

CREATING A FEDERATED AUTHENTICATION TRUST

The process of creating a federated authentication trust is much more than what trust protocol you'll be using. There are a number of legal, business and technical issues that must be clarified before implementation. This paper highlights some of these areas and points readers to more detailed resources.

TRUST SCOPE DOCUMENT

The first thing that needs to be created is a trust scope document. This must define:

1. What the overall goals are for the trust
2. Describe the participants for the trust
3. Describe the identity registration requirements for each party
 - a. Are background checks required?
 - b. What pieces of identification are required?
4. Describe the identity provisioning process for each party
 - a. How are users provisioned?
 - i. What is the time frame for provisioning?
 - b. How are user role changes made?
 - i. What is the time frame for role changes to be made?
 - c. How are users de-provisioned?
 - i. What is the time frame for deprovisioning?
 - d. How are identities archived?
 - i. How long are identities archived for?
 - e. What is the responsibility of each party for the overall provisioning, role change, termination and archiving?
5. Describe the identity authentication requirements for each party
 - a. What authentication assertions are going to be used for SSO (Single Sign On)
 - b. What attribute assertions are going to be used?
 - i. Roles, titles, credentials etc.
 - ii. What is the privacy policy for each of these attributes
6. Describe the authorization requirements for each party
 - a. What are the authorization assertions to be used?
 - b. What are the authorization policies for a specific user and resource
 - c. How are authorization policy changes going to be agreed on in the future?
7. Describe the audit requirements for each party
 - a. What audit information is each party required to hold?
 - b. Is there a central audit repository?
 - c. What is the time frame for the audit archive?
 - d. What is the audit data format each party must use?
8. Describe use case scenarios for each party
 - a. Describe the parties
 - b. Describe the situation
 - c. Describe the interactions, one step at a time

CREATING A FEDERATED AUTHENTICATION TRUST

- d. Describe the use case from the parties perspective
- e. Describe the use case from the user's perspective
9. Describe the authenticated trust management
 - a. Define the management requirements
 - b. Define the management roles
 - c. Define what each party must do for management
 - d. Describe how any changes to management need to be agreed upon and communicated between the parties

FEDERATION AGREEMENT DOCUMENTS

Technical:

Federation Standards:

1. Federation Standards to be used:
 - a. WS-Federation
 - b. Liberty Alliance
 - c. SAML
 - d. Shibboleth
 - e. Other
2. What version of the specification will be used?
3. Identity attributes to be required
4. Are artifacts or post profile used?
5. Protocol specifics
6. Encryption level to be used?
7. Digital signatures required?
8. Hash standard?
9. Other?

Communications Security:

1. What channels are to be encrypted?
2. What data is to be encrypted?
3. Which encryption technology is to be deployed?
4. Other?

Certification:

1. What is the certification process for each party?
2. What are the credentials to be acknowledged?
3. Are certificate authorities (CA) to be used?
4. Which CA's will be accepted?
5. What is the CA revocation process that is to be followed?
6. What are the management rules for certificates?
7. What are the lifecycle rules for keys and credentials?
8. What is the required Certificate Practice Statement?
9. What is the security protection of keys?
10. What are the signing levels for sessions and/or messages?

CREATING A FEDERATED AUTHENTICATION TRUST

Authentication:

1. What are the risk assurance levels to be used for each type of service?
2. What is the authentication strength to be used for each level of risk?
3. Who are the approved vendors of authentication?
4. What is the approved assertion timeout?

Identity Attributes:

1. Are LDAP directories to be used?
2. What directory services are approved?
3. Attribute definitions
4. Rules for each attribute
5. Protection requirements for each attribute
6. Account mapping

Policy Management

1. What access policies are agreed to?
2. What are the roles?
3. What are the applicable rules for the roles?
4. What are the associated access rights?
5. What are the policy exceptions:
 - a. Failed authentication?
 - b. Failed authorization?
 - c. Dropped connection?
 - d. Other?
6. What is the policy expression language for defining policies?
7. What are the actions for successful post-authentication?
8. Are any attributes to be passed to the applications?
9. What are the session inactivity timeout policies?
10. Does it vary by application?
11. What are the session logout policies?
 - a. Is this applicable across domains or not?

Audit Requirements

1. Is there a central audit service?
2. What are the requirements for each participating party?
3. What are the audit data security requirements?
4. What is the audit log formats?
5. What is the audit log methodology for releasing audit logs for audits?
6. How often are audit reviews held?

Privacy Policy

1. State applicable privacy legislative or regulatory requirements
2. What are the trusted federation technical requirements to adhere to each legislative or regulatory requirement?

CREATING A FEDERATED AUTHENTICATION TRUST

Error Handling

1. What are the required alert response timelines?
2. How are DoS attacks responded to?
3. What is the process for handling unauthorized users?
4. How are reject messages handled and processed?
 - a. Is this altered due to policy or practice issues?
5. How are reject messages handled and processed for expired user credentials?
6. How are reject messages handled and processed for expired Identity Provider credentials?

Security

1. What are the firewall requirements?
2. What are the anti-virus requirements?
3. What are the approved security protection techniques?
4. What are the required patch levels?
5. What is the required time to install patches after they're released?

Risk and Liability Limits

1. What is the limit on liability between federating parties for:
 - a. Security breaches
 - b. Identity theft
 - c. Errors
 - d. Omissions
 - e. Service level agreement failure
2. What are the liability shift conditions:
 - a. Deficient authentication
 - b. Authentication levels
 - c. Outstanding alerts for identities
 - d. Inadequate data
 - e. Compromised data
 - f. Out of compliance
 - g. In compliance
 - h. Access policy breach
 - i. Authentication hardware failure
 - j. Service level agreement failure
 - k. Other

CREATING A FEDERATED AUTHENTICATION TRUST

Contractual

1. What is the time of the agreement?
2. How are modifications to the agreement to be handled and processed?
3. Defining legal jurisdiction for the agreement?
4. Legal name of each party
5. Notification of action process

These are just the highlights of creating a federated trust agreement and implementation between two or more parties. As you can see, there is a lot more than buying a product and implementing. Your legal department must be involved early on in the discussions.

OTHER RESOURCES ON FEDERATED AUTHENTICATION

1. One of the best resources is the [Ping Identity](#) web site. Their [information library](#) contains checklists for federated trust, sample legal agreements as well as numerous other papers outlining federated authentication. You must register for free to receive the papers.
2. [Liberty Alliance](#) also has a vast number of [resources](#) for identity federation. These include developer resources, need development resources and all sorts of whitepapers covering a wide range of topics.

ABOUT THE AUTHOR:

Guy Huntington, President of Huntington Ventures Ltd., has many years of experience leading large, complex, Fortune 500 identity projects. His work has included leading Boeing's single sign on, Capital One's single sign on, Capital One's Sarbanes-Oxley provisioning project and Kaiser Permanente's web single sign on review.

He maintains a website on authentication at www.authenticationworld.com. He also maintains an authentication blog available off his website. He can be reached at guy.huntington@authenticationworld.com or by phone at 604-921-6797.