



White Paper

Written by Keith Grayson and Mark Jones

Federated Identity and you

Imagine this. You work for a modern, large corporation, called Mycorp. There is a corporate intranet that provides access to corporate data, news, information and a range of outsourced services. These outsourced services could include business travel bookings, pension management, benefits management, company car management, human resources and other common functions.

Now take a moment to think about the number of usernames and passwords that you would have in this environment. Think about the number of times that you need to enter a separate username and password to gain access to the internal and external resources that you need to do your job. Hmm; I'm thinking about handing in my notice at MyCorp already and I have only worked there for thirty seconds.

Let's look at a typical action like booking company travel to an overseas destination. First, you log into the operating system on your laptop or desktop computer. Then you log into the company portal application with another password, which allows you to access the travel portal. The travel portal is outsourced and requires a different username and password, which you provide. You then need to check the company travel insurance policy is up to date, so you need to visit the current insurance providers portal and you guessed it, another username and password. Hang on, its been a while since you logged on to this portal, you have forgotten your password, lets hope their helpdesk doesn't keep you on hold too long, you still have that company finance report to finish by lunch time. Recognise the scenario? Me too.

Have you ever stopped and asked "Why?". Why do we have to provide all of these different usernames and passwords? What makes an outsourced service provider so special that they have the right to require you to remember yet, another username and password? I mean, after all, your company already knows who you are. They've already asked you to login twice, once on to your computer and once into the company portal. Why can't your company tell your external provider, "This is Joe Bloggs, we know, because we have already asked him to log in twice. Take our word for it, and give Joe Bloggs access to his relevant details."? Wouldn't all our lives be so much easier?

That is what Federated Identity is about, making your life easy.

Contents

| | |
|---|---|
| Win-win benefits | 1 |
| Delivering business agility | 1 |
| Responding to rapidly evolving markets | 2 |
| Taking the pain from mergers and acquisitions | 2 |
| What is Federated Identity then? | 3 |
| What are the next steps? | 4 |

Let's look at how this process could work. You log into your laptop or desktop computer. You fire up the company portal; the company portal knows it's you because you're already logged in successfully to the corporate network. It presents you with your personalised front page with no further ado. You click on the business travel link and it presents you with your personalised booking page, having welcomed you without the login ceremony. You book your travel, no calls to the travel help desk for lost passwords, and your finance report makes the lunch time deadline. Everybody is happy.

Not only that but you didn't have to fill in your personal details again for the business travel provider. They already knew your address, telephone number, email and potentially other personal information such as your passport number, because you had signed the electronic form requesting permission for the details.

Now think about all the other Web sites that you use on a regular basis, your pension provider, your health insurance provider, your market analyst's subscription site, the industry working group that your company is a major sponsor to. Wouldn't it be nice if you could also be welcomed by their sites rather than going through the charade of clicking the "forgotten password" link having just come back off a 2 week holiday.

We can achieve this with today's technology, by implementing federated identity solutions.

Win-win benefits

It could be so much easier. Why isn't it?

Maybe it's because some people think the benefits just don't justify the costs, or the wins just aren't big enough. Let's consider that point for a moment. The benefits to Mycorp of Federated Identity are:

- > Employees don't have to call the IT helpdesk to get their myriad passwords reset as often. They only have one password to remember for all corporate intranet activities.
- > Employees don't have to waste their time calling the business travel helpdesk to remind them of their username or to get their password reset.

- > Employees become productive more quickly, since they are registered with partner systems as soon as they are given a login account by their organisation.
- > Along similar lines, as soon as an employee leaves a company, access to all corporate resources can be disabled, including access to partner systems that non employees should no longer have any access, by the management of a single account.
- > Employees feel part of a progressive organisation with IT that empowers them rather than wasting their time.

Some benefits to outsourced service providers of providing Federated Identity facilities are:

- > Ability to offer a uniquely personalised service to their clients
- > Elimination of password reset calls to their customer support helpdesks, as all password resets would be managed by their clients
- > Automatic feed of current personal information, as allowed, from the client's systems, saving on the costs of gathering personal information through operators.

It looks like there are benefits to both sides that could be regarded as cutting costs or delivering competitive advantage.

Delivering business agility

These benefits are not one-offs either. Once a business has invested in Federated Identity technology, it can use the same technology to connect to multiple outsourced service providers, giving exactly the same set of benefits many times over. Having provided single sign-on from the portal to the business travel provider, it can be easily extended to the pension provider site. If the company changes pension providers, no problem, with federated identity the new provider can be plugged into the system giving seamless integration with the new provider. It gives the business a higher level of agility in that it makes services more accessible to employees, within a technical infrastructure that allows a rapid change of service provider with the same levels of on-line service.

