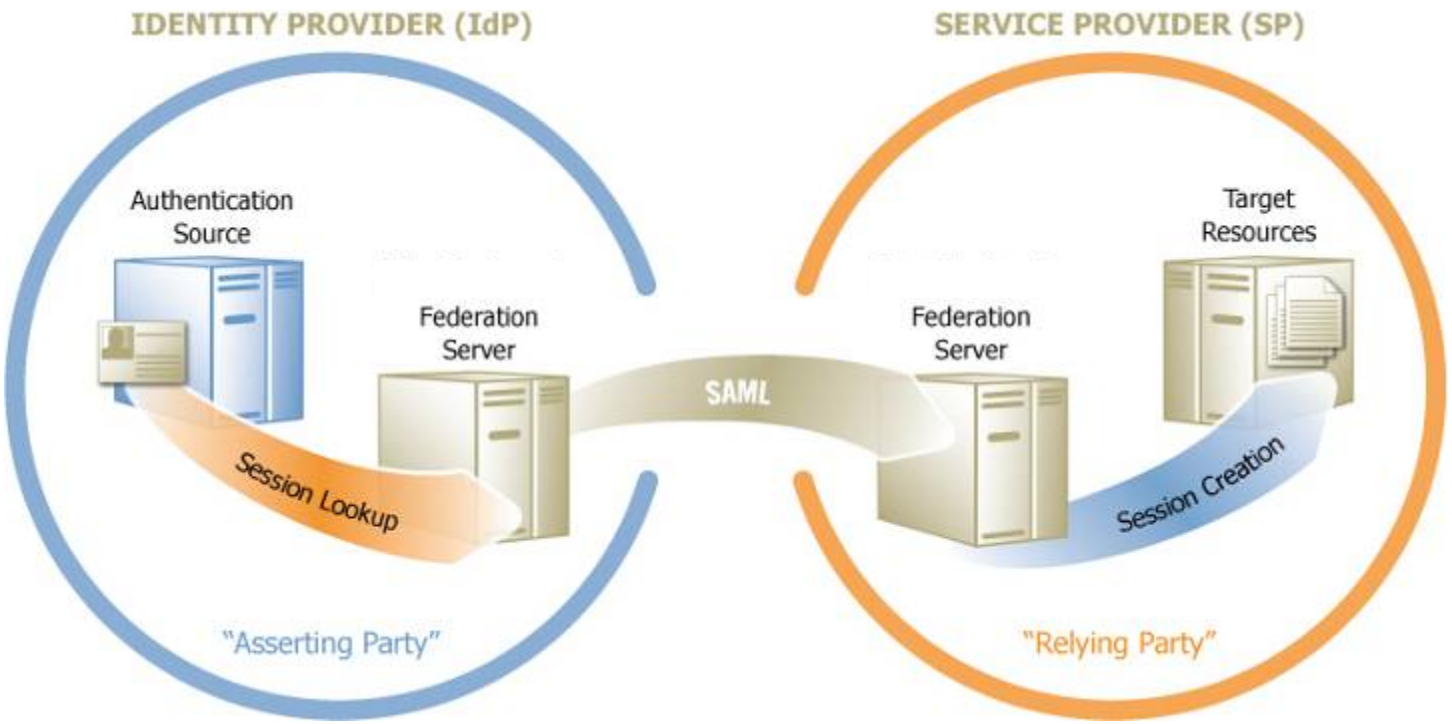
What is SAML, really?



- A XML-based framework for exchanging security and identity information.
- A “short-lived credential” whose lifespan is usually tied to a single browser session.
- Companies can share applications/resources without needing to adopt the same technologies for directory services, security, and authentication.
- Security information is expressed in the form of Assertions about Subjects, where a subject is an entity (human or computer) that has an identity in some security domain.
- Introduces the notion of two roles: An Asserting Party (AP) or Identity Provider (IdP) that provides authentication statements about an entity to a Relying Party (RP) or Service Provider (SP). The RP/SP provides the entity with access to its own applications based on trust of the original authentication.

