Barriers to Service Providers - Recommendations

Barriers for Service Providers

Overview

Research and education federations can now claim to be well embedded within their respective communities, and most of the national federations that participate in REFEDS have signed up a large proportion of their institutional (IdP) constituents. Although external service provider representation is growing within federations, there continue to be significant barriers for SPs wishing to join multiple federations. Recent experiences of two small organizations - the Shibboleth Consortium and TERENA - have identified a number of pain points and problems for SPs wishing to join federations. This document provides an overview of these problems and makes a series of recommendations for REFEDS to consider in order to breakdown these barriers.

Many of the barriers will not apply to all federations and some may not effect some federations at all. No criticism is intended of any single federation by this investigation, which has attempted to view the federation approach purely from a Service Provider perspective.

Recommendations Summary

1. REFEDS should maintain a watching brief on PEER with a specific remit of understanding the PEER-SP-FEDERATION relationship .
2. REFEDS should consider creating the supporting material for eduGain as described and develop common clauses descriptors for federation policies..
3. REFEDS should pursue the identification of one-off clauses in federation agreements as part of the work on common clauses..
4. REFEDS should maintain a watching brief on data protection issues through appropriate members (E.G. ANDREW CORMACK).
5. REFEDS should eatablish which of the federations classified as unknown (below) currently require sponsorship letters and encourage federations to move to a model of 'verification if required' rather than upfront sponsorship.
6. The options described for improving fees structures within federations should be debated by REFEDS at its spring meeting in Prague, 2011.
7. REFEDS should look to document acceptable IdP and SP software used within federations, per federation.
8. REFEDS should look to document current practises in certificate acceptance and management within federation and make appropriate recommendations to federations.
9. REFEDS should actively promote Federation Labs as a place for Service Providers to test implementations.

1. Multiple registry of entity information

1.1 Background

The problem faced by SPs at the moment in this area is clear - if they make any changes to their entity metadata they have to register that change with each and every federation - potentially 26 if all the federations currently regsitered on the REFEDS wiki are required. This creates an unnecessary burden, and the processes for updating information are subtly different in each case.

1.2 Possible solutions

The PEER project has been established to tackle this very problem. No further action is proposed at this point in time, but this REFEDS workarea should keep a watching brief on ensuring that PEER develops a workable model for SP use and interaction. Specific attention should be made to differences in how federations might expect SPs to use PEER, and any federation joining processes that will be expected.

RECOMMENDATION:
MAINTAIN A WATCHING BRIEF ON PEER WITH A SPECIFIC REMIT OF UNDERSTANDING THE PEER-SP-FEDERATION RELATIONSHIP.

2. Multiple legal documents

2.1 Background

Education and Research Federations by and large seek to provide a level of behavioural trust amongst their participants as well as brokering technical trust. In order to achieve this, it is necessary for each federation to have a policy or rules of membership that participants are expected to sign up to. A study by JISC among emerging federations in 2008 delivered the good news that most differences in federation policy were geographical or cultural rather than legal in nature. However, little has been done since this report to work on the differences in federation policy and provide clear guidance for SPs.

2.2 Possible Solutions

a) **Role of eduGAIN**. eduGAIN as a vehicle will break down the need for SPs to join multiple federations but in turn creates a complex set of information building for SPs in order to discover which of their IdPs can access resources through the interfederation metadata. There is a need for good documentation for Service Providers regarding the use of interfederation metadata. The business impact of interfederation should also be considered for fee charging federations.

b) **Common Clauses** Many of the federation policies have very similar clauses that are simply described in different ways and in a different order. A 'creative commons' style analysis of the clauses with a plain english description of each point and a breakdown of where this sits with a federations policy would be a useful tool for a Service Provider.

RECOMMENDATION:
REFEDS SHOULD CONSIDER CREATING THE SUPPORTING MATERIAL FOR EDUGAIN AS DESCRIBED ABOVE AND DEVELOP COMMON CLAUSES DESCRIPTORS FOR FEDERATION POLICIES

3. One-off clauses

3.1 Background

One-off clauses are a symptom of the differing document structures as described in section 2 of this report, but present a very specific requirement of 1 or a small number of federations that are not typically seen across the board. In some cases, these clauses simply represent a new learning curve for SPs as they attempt to understand the requirements of the various federations. In other cases, the clause may present a significant barrier or challenge that will prevent a provider joining a specific federation.

Examples of these known to date are:

- Requirement by InCommon for the SP to hold a $3million insurance policy. For some small companies, this bar is far too high. Most federations do not have such a requirement as federation policies make it clear that liability is strictly limited.
- Requirement by Renater that will not allow third-party SPs to pass PII. Whilst all federations are very clear in their policies that data protection must be followed, most leave it to the IdP and SP to ensure that PII is required and consent as appropriate has been given for passing the information.

3.2 Possible Solutions

The simplest way to address the issue of one-off clauses is to attempt to eliminate them as far as possible by working with federations on commonality and understanding why these clauses are felt to be important. As part of the work on common clauses, work should be done to identify one-off clauses. These should then be discussed by a REFEDS working group to better understand their requirements.

RECOMMENDATION:
REFEDS SHOULD PURSUE THE IDENTIFICATION OF ONE-OFF CLAUSES IN FEDERATION AGREEMENTS AS PART OF PROPOSED WORK ON COMMON CLAUSES.

