ABFAB
Internet-Draft
Intended status: Informational
Expires: September 26, 2012

J. Howlett
Janet
M. Wasserman
Painless Security

March 25, 2012

Trust Router Problem Statement
draft-howlett-abfab-trust-router-ps-02.txt

Abstract

This document is a problem statement for a Trust Router Protocol. A Trust Router Protocol is needed to support large, multihop ABFAB federations, without the need for credentials to be configured for every pair of Identity Providers and Relying Parties.

Status of This Memo

Copyright Notice

Table of Contents

1. Introduction

The ABFAB architecture [I-D.lear-abfab-arch] describes an access management model that enables the application of federated identity within a broad range of use cases. This is achieved by building on proven technologies and widely deployed infrastructures. Some of these use cases are described in [I-D.ietf-abfab-usecases].

In the canonical case, an ABFAB transaction only implies two organizations: an Identity Provider (IdP) and a Relying Party (RP). In this simplest case of a bilateral connection, the amount of configuration needed by both partners is very small; probably just an AAA credential and the peer system's host name for the other party.

However, in practice an community may consist of more than two partners. In the case where bilateral connections are used, the amount of configuration at each partner increases in proportion to the number of connections. As the number of partners increases, the amount of configuration churn may become too onerous to manage. Also, the operational costs of managing that configuration information is borne, to an unreasonable degree, by the RPs. When a new IdP is added to a partnership, it is necessary for all of the RPs to update their configuration information before the new IdP's users will have full access to the services accessible to the partnership.

There is also an operational need to separate the authentication process from the creation of a partnership, so that existing credentials my be leveraged for new communities, and so that new communities can be formed with minimal operational and infrastructure costs.

This document is a problem statement for a Trust Router Protocol. A Trust Router Protocol is needed to eliminate the need the need for a bilateral exchange of credentials between each IdP and RP.

A Trust Router Protocol allows a new partner to be added to an ABFAB community by peering with any member of the Trust Router network, instead of requiring configuration changes by every partner who may wish to connect with the new partner. A Trust Router protocol addresses the problems described in this document by distributing information about existing trust relationships within the partnership, thus avoiding the operational costs and limitations of using a Public Key Infrastructure (PKI).

This document is broken into two sections: High-Level Problems and Specific Problems. The High-Level Problems section describes the problems that the Trust Router Protocol has been designed to address at a conceptual level, and the Specific Problems section discusses a

more concrete set of problems that the Trust Router Protocol is intended to address.

2. Terminology and Concepts

This section defines terms and concepts that will be used through the rest of the document while exploring the problems that could be solved by a trust router protocol. Although this section does not define any problems, per se, a trust router protocol would be expected to support all of the concepts discussed here.

- Partner: An organization that participates in an ABFAB federation as an IdP, an RP or both.

- Community: A group of IdPs and RPs that are associated with each other for a specific purpose.

- Community of Interest: A community that is formed to share a set of resources and services.

- Community of Registration: A community that provides registration and authentication services for its members.

3. High-Level Problems

3.1. Connecting your Partners

Organizations want to be able to connect to an arbitrary number of partners without being overwhelmed by configuration management of many bilateral connections.

3.2. Identifying your Partners

It is not generally sufficient to simply configure a partner. In most cases, it is also necessary for organizations to have confidence that the configuration that they have for their partner(s) actually corresponds to their partner(s) and is not, for example, an attacker claiming to be their partner. Unfortunately identifying partners and binding them cryptographically to the corresponding configuration can be very expensive.

Organizations want to minimise the cost of validating their partners' identities, and of proving their own identity to their partners.

3.3. Knowing your Partners

Organizations and their partners generally interact within the context of a particular context. The context can be established in a

number of ways; for example:

- A pair of organization may have a formal business relationship that unambiguously establishes the nature of the relationship between the partners (for example, in the case of a supplier's relationship with a customer). In this case, the customer's ABFAB-based interactions with the supplier are governed by this business relationship.

- A group of organization may also share a formal business relationship (for example, a number of suppliers within a manufacturer's supply chain). In this case, the business relationship might govern the ABFAB-based interactions between the suppliers, and the suppliers and the manufacturer.

- A group of organizations may not share a formal business relationship but instead share common best practices. In this case, the best practices might govern the ABFAB-based interactions between these organizations.

Given the potential diversity of contexts, organizations need to know which context is in force for a particular ABFAB-based transaction and apply policy that controls which entities within an organization are permitted to operate within particular business contexts.

3.4. Policing and Managing Policy

Organizations want to have effective tools for policing and managing policies controlling ABFAB-based transactions with their partners.

4. Specific Problems

4.1. Many IdPs, Many RPs

It is fairly easy to see how ABFAB, without Trust Routers, could be deployed in a small federation with stable membership, or even in a large federation with a single RP that provides services to all of the other members, such as an industry consortium.