Ping Identity®

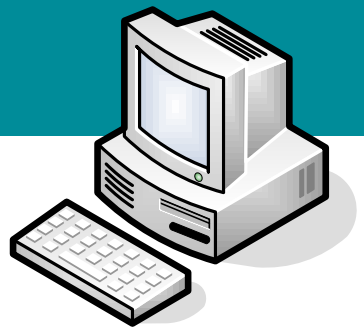
First & Last Mile Integration



- One-off solutions require maintenance and repeated integration
- IdP must integrate with Authentication Source
- SP must integrate with Target Resources

Ping Identity®

Web-based SSO (Simple Example)

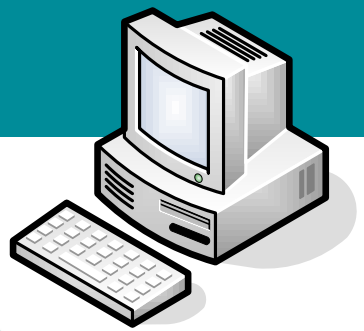


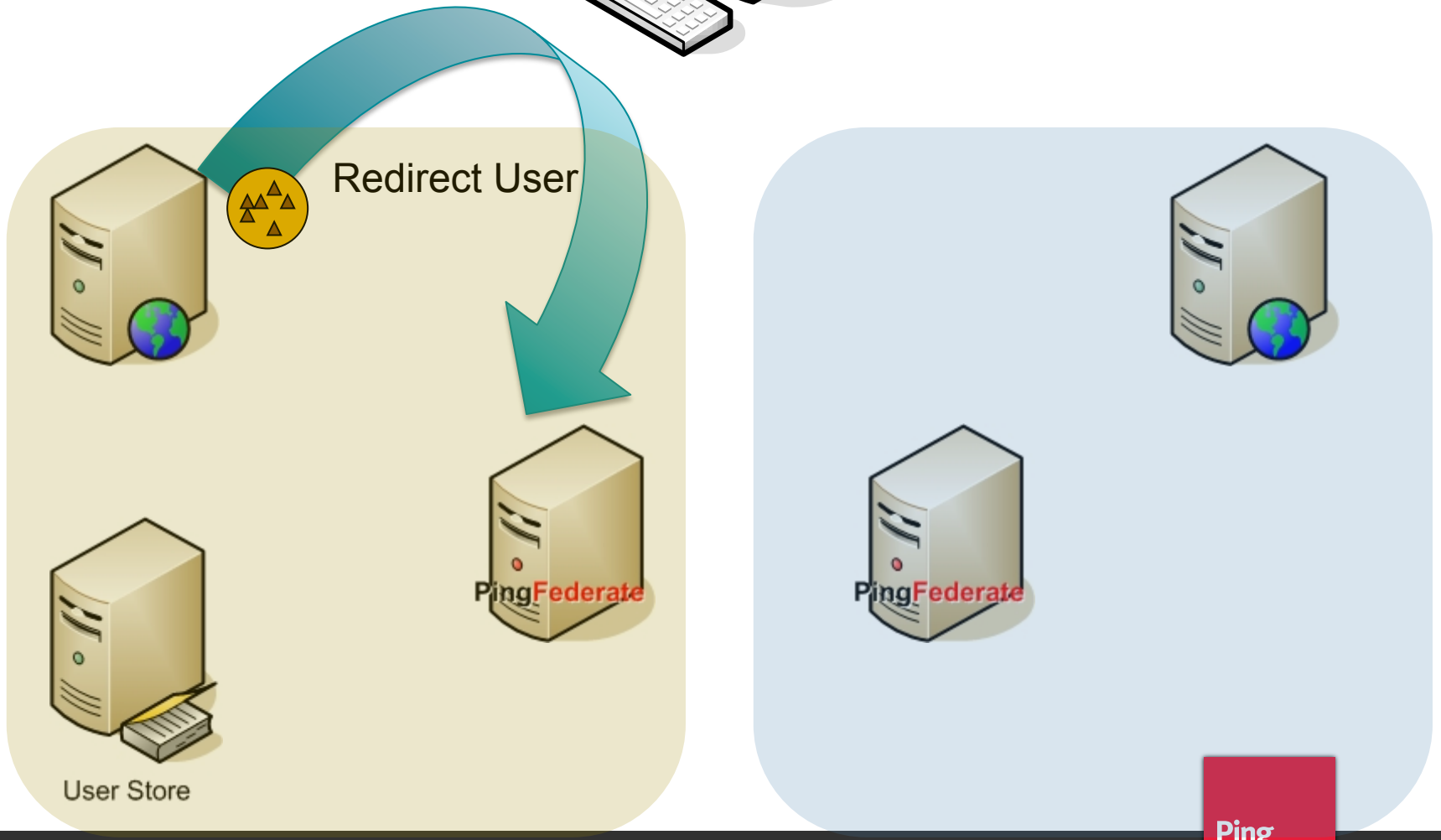
Access Web Portal

Identity Provider

Service Provider

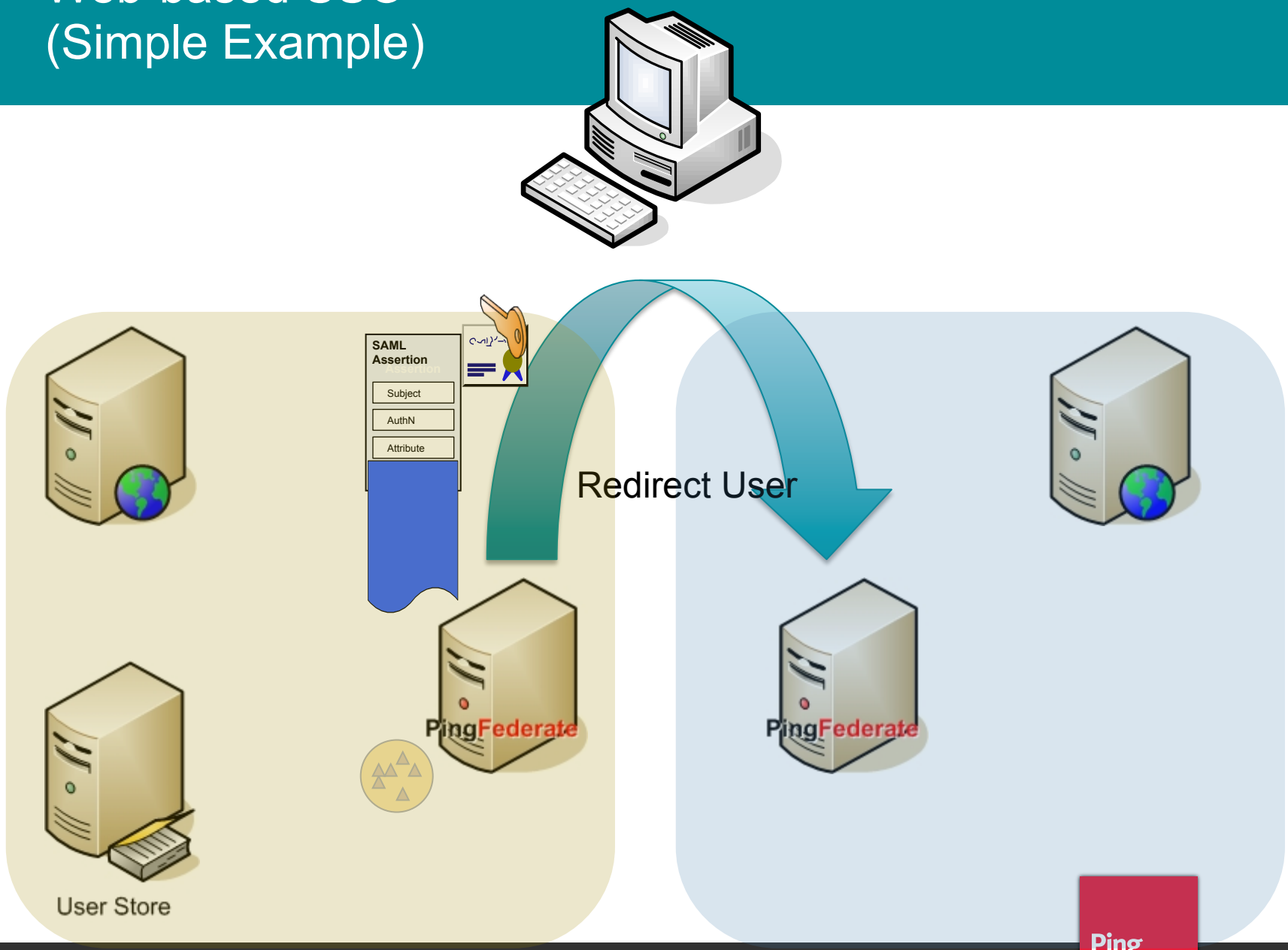
Web-based SSO (Simple Example)





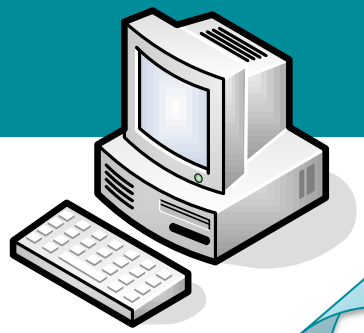
Ping Identity®

Web-based SSO (Simple Example)



