gFIVO

Abstract

This report looks at the feasibility of using external Identity Providers for external collaborators who wish to partake in a Virtual Organisation with Newcastle researchers. This report looks at two options for an external Identity Provider, the OpenID protocol and ProtectNetwork and why our preferred option is ProtectNetwork.

Table of Contents

1. Introduction

The core objective of the GFIVO project is to develop a Grouper based group management infrastructure to promote the formation, management of research based Virtual Organisations (VO). The infrastructure will be used by Newcastle researchers and external collaborators to enhance community communication via the use of simple web based tools like wikis, blogs and mailing lists. Among the issues raised is how do we implement an Identity Management system that caters for both internal and external collaborators.

External users will expect the same level or reliability and support provided to internal users when it comes to managing user accounts. External users should be able to sign up for an account in a quick and efficient manner and be assured of the confidentiality of their data.

This report explores the feasibility of using an external Identity Provider to manage Identity Management functions such as account creation, authentication and account management.

This report also looks at two options for an external Identity Provider, the OpenID protocol and ProtectNetwork and why our preferred option is ProtectNetwork.

2. Identity Providers

2.1 Introduction

When deciding upon the feasibility of outsourcing Identity Management functions to an external Identity Provider (IdP), our primary requirements are that our external users can sign up for a user account in a quick and efficient manner and comply to relevant UK legislation and University regulations.

We do not consider identity requirements such as whether the IdP can provide Level of Assurance (LOA) or if it is considered legally authoritative. Unlike Grid applications or medical based applications, which require a very high degree of trust and accountability, the collaborative effort at Newcastle is restricted to wikis, blogs, and mailing lists.

2.1.1 Advantages of using an external Identity Provider

Providing access to external collaborators requires account creation, role definition, user account management. Account creation can prove to be a difficult if there is a high volume of new users. This will take up time and any potential new users might have to wait before being provided with new accounts. All applications are treated on an individual basis and account creation will take up time. This might be acceptable in limited numbers but it will not scale if there is a high volume of new users.

Using an external provider such as ProtectNetwork, bulk account creation and automation can be done. Users are provided with a familiar Web based administration interface and they will be able to self register. They will also be given a certain degree of control over the personal attributes they wish to divulge. However, we will still insist that certain attributes have to be divulged if they wish to use our services.

The demands on our staff on managing user accounts will lessen and we can concentrate on managing access control to our services.

2.1.2 Disadvantages of using an external Identity Provider

The disadvantages of using an external IdP include:

- **Stability of service**: From the point of view of users, this external IdP has to be seen as a service offered by the University with the same level of assurance and reliability that they come to expect from University services. This requires that the external IdP to be always available and with very little unscheduled downtime.
- **Support**: Users have to be able to rely on service support when encountering problems or performance issues. This might be an issue if the external IdP is located overseas and is in a different time-zone and support may not be available when required.

- **Confidentiality**: The external IdP has to comply with the UK Data Protection Act and relevant legislative requirements when holding personal data. User information could be at greater risk of unauthorised exposure then if held within the University.

2.1.3 Overview

In conclusion, although there are several disadvantages to using an external IdP, it is however our view that having an external Identity Provider to manage Identity Management functions is the better option. This is especially true when it comes to ProtectNetwork as it is widely supported by the Shibboleth community and it provides a high level of reliability and support.

The next two sections looks at two options for an external IdP, the OpenID protocol and ProtectNetwork. The drawbacks of the OpenID protocol and why our preferred choice for an external IdP is ProtectNetwork are explored.

2.2 OpenID

2.2.1 What is OpenID?

OpenID [1] is an open, decentralised protocol for implementing Single-Sign-On (SSO) on the Web. At its most basic level, an OpenID is a URL that can be used to sign into sites that support OpenID. This URL can be the domain name of a user's website or more commonly, the URL of an OpenID Identity Provider. For example, myopenid.com/john.smith, where *myopenid* is the Identity Provider. Because of its decentralised nature, anyone at all can provide OpenID identity services and interact on the Web. As long as the Identity Provider conforms to OpenID specifications, it can deliver OpenIDs to be used by any site that supports OpenID. OpenID is meant to eliminate the need of multiple usernames/passwords since the same username/password can be used to log on to any site that supports OpenID.

