Technical White Paper

Simplifying Federation Management with the Federation Router

HP Select Federation

By: Jason L Rouault

Introduction

Enterprises today need to be flexible and agile. Rapidly evolving market forces dictate a constant change on the enterprises that hope to win in today's dynamic environment. As a result, reorganizations, mergers, and acquisitions are an ongoing activity instead of a one-time event. Additionally, enterprises continue to be driven to greater degrees of collaboration with business partners while the number and diversity of systems and applications continues to increase. And if that were not enough, privacy concerns, conformity with compliance regulations and increasing demands by customers for seamless end-user interaction is forcing organizations to rethink how they are providing access to data and services.

Enterprise identity architectures on the other hand have remained relatively static and have increasingly become an impediment to enterprise flexibility. The forced centralization in today's identity architecture and the lack of independence for individual businesses, departments and applications has led to a "snapshot in time" kind of solution: It worked well when it was implemented, but has failed to evolve as the enterprise organization and structure have evolved, and have caused a lot more "one-offs" than originally intended.

The advent of federation technologies and the leveraging of rapidly maturing standards have helped bridge the gap between identity domain silos both within and between enterprises. Today, federated identity management systems are fundamental to underpinning accountability in business relationships; providing customization to user experience; protecting privacy; and adhering to regulatory controls.

However, as the adoption of federation technologies has grown, it has become increasingly evident that that required pair-wise business and technical agreements between federating