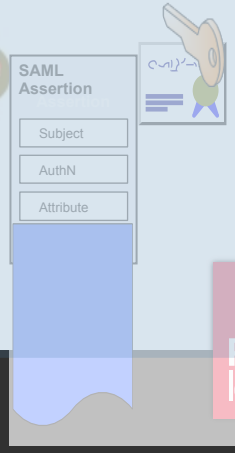
Ping Identity®

Web-based SSO (Simple Example)

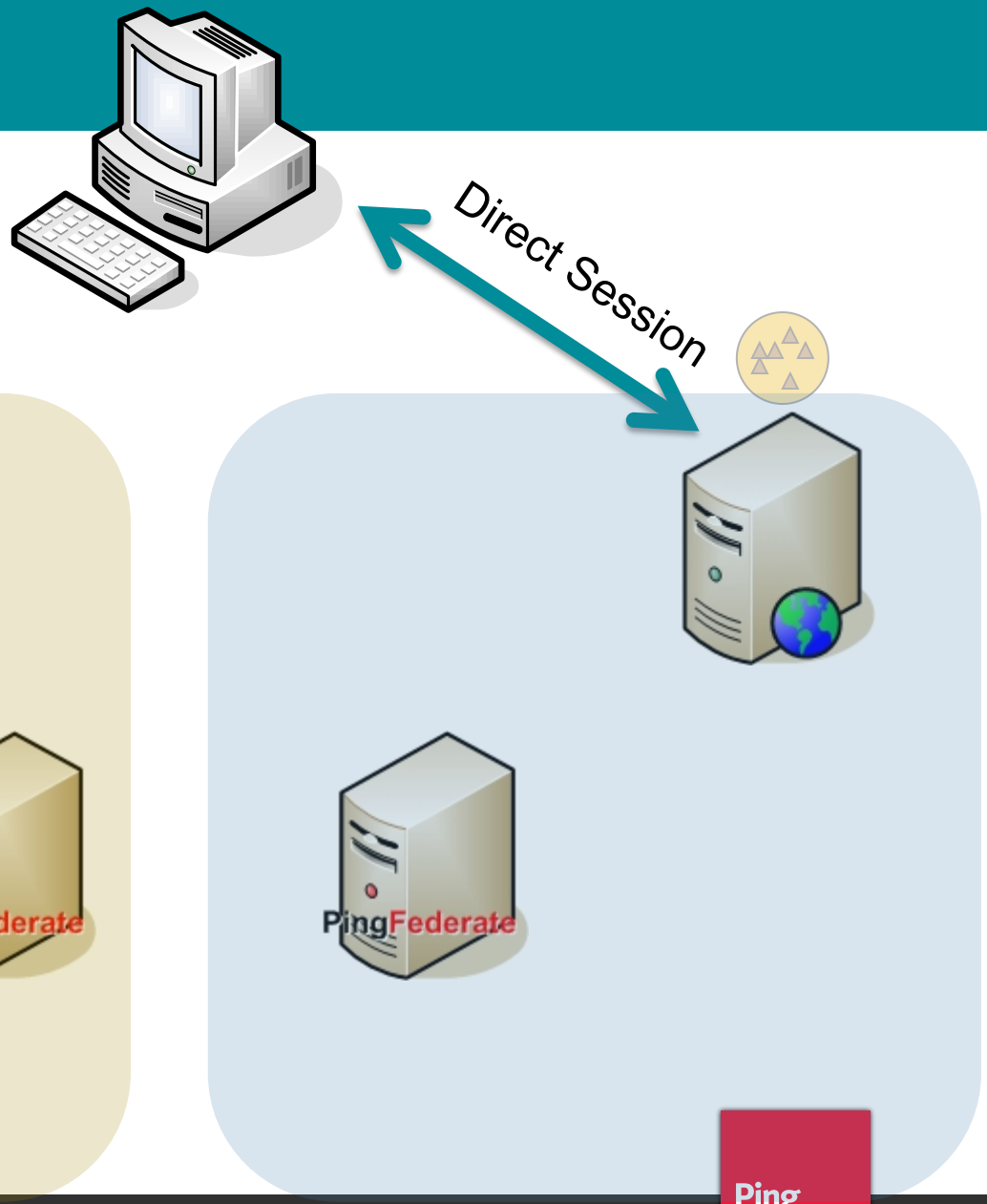


User Store

Redirect User



Web-based SSO (Simple Example)



Application Integration – Quick Example

```
Agent agent = new Agent("<PATH_TO_FILE>/agent-config.txt");

String username =
 (String)request.getSession().getAttribute("username");


 Map<String, String> userInfo = new HashMap<String, String>();


 userInfo.put(Agent.TOKEN_SUBJECT, username);


 String returnUrl = "https://<PingFederate-DNS>" +
 request.getParameter("resume");
 . . . .
 try {
    UrlHelper urlHelper = new UrlHelper(returnUrl);
    agent.writeToken(userInfo,response,urlHelper,false);
    returnUrl = (String)urlHelper.toString();
 }
```

Decision: SAML – Now what? How?