2.2.2 OpenID Drawbacks

The OpenID protocol is a not a feasible option for us because it is an extra protocol we would have to support. Our current tool set does not support it and the implementation effort in doing so would be too high. Users will have to be told on how to apply for an OpenID and this support overhead of explaining how to login via multiple techniques would be too costly.

We would also have to insist that external collaborators only use OpenID providers that we approve of but this would lead to usability problems that OpenID was meant to solve in the first place.

2.2.3 Conclusions

The implementation efforts to supporting OpenID would be too high and our implementation efforts would be better served supporting external users internally. We would need the external IdP to handle bulk account creation without any help from us.

2.3 ProtectNetwork

2.3.1 What is Protect Network?

ProtectNetwork is an independent Identity Provider service that is widely used within the Shibboleth community. It is generally seen as a Guest ID management system whereby users who are not affiliated with the institution can access Shibboleth protected services with a ProtectNetwork ID. End users can also use a ProtectNetwork ID to access any OpenID, SAML or Shibboleth enabled site.

ProtectNetwork [3] provides users with IDs at two different levels of assurance (LOA), LOA-1 Self Service ProtectNetwork-ID and LOA-2 Validated ProtectNetwork-ID. Registering for a LOA-1 Self Service ProtectNetwork-ID requires the user to merely provide a username, password and a valid email address. We expect most of our external users to only require a LOA-1 Self Service ProtectNetwork-ID to access any of our Shibboleth enabled sites. In the case of LOA-2 Validated ProtectNetwork-ID, the user has to go through a more stringent identification process that includes the user having to sign a ProtectNetwork document in front of a Notary or ProtectNetwork trusted agent [2]. Although we do not require any external user to have a LOA-2 Validated ProtectNetwork-ID, it is however a useful scheme to acquire in the future if medical use cases are involved.

Getting an external user to obtain a ProtectNetwork ID means that Identity Management functions such as user registration, authentication, and user account management is the responsibility of ProtectNetwork. From a system administration point of view, Newcastle only has to update the Shibboleth SP metadata file and configure the Attribute Acceptance Policy (AAP) file to accept attributes from ProtectNetwork.

2.3.2 Conclusions

ProtectNetwork is our preferred option when dealing with external users since it takes away the responsibility of Identity Management functions such as user registration, authentication, and user account management. It also enables users to setup and control the attributes they wish to divulge to a certain extent. We, as the Service Provider, can instead concentrate on insuring our services are readily available to both internal and external users in a VO.

2.4 Dual Login

We plan to implement a dual login system whereby a user is able to choose if he wishes to access a Shibboleth protected service either by using a UK Federation account (if the user is part of the UK Federation) or a ProtectNetwork ID. If the user chooses to authenticate himself using a ProtectNetwork ID, he will be redirected to the ProtectNetwork website if he has not already done so. After obtaining a ProtectNetwork ID, the user is then able to access the Shibboleth protected service.

This lets us manage access control to services while delegating Identity Management functions to an external IdP. This will allow for improved collaboration because external collaborators will benefit from self registration and instant access to services after registration. If user account creation was handled internally, users will have to wait for accounts to be created since all applications are treated on an individual basis.

The dual login system will allow for a practical and usable group management infrastructure for use by Newcastle University and its collaborators. Researchers in a VO will be able to expand group membership in a quicker and more efficient manner with a dual login system because of the simplicity of getting an account.

3. Conclusions

Among the core requirements for collaboration in a VO is the creation and management of external user accounts. Identity Management functions such as user account creation, authentication and user account management is time consuming and can be prove to be unscalable when a high volume of new users apply for accounts. All applications for new accounts are treated on an individual basis and delays can be expected especially if there is a high volume of new users. To this end, getting external users to apply for an ID that is provided by a trusted external Identity Provider is the best option.

Our preferred choice of an external Identity Provider is ProtectNetwork because it is well supported within the Shibboleth community and provides a high level of reliability and support.

This report also explains how we plan to use a dual login system to allow both internal and external users to access our Shibboleth protected services.

4. References

1. OpenID, http://openid.net/
2. ProtectNetwork Applicant Identity Confirmation Application, http://www.protectnetwork.org/docs/pnidapplicant.pdf
3. ProtectNetwork, http://www.protectnetwork.org/