Once an outsourced service provider has deployed a Federated Identity solution, likewise the benefits are cumulative. With relatively little additional effort, the service provider can offer the benefits outlined to their new clients rapidly and at very little incremental cost. The service provider can offer a differentiated service to a large number of corporate clients, integrating seamlessly with their intranets without requiring privileged access into their client's IT resources or privileged access to their client's employee data.

Responding to rapidly evolving markets

This model can be extended to numerous scenarios where there are relationships between organisations and outsourced service providers. A typical example is the provision of value-added data content services provided through mobile phones. An example would be, providing access to subscription-based services offering ringtones, games, photo-sharing facilities, maps, etc. through a central portal. The use of Federated Identity technologies would mean that telecoms providers would be able to rapidly provide new services by linking their users to added value service providers, while offering the ability for service providers to link rapidly to multiple telecoms providers. These sorts of solutions are being adopted by mobile telecoms operators such as Orange and Vodafone that are looking to provide leading edge premium services rapidly.

Taking the pain from mergers and acquisitions

Let's look at the other areas where Federated Identity might help Mycorp. Mycorp is in the process of a merger with Beecorp. Both organisations are of a similar size. It is important to Mycorp to ensure that from day one, all employees of the new merged BeeMyCorp should have access to a single re-branded company portal, to give everyone the sense of working within a new organisation with a new identity. In fact, this is viewed by the CEO to be a key indicator of how successful the initial phase of the merger will be.

Both organisations have spent a considerable amount of time and money in terms of deploying their own individual portals. However both companies selected different vendor products for authentication and authorisation of users to their portals. Switching products after extensive separate integration and deployment cycles would take a significant amount of time. Both companies have directory infrastructures to store user credentials, such as their laptop or desktop computer usernames and passwords, a due diligence process has uncovered the fact that both directories have different sets of personal attributes across both sets of employees and contractors.

How can they ensure that both user communities are brought together to be able to access a common intranet while providing access to all of the various systems and services that both sets of employees are used to? Federated Identity provides another solution to help the process of corporate integration in a merger or acquisition scenario.

Offering an IT infrastructure that can react rapidly to bringing in new user populations under a federated model will be a key success factor for company's that are pursuing corporate acquisitions. Equally, for company's that are looking for buyers, ensuring that they have an IT infrastructure that can be rapidly integrated with those of an acquiring company will give them a premium over prospects whose IT assets will be less easy to integrate with and remove what can turn out to be a key obstacle to acquisition.

We've discussed some of the benefits of applying the concepts of Federated Identity into the IT infrastructure in the context of corporate intranets, outsourced service providers, telecommunications providers and the value in merger and acquisition scenarios.

This should show that the benefits of Federated Identity solutions scale with the degree to which they are deployed across the organisation.

What is Federated Identity then?

This leads us to the key questions, “What is Federated Identity? How can it deliver on the benefits that we’ve talked about?”

Historically organisations have developed silos of systems that manage IT services and resources within corporate, departmental or network boundaries. Each of these “data silos” will maintain a number of business critical applications, e.g. purchasing and supply chain systems, personnel systems and desktop services. Each of these applications has typically maintained its own set of user identities and credentials. This contributes to the bewildering increase in the numbers of corporate and Internet usernames, passwords and other authentication methods with which we are required to authenticate ourselves to information resources that we want access to.

Broadly speaking, Federated Identity is about the concept of trusted users being allowed automated and seamless access to IT services and resources across corporate, departmental, or network domains with a single logon. It works on the basis that if you are identified and authenticated to one domain, such as your corporate intranet, using a set of trusted credentials, then you should be able to be identified automatically to systems in another domain without further identification and authentication. It follows a sort of “any friend of yours is a friend of mine” approach.

The point about Federated Identity solutions is that the technical processes are automated and just happen “under the bonnet”. That isn’t to say that you can’t control them, either as a user or as a provider or information resources.

While you may believe the assertions that I make about my friend, it may be that you don’t trust them with the same fervour that I do. What Federated Identity implies is that while you believe that my friend is who you say they are and the assertions that you make about them, you still control what access they have to your systems and resources.

Of course this is a gross oversimplification, and the various use cases and standards cover off the issues of account linking, pseudonymity, anonymity and so on, that address concepts of user privacy and data protection.