- Build In-house with Developer Toolkits?
  - Integration with all types of platforms (AuthN, portals, web servers)
  - Generating and Consuming “Tokens”
  - Support for multiple protocols and token types???
  - Multiple profiles, certificates
  - Ability to scale???
- Use a “Stack” Vendor?
  - Must implement full Identity and Access Management (IDM/IAM)
  - **Proprietary SDK for developers**
  - Cost (dollars and time) of consulting services to implement
  - Often requires a homogenous environment
- Are there any other options?

Ping Identity®

But what about…

Additional capabilities beyond consuming and generating tokens?

- Secure API Access internally or with partners; SOAP or REST
- Provisioning of users to cloud services
- Secure Mobile Access; support for Mobile Apps
- Accepting Social Identities; leveraging Facebook, Twitter, Google, etc.
- Integration with Strong Authentication
- Leveraging existing attribute sources; for authorization

There are more protocols to consider than just SAML 2.0…

- SAML 1.X, WS-Federation, SCIM, WS-Trust, OpenID, OAuth 1.0a, OAuth WRAP, OAuth 2.0, OATH, XACML, OpenID Connect

Ping Identity®

and then there are the Enterprise capabilities

- Integration with existing infrastructure
  - IdM systems, Authentication Systems, Portals, databases, commercial applications, application servers, web servers
  - Staying current with new releases
- Scalability and High Availability
  - Managing larger numbers of connections, clustering for failover, disaster recovery
- Meet Internal Security Requirements
  - Third party assessments, penetration analysis, secure implementation of the specifications
- Operational Processes
  - Logging, Monitoring, migration from dev to prod environments, support

Not to mention…

Customer, Partner, Supplier Requirements:

- Interoperability Testing and Troubleshooting
  - Validation against each specification?
  - Troubleshooting implementation of the spec with every partner?
  - Advanced logging for troubleshooting?
- Third party security audits
  - Was the specification implemented properly?
  - Were known security vulnerabilities addressed?

What does it take to build your own?

- The Task List*…

1. Document the project needs
2. Research
3. More research
4. Design the solution
5. Research
6. Redesign to meet needs (second pass)
7. Build the enterprise solution
8. Test in DEV
9. Fix issues and redeploy in DEV (repeat 7, 8, and 9 until good)
10. Move to QA and test (Developers learning to integrate into App)
11. Fix issues and redeploy in DEV and QA (repeat 10 and 11 until good)
12. Move to UAT and test (Developers still learning to integrate)
13. Fix issues and redeploy in DEV, QA, and UAT (repeat 12 and 13 until good)

