



PIREAN

WHITE PAPER



CLASSIFYING AND CHOOSING A FEDERATED IDENTITY MANAGEMENT APPROACH

Stephen Williams
Security Consultant

In this white paper, Pirean Security Consultant Stephen Williams discusses why different Federated Identity Management approaches exist in the marketplace and why it is important that an organisation fully understands their own business environment, existing relationships and partners before they select a Federated Identity Management solution.

DEFINING A FEDERATION

The Oxford dictionary defines a federation as “an organization or group within which smaller divisions have some degree of internal autonomy”. In the current climate of Software-as-a-Service (SaaS) adoption and Cloud service advocacy, a number of commentators are attempting to predict the future path of Federated Identity Management (FIM). To better understand how a federation of IT systems can be best managed it is wise to consider that federations within business have existed for a long time, and that these relationships have only recently been transferred to the IT systems that support them.

When considering the purpose of a federation and the relationships that exist between its partners, it is useful to look for similarities in the real world. A federation will usually be created by a set of partners looking to solve mutual problems or to unify around a common goal/vision. By creating such a union each partner is able to preserve a great deal of their existing structures whilst gaining the benefits of increased efficiency by leveraging the resources of other partners through a stable and well defined relationship. Outside of Information Technology, federations can most prominently be seen in business in the form of trade federations and in governments such as in the United States of America and India. Wherever one is formed, a federation can most prominently be found in two forms; symmetric and asymmetric.

UNDERSTANDING DIFFERENT FEDERATION TYPES

Within a symmetric federation each partner has equal power and there is no significant difference between each partner. Within an asymmetric federation one or more partner has significantly more power and responsibility when compared to the others.

For the most part the United States of America can be viewed as an example of a symmetric federation when its insular areas, which are under the direct control of the Federal government, are excluded. Each of the 50 states within the USA are internally sovereign and so reserve many important powers, such as taxation, but also transfer others to the central federal government, such as defence and foreign policy. Countries such as India and Malaysia can be classed as asymmetric federations as the partners within them are structured in a hierarchy giving some written authority to hold more power than others.

When comparing both types of federalism to the world of Information Technology we can see a great deal of similarity. Today federations exist in their broadest sense within IT as distributed computing, most obviously in the form of the Internet. This has allowed a set of organisations with previously isolated IT systems to inter-communicate for the purpose of achieving a common goal. This common goal could be to take advantage of the skills, services or resources of one or more partner organisations, which would, for example, allow all partners to jointly enter a new marketplace - symmetric federation. Alternatively a federation could arise from a merger or acquisition, which results in the delegation of some IT services (e.g. email) to a parent organisation whilst preserving others locally (e.g. help desk support) - asymmetric federation.