There are also some broad security and risk concepts that are attached to Federated Identity. As an organisation or division participating in a federated “Web of Trust”, you will want to know that users that you are accepting from divisional resources outside your own are as well known and authenticated as strongly to their department as your users are to access your resources. Of course, this sounds like common sense, but depending on the formality between the parties engaging in Identity Federation partnerships expected standards of behaviour may just be enshrined in cross-divisional policy documents or in formal legal agreements with defined procedures and safeguards. Making sense of the standards

So far we’ve talked about Federated Identity and benefits and IT systems in a broad sense, we’ve not mentioned the technical standards that make this all happen. It should be clear by now that Federation is about making IT systems recognise users across “domains of trust”. Where interoperation at this level is involved, it is invariably governed by open standards. And with Federated Identity there are certainly enough open standards to choose from! Over the few years that federation technology has evolved, there have emerged a number of different standards sponsored by various industry groupings.

That has now consolidated to 3 broad sets of standards, between which there is extensive cross-fertilisation. The foundation for all of them is SAML (Security Assertions Markup Language). The SAML standard is governed by OASIS (Organisation for the Advancement of Structured Information Standards). It provides the basic standards for exchanging identity information between domains in a secure way. Another set of standards are created and controlled by The Liberty Alliance.

The Liberty Alliance has members taken from a huge range of industries including telecoms infrastructure providers, application software vendors, security solution vendors, financial services giants. They include household names such as AOL, GM, Oracle, RSA Security, American Express. The relative newcomers to Federated Identity standards are Microsoft and IBM with their WS-* set of standards.

What does this tell you in terms of adopting Federated Identity in your organisation? Our view is that it tells you that there is an overwhelming momentum behind the technologies and the client needs that are driving them. Also that there are Federated Identity solutions to business issues that will deliver tangible business benefits for organisations from small service providers up to major diversified international corporations.

What are the next steps?

This paper sets out to explain what Federated Identity is and how you can use it to make a difference to your business, in terms of efficiency, costs and development of new business opportunities.

Our recommendation would be to start looking at your internal IT environment and processes. If they resonate with the various issues and scenarios that we have presented in this paper, then there are probably grounds to look at Federated Identity solutions more closely.

In doing so, see if you can come up with some cases where you think a Federated Identity solution might help and a roadmap on how to achieve them.

When you have made the decision to investigate more fully you might benefit from evaluating:

- > Different Federated Identity standards and the uses that their referees are putting them to. They all have their strengths in particular applications and environments
- > Vendor solutions. Look at their references and what they have done. They will all tell you that their platform complies with a wide variety of standards, but they generally won't tell you what the best ones are for you
- > Engagement with the stakeholders within the business that own the IT resources and the relationships with outsourced service providers. Work with them on the business case benefits
- > Benefits of applying Federated Identity across the whole business. In general, bear in mind that it is good to start modestly with tightly scoped pilots delivering measurable and defined business value.

Ignoring the marketing hype around the Federation bandwagon, we believe that Federated Identity can deliver true business value and competitive edge for many businesses. In your IT strategy, what is your roadmap for Identity Federation? Can you afford to be left behind?

Conclusion

We have all been driven by the revolution that is outsourcing, industry and government alike have responded to it whilst not always considering as fully as they might the fragmentation that third party service provision causes in terms of employee experience.

We have all been driven by the need to grow and change our organisations whilst not always considering the tremendous inertia which IT infrastructure integration can introduce into M&A and indeed the acquisitive growth and change process.

We all understand that collaboration and the ability to form and sustain collaborative relationships is at the heart of modern innovative organisations.

Atos Origin believes that Federated Identity leverages all these concepts and can help your organisation to gain further value and competitive advantage from its IT asset base.

Let's not imagine, let's investigate.

For further information, please contact the Security and Information Risk practice on: +44 (0)20 7830 5444 or email: SecurityInfoRisk@atosorigin.com

About Atos Origin

Atos Origin is an international information technology services company. Its business is turning client vision into results through the application of consulting, systems integration and managed operations. The company's annual revenues are more than EUR 5 billion and it employs over 46,000 people in 40 countries. Atos Origin is the Worldwide Information Technology Partner for the Olympic Games and has a client base of international blue-chip companies across all sectors. Atos Origin is quoted on the Paris Euronext Market and trades as Atos Origin, AtosEuronext, Atos Worldline and Atos Consulting. For more information, please visit the company's web site at www.atosorigin.com

About Atos Consulting

Atos Consulting is a leading provider of business, process and technology consulting services. With more than 2,500 staff globally, it focuses on delivering proven, pragmatic solutions to the telecom, manufacturing, financial services and public sectors.