*Actual tasks executed by Ping Identity customer before choosing PingFederate

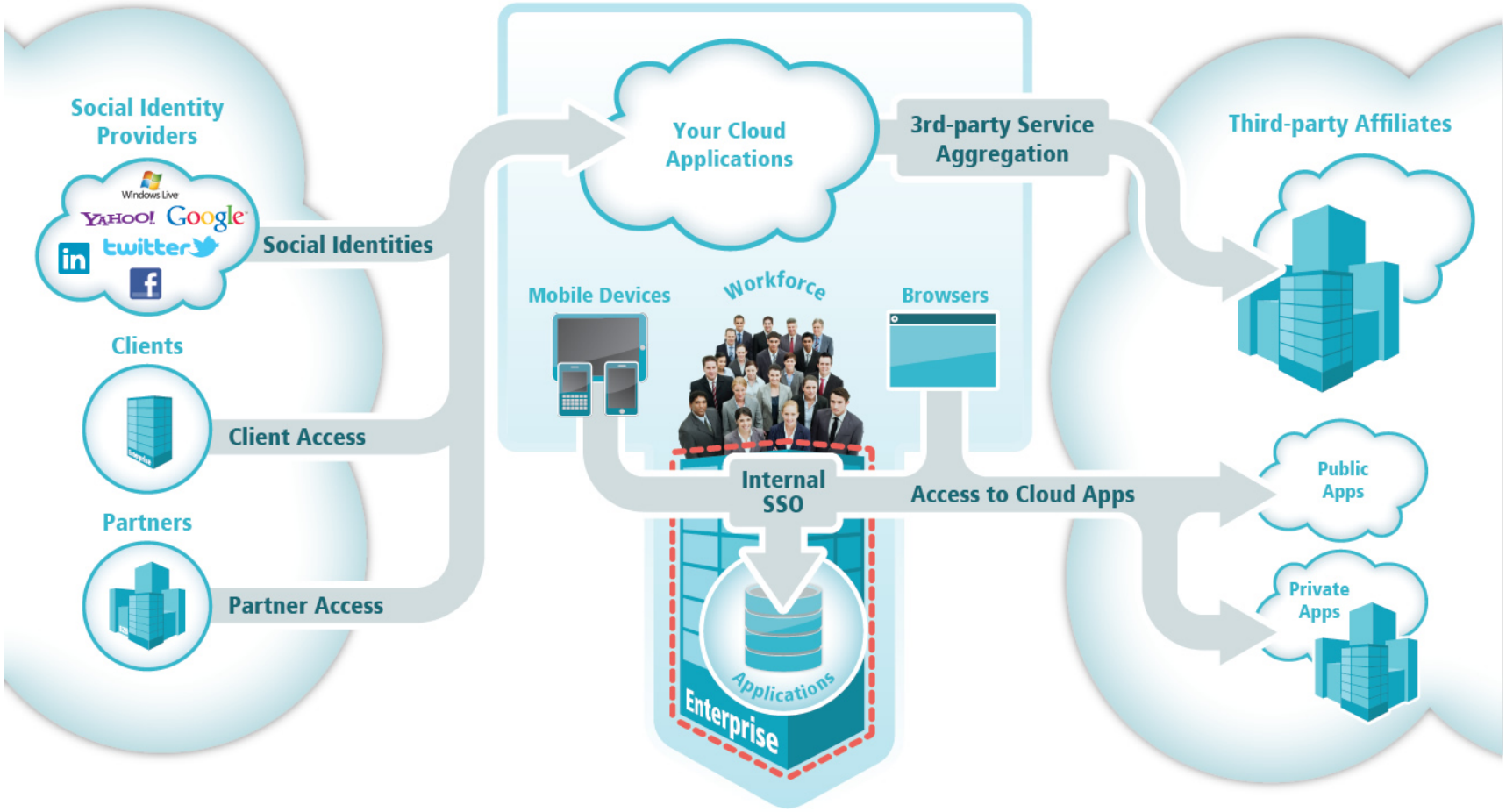
Ping Identity®

30 days later*…

- **Delivered on Step 8, Test in Dev**
- **Support for SAML 2.0 only**
- **Identity and attribute data from a JDBC source only**
- **Standard Connection took one week each to configure**
- **Non SAML 2.0 connections required custom development**