However, there are operational problems that arise when ABFAB is used in a federation with a large number of RPs providing services to an even larger number of IdPs. In these cases, it can be challenging to manage the credentials that need to be exchanged, and manually configured, between each RP/IdP pair.

4.2. Frequent Changes in Membership

It must be possible to support changes in membership (adding new partners, or removing former partners) with minimal operational effort, and without requiring manual configuration changes that could result in new partners having delayed or incomplete access to services, or former partners retaining some access to services beyond the end of their membership.

4.3. Minimal Costs for Adding a New Partner

There is a need to support large federations in a cost-effective manner. This includes minimizing the operational costs of adding a new partner (either an IdP or RP) to an existing community. Without Trust Router, the operational costs of adding a new partner to an existing community might be quite high -- requiring credential exchange between a large number of parties, and requiring manual configuration changes on a large number of different systems.

4.4. Costs Incurred by the Party that Benefits

Without Trust Routers, a high portion of the operational cost related to adding and removing partners is born by the RPs, who need to maintain bilateral credentials for each IdP whose users can access the services provided by the RP. This is fine in a case where a single RP provides services to a group of IdPs that pay for membership in the community, or pay for access to specific services. However, in a less-centralized partnership the costs of exchanging credentials with each IdP could serve as a disincentive for organizations to provide services to the community and/or result in cases where an RP is unwilling or unable to incur the costs of providing access to new partners. Therefore, it is important that we devise a mechanism where the operational costs are distributed to the organizations that are receiving benefit from incurring the costs.

4.5. Minimal Costs for Forming a New Community

It should be possible for a group of potential partners to form a new Community of Interest with minimal intrastructure and the lowest possible operational expense.

In order to minimize start-up costs, it should be possible to leverage existing shared credentials and use those credentials for a new Community of Interest.

Practically, this resolves to two problems:

- It must be possible to create a new Community of Interest that uses credentials from one or more existing Communities of Registration.

- It must be possible for a partner to join multiple Communities of Interest using a shared Community of Registration, and for different entitities (such as users or servers) within a partner to participate in different Communities of Interest. Practically, this means that information about the Community of Interest in use needs to be transmitted to an IdP, so it can be used as part the authentication process.

4.6. Supporting Community Growth

It should also be possible for Communities of Interest to grow to encompass more partners, partners in different regions of the world, or partners who have different Communities of Registration available to them.

It must, therefore, be possible for a single Community of Interest to be serviced by multiple Communites of Registration. While it might be necessary for any given RP/IdP pair to share at least one Community of Registration, it should not be necessary for all of the partners within a given Community of Interest to share a single Community of Registration.

4.7. Multi-Role Participation

It must be possible for a single partner to participate as both an RP and an IdP within a single community (either a Community of Interest or a Community of Registration).

4.8. Multi-Purpose Communities

It also must be possible for a single community to serve both as a Community of Interest and as a Community of Registration. An use case for this requirement woudl be a Community of Registration that provides services to its own customers, perhaps for maintenance of their own Community of Registration membership.

4.9. Deployment Challenges with Public Key Infrastructure

Deployment problems with Public Key Infrastructure (PKI) make it unsuitable for use by many ABFAB communities. The costs are prohibitive for the use of ABFAB federations in many educational environments, and the policies of PKI Certificate Authorities are not well-aligned with the policies of many communities. Also, the support costs associated with having every every IdP generate keys

and provide a public key (but not their private key) to each RP in a partnership may be prohibitive.

5. Security Considerations

This is a problem statement document, not a protocol definition, and therefore it does not define anything with its own Security Considerations. The Security Considerations for the protocols discussed in this document are (or will be) provided in the documents defining those protocols.

6. Acknowledgments

This document was written using the xml2rfc tool described in RFC 2629 [RFC2629].

The following people have provided useful feedback on the contents of this document: Sam Hartman.

7. Informative References

[I-D.lear-abfab-arch] Howlett, J., Hartman, S., Tschofenig, H., and E. Lear, "Application Bridging for Federated Access Beyond Web (ABFAB) Architecture", draft-lear-abfab-arch-02 (work in progress), March 2011.

[I-D.ietf-abfab-usecases] Smith, R., "Application Bridging for Federated Access Beyond web (ABFAB) Use Cases", draft-ietf-abfab-usecases-01 (work in progress), July 2011.

[I-D.mrw-abfab-multihop-fed] Wasserman, M., Tschofenig, H., and S. Hartman, "Multihop Federations for Application Bridging for Federation Beyond the Web (ABFAB)", draft-mrw-abfab-multihop-fed-01 (work in progress), July 2011.

[RFC2629] Rose, M., "Writing I-Ds and RFCs using XML", RFC 2629, June 1999.

Authors' Addresses

Josh Howlett
Janet

EMail: josh.howlett@ja.net

Margaret Wasserman
Painless Security
356 Abbott Street
North Andover, MA 01845
USA

Phone: +1 781 405 7464
EMail: mrw@painless-security.com
URI: http://www.painless-security.com