4. Data protection interpretation

4.1 Background

Although European Data Protection law is supposed to be harmonised by Directive 95/46/EC [1], member states and their courts have developed significantly different interpretations, particularly in the area of indirectly linked identifiers (such as IP addresses and eduPersonTargetedID) that the current law does not handle well. European law also differs considerably from law in other parts of the world, indeed only a handful of non-European countries [2] are recognised as providing equivalent levels of protection. This means that Service Providers and Identity Providers that want to work internationally may find that they are subject to different legal requirements in different countries.

4.2 Possible Solutions

Refeds has already published a summary of the implications of the current Directive for federated access management [3]. The European Commission is currently (2011) preparing to revise the Directive and the problems for indirectly-linked identifiers [4] have been pointed out at both European and UK level.

RECOMMENDATION:
REFEDS SHOULD MAINTAIN A WATCHING BRIEF ON THIS AREA THROUGH APPROPRIATE MEMBERS (E.G. ANDREW CORMACK).

5. Sponsorship letters

5.1 Background

Some federations require service providers (variable described as partners, affiliate members etc.) to provide an up-front sponsorship letter from an educational institution that is a member of the federation, supporting their application to become a member of the federation.

Sponsorship Letter Required: Denmark, Switzerland (except for well established, contracts-based, relationships with SWITCHaai Participants), US.

Sponsorship Letter not Required: Australia (although references are encouraged), Austria, Canada, Germany, Spain, Finland, France, Greece, Ireland, Italy,Norway, New Zealand,Portugal, UK, Brazil

Unknown: Czech, Croatia, Hungary, Japan, Latvia, Netherlands, Sweden, Slovenia,

5.2 Possible Solutions

Most federations have something in place to vet Service Providers and ensure that they are not introducing inappropriate providers in to the federation. For many services, it is easy to establish that service is education-appropriate and a domain check and contact check provides the level of security required. For providers that are not clearly education-appropriate, it is sensible to reserve the right to make further checks and potentially establish a sponsor from the community at this point, but upfront sponsorship for all providers is unnecessarily bureaucratic as a default.

RECOMMENDATION:
REFEDS SHOULD ESTABLISH WHICH OF THE 'UNKNOWN' FEDERATIONS CURRENTLY REQUIRE SPONSORSHIP LETTERS AND ENCOURAGE FEDERATIONS TO MOVE TO A MODEL OF 'VERIFICATION IF REQUIRED' RATHER THAN UPFRONT SPONSORSHIP.

6. Fees

6.1 Background

This is probably one of the most complex areas to manage and yet one of the most prevalent barriers for Service Providers. Charging fees is an inescapable problem - not all federations have the luxury of central funding. Of the 26 national federations on the REFEDS wiki, the following status can be observed.

Fee charging: Australia, Canada, Finland (not all), Netherlands, New Zealand, US.

Non fee charging: Austria, Switzerland, Germany, Denmark, Spain, France, Greece, Croatia, Ireland, Italy, Japan, Latvia, Norway, Slovenia, UK, Brazil.

Unknown: Czech, Hungary, Portugal, Sweden.

A common problem when charging fees to larger Service Providers is that this cost is often simply added on to the customer bill for the service being procured, so in the long-term IdPs are in reality funding the complete model. Fees provide greater barriers to the very small service providers, particularly those offering free services such as wiki and blog platforms. Although many federations try to differentiate fees by SP size and income, a charge of 1,000 euros per annum is still a significant cost for such small providers.

6.2 Possible Solutions

a) Establish a baseline of service providers that all federations agree to accept 'fee free'. These might be services that are considered 'friends of REFEDS', services of a certain size or type (wiki, blog etc.), services that are publicly funded or some other metric.

b) Fee charging federations move to a model of only charging IdPs.

c) Centralise fee charging for SPs at REFEDS, which in turn could subsidise REFEDS activities.

RECOMMENDATION:
THE OPTIONS DESCRIBED SHOULD BE DEBATED BY REFEDS AT ITS SPRING MEETING IN PRAGUE, 2011.

7. Technology Barriers

7.1 Background

One of the questions that is often asked of the UK federation is 'can I use this software within another federation?'. The UK has a reasonably mixed economy of software implementation although all are expected to use SAML as a basis. Other federations will only accept one specific software package (e.g. Shibboleth). This can be particularly complex when SPs are trying to understand if their software is capable of interacting with other SAML offerings. Clarity over the link between federations and software use is needed.

Other issues that have caused potential problems for Service Providers are differing processes for accepting certificates within federations and issues with testing Service Provider installations.

7.2 Possible Solutions

The REFEDS wiki currently captures software type per federation [5]. However, this is not user friendly for service providers and can be complex in terms of answering the simple question, 'can I join your federation with this software?'. This situation could be easily solved with more user friendly information for SPs, although REFEDS would need to be assured that information was correct and current.

RECOMMENDATION:
REFEDS SHOULD LOOK TO DOCUMENT ACCEPTABLE IDP AND SP SOFTWARE USED WITHIN FEDERATIONS, PER FEDERATION.

The current processes for certificate acceptance are not documented for individual federations. This information will need to be captured before further information can be made.

RECOMMENDATION:

REFEDS SHOULD LOOK TO DOCUMENT CURRENT PRACTISES IN CERTIFICATE ACCEPTANCE AND MANAGEMENT WITHIN FEDERATIONS AND MAKE APPROPRIATE RECOMMENDATIONS TO FEDERATIONS.

The Geant3 Identity Federations work area has produced the 'Federation Labs' toolkit. This should be promoted as a vital tool for Service Providers wishing to test their FAM implementations.

RECOMMENDATION:
REFEDS SHOULD ACTIVELY PROMOTE FEDERATION LABS AS A PLACE FOR SERVICE PROVIDERS TO TEST IMPLEMENTATIONS.