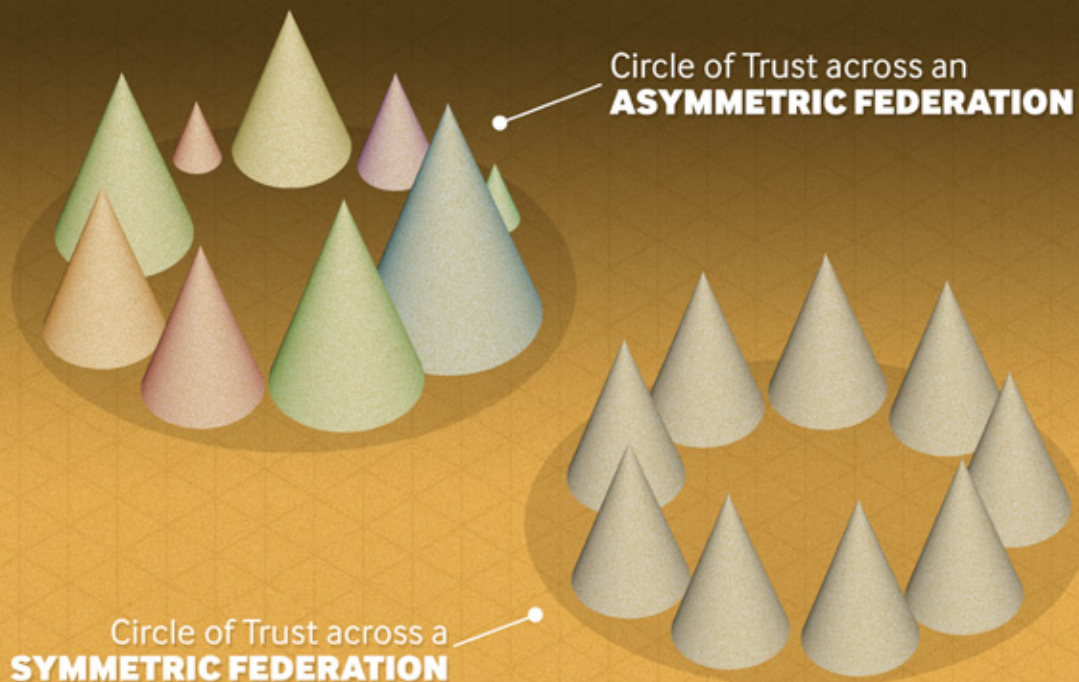


Fig.01 Diagram showing Symmetric and Asymmetric Federation

EVOLUTION OF FEDERATED IDENTITY MANAGEMENT

Whilst the concept of a federation within IT has existed for some time, the standards and tools that have existed to support such a relationship have been slow to evolve and keep pace with the current rate of change. Only now with the wide acceptance and usage of technologies such as SAML, OAuth and REST are organisations finally able to realize their federations, of whichever type, in the most practical and efficient manner.

Before Federated Identity Management tools reached their current level of maturity, organisations required bespoke data synchronization and/or specific point-to-point web service channels to join together the partners of a given federation. Whilst this allowed organisations to meet their immediate business needs, it created islands of integration, which would normally rely on different tools, techniques and protocols. The advent of the WS-* standards, which were ratified in the mid 00s, introduced technologies that could more effectively manage and secure a federation and its associated partners, which importantly also allowed for much more efficient and rapid integration between partners. The usage of these technologies within service hosting and Federated Identity Management products is now becoming the norm, primarily in response to the massive interest that has been generated around the Cloud and usage of services deployed here.

DIVERGENCE OF FEDERATED IDENTITY MANAGEMENT SOLUTIONS

Recently vendors of Access Management and Federated Identity Management solutions have begun to diverge on how they believe federations within IT can be best managed in light of the dramatic rise in Cloud service adoption. On one side some commentators voice a strong belief that due to data security and audit concerns within a multi-tenant environment, and legislation in some countries, using a centralized IDentity-As-A-Service (IDaaS) solution hosted in the Cloud to centrally manage an entire asymmetric federation is simply not an option. Instead these commentators believe that a collection of intelligent FIM solutions should exist separately within a wider symmetric federation, each hosted fully or partially on-site (referred to as private and hybrid Cloud respectively) at each partner.

Conversely vendors operating in the IDaaS market believe their tools provide organisations with the ability to deploy advanced Identity Management processes in a very rapid manner, as well as reducing need for each partner to manage a large onsite data centre. By transferring all Identity Management services to an IDaaS solution and locally preserving only service delivery, it is also advocated that each partner organisation could reduce their local resource requirements and carbon footprint.

When deciding on a Federated Identity Management approach it is critical that an organisation fully understands the maturity of their own IT systems and that of their business partners, as well as the legal and business impact of potentially transferring some of their responsibilities to a Cloud service provider.

CLASSIFYING AND CHOOSING A FEDERATED IDENTITY MANAGEMENT APPROACH

If we go back to the original purpose of a federation and its examples, it is clear there is no need to aim for the creation of a single unifying Federated Identity Management approach as a partner can legitimately exist in a symmetric or asymmetric federation. One type of federation could not be classified as being 'better' than another as the role a partner plays and the type of federation they are part of are unique to the challenges, relationships and partners involved. This is just as much the case for a federation of large nation states as for a set of small business partners.