*Actual results from Ping customer before choosing PingFederate

Evolution of Federation, Part 2



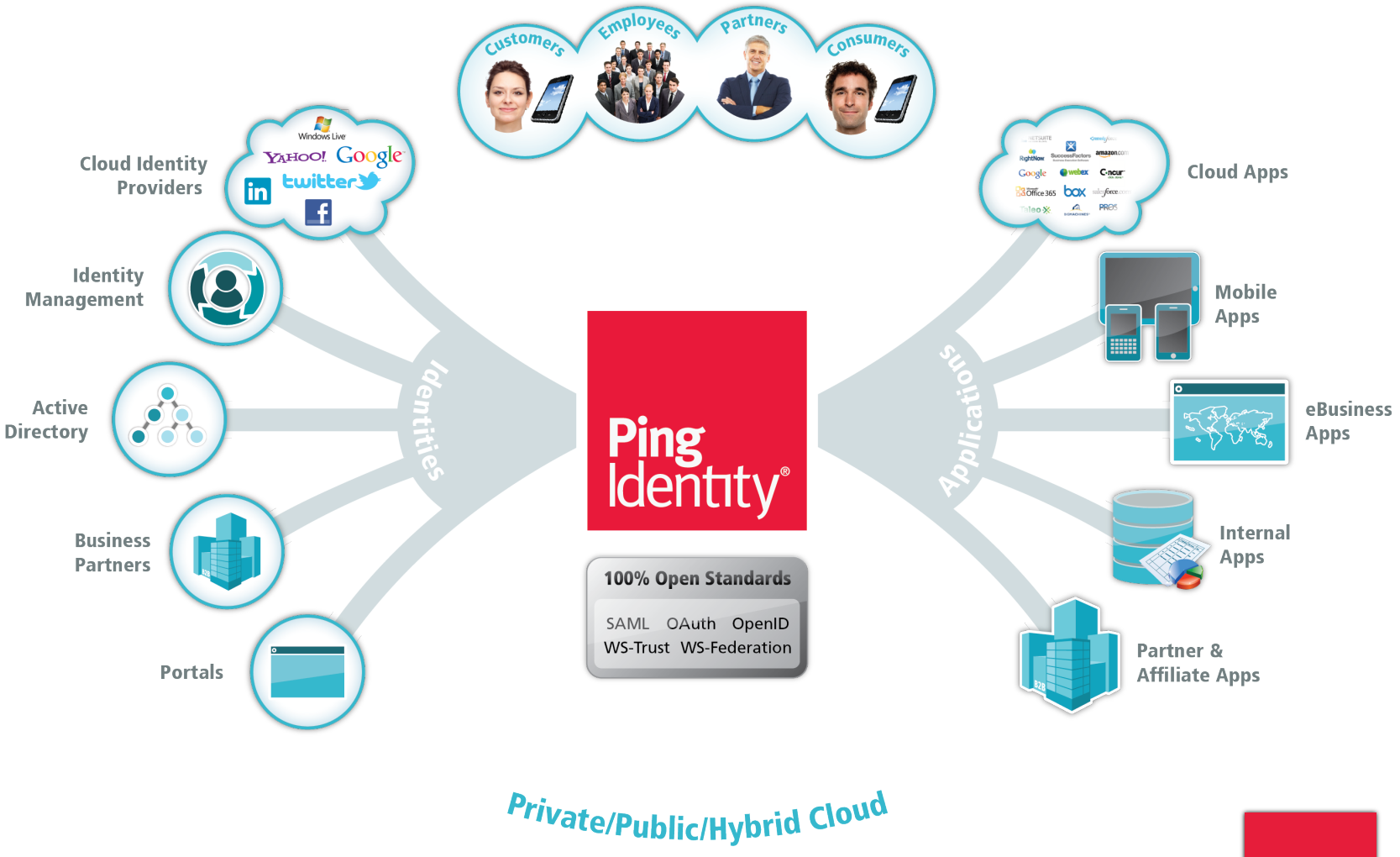
Ping Identity

Secure the Cloud – Best Practices

1. **Separate identity from applications** – centralize IT control of identities and access
2. **Eliminate passwords** – don't sync, replicate or hide them
3. **Adhere to standards** – leverage secure and proven identity standards to maximize interoperability and scale
4. **Leverage existing identity infrastructure** – look for supported integrations and standards to avoid costly, fragile or high maintenance architectures
5. **Avoid purpose-built identity silos** – design a single identity architecture that supports all required use cases

Ping Identity®

The PingIdentity Advantage



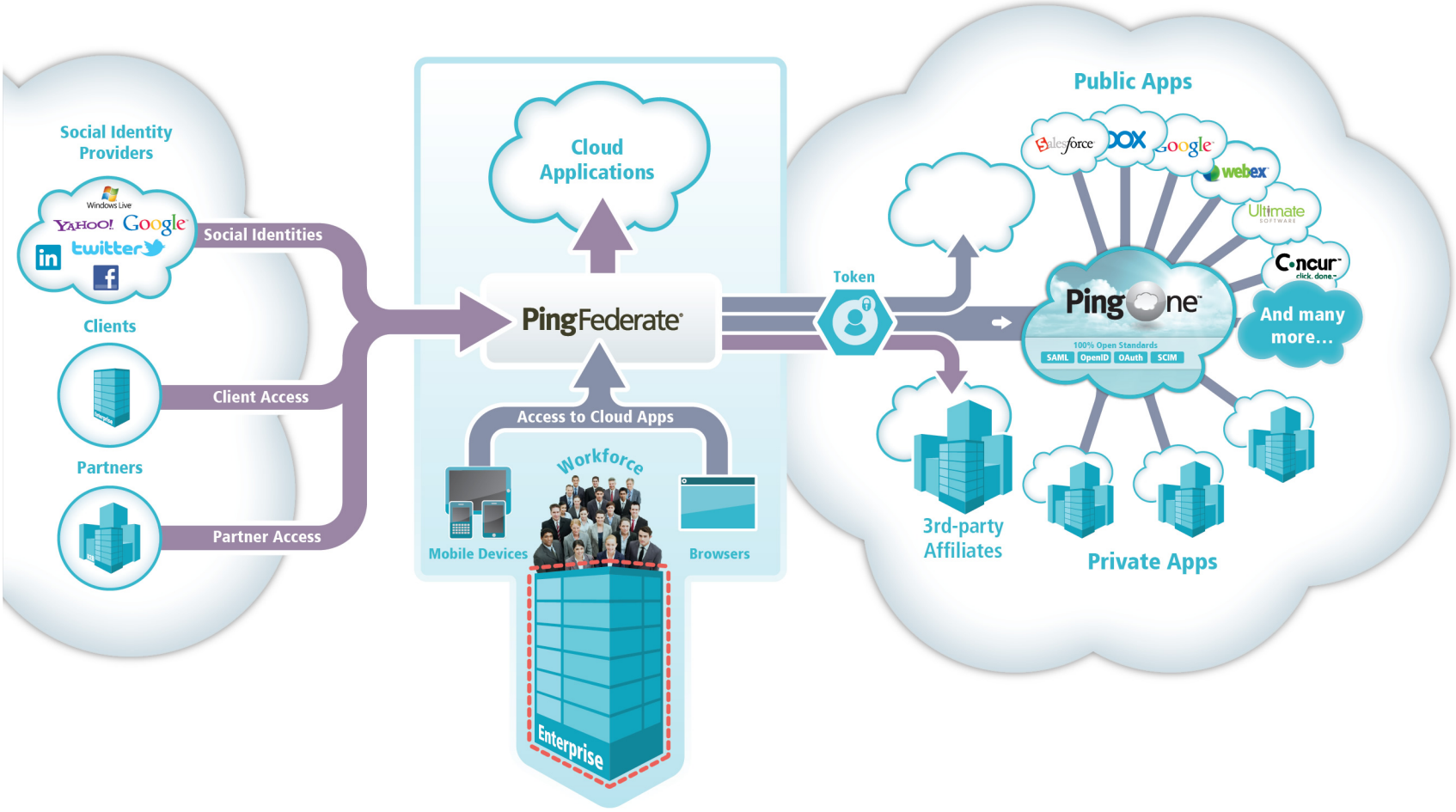
Ping Identity®

PingIdentity Customers

825+ enterprises, government agencies and services providers worldwide trust Ping Identity – including 42+ of the Fortune 100.

Finance	Healthcare	Consumer	Manufacturing	Media
Wells Fargo	Genentech	Best Buy	Cisco	Disney
Bank of America	Kaiser Permanente	Marriott	Dell	CBS Interactive
JPMorgan	UnitedHealthcare	SC Johnson A Family Company	BMW	Houghton Mifflin Harcourt
SunGard	Aetna	Walgreens	3M	Dow Jones
Visa	Blue Cross Blue Shield	Ahold	GE	Comcast
PayPal	HCA Hospital Corporation of America	Pepsico	Black & Decker	Thomson Reuters
RBC	Merck	Kraft Foods	Land Rover	Time
E*Trade	Lilly	Diageo	Volvo	NBC
Fidelity Investments	Pfizer	Target	EADS	Discovery Communications
Morgan Stanley	Premera Blue Cross	McDonald's	Chrysler	
			Boeing	

Secure the Cloud. Free your Business: A Case Study



Ping Identity®

“1” stands for…

PingIdentity is the **ONE** company you can turn to for

SIMPLE

SECURE

PROVEN

federation solutions!

PingFederate Cloud Identity Management Software

Administration Console

Management Services

Integration Kits

SaaS Connectors

Cloud Identity Connectors

Token Translators

SDKs

Cloud Single Sign-On & Federated Identity

Secure Mobile Access

Automated Cloud User Provisioning

API Security

Runtime Services

Logging & Monitoring

Ping Identity®

Beyond SAML – Examples for discussion

- **WS-Trust (Secure Token Service)**
- **oAuth (Open Authentication)**

Numbers that really matter…

250 Dedicated Employees

99 % Customer Satisfaction

10 Years of Federation Focus and Developing Standards

1 PingOne.com

Questions and Answers

PingFederate®

PingFederate® CloudDesktop

PingOne™

Ping Identity

The **Cloud Identity Security** Leader™

Nathan Sargent
nsargent@pingidentity.com