If an incorrect FIM approach is chosen then there is real risk that the resultant federation will be ineffectual and not serve the original purpose that it was created to support. For example, if a partner with an existing and mature FIM solution joined a symmetric federation with a set of partners that each had an underdeveloped security management platform, the effectiveness of the entire federation and its ability to support complex inter-communication would be significantly hampered as only the most basic of interactions would be supported. Furthermore if a set of well-established multinational corporations with advanced yet structurally dissimilar security management platforms wished to form a federation, it would not be feasible for all partners to restructure their internal systems around a common FIM solution.

In both scenarios it is critical that a single unifying FIM solution be adopted but not to the detriment of one or more partner. If this means that a new partner must be added to the federation and promoted as a central authority with an asymmetric federation, then this would be the correct approach in this situation. Conversely if all partners within a federation have existing and compatible FIM solutions, then it is right to preserve such a symmetric federation in this manner.

To conclude, when deciding on a Federated Identity Management approach it is critical that an organisation fully understands the maturity of their own IT systems and that of their business partners, as well as the legal and business impact of potentially transferring some of their responsibilities to a Cloud service provider. Only once such analysis has been carried out can an organisation effectively classify and choose the right Federation Identity Management approach for their requirements.



If you have any questions or require further information then please do not hesitate to call +44(0)845 226 0542, or email claire.boxer@pirean.com.

To further share in Pirean's unrivalled IT Service and Security Management knowledge and expertise, and to be automatically informed of any new Pirean whitepapers and/or industry insight information in the future, please register your details here, or email your request to claire.boxer@pirean.com.

To find out how Pirean can enable your enterprise visit www.pirean.com
call +44 (0)845 226 0542
or email info@pirean.com

Head Office (UK):

Pirean Limited,
Faretec,
Cams Hall Estate,
Fareham,
Hants.
PO16 8UY

SWITCHBOARD: +44(0)845 226 0542

FAX: +44(0)845 226 2742

ABOUT PIREAN

Pirean is a leading technology partner and consultancy. We are recognised leaders in the management of business change, pairing consultancy with an industry leading portfolio of technical services across the design, development and delivery of IT Service and Security Management solutions.

We focus on helping our clients to achieve their business goals and provide ongoing support through proven capabilities in:

- Asset Discovery, Change and Configuration Management;
- Business Service Management, Availability Management and Dashboarding;
- Endpoint Security and Compliance Management;
- E-Commerce Security;
- Identity and User Lifecycle Management; and
- IT Service Management Consultancy and Transformation.

Our unique blend of services and capabilities enables us to help you take a strategic view of your business; where you are, where you want to go and how to better leverage the resources you have to get there.

Pirean is one of Europe's Leading IBM Premier Business Partners. Having been awarded IBM Tivoli's AAA Accreditations across both the IT Service and Security Management portfolios we have been, for 2010 and 2011, recognised by IBM as the most qualified IBM Tivoli Business Partner in the world.



*Source: IBM, based on AAA accreditations for IT Service and Security



*Source: IBM Tivoli Deployment Accreditation Partner Finder Tool, July 1st 2011

At IBM Tivoli Software's Pulse 2011 conference Pirean were finalists for both the 'ISM Summit Cup' and 'Business Partner Innovation Award'.

Other recent accolades include the 2010 IBM Tivoli Software 'Business Partner Service Management Solution Award' as well as the 'Business Partner Innovation Award' and 'Beacon Award Finalist – Outstanding Service Management Tivoli Solution' in 2008 and 2009 respectively.

In September 2010, Pirean was listed among global and regional system integrators for IBM Tivoli Software in Gartner's Magic Quadrant for User Provisioning.

For more information, visit www.pirean.com.

Copyright © 2011, 2012 Pirean, all rights reserved. No part of this publication may be reproduced, stored in a retrieval system, used in a spreadsheet, or transmitted in any form or by any means – electronic, mechanical, photocopying, recording or otherwise – without the permission of Pirean.

'Pirean', and the Pirean logo are registered trademarks of Pirean Limited (UK). Registered in England No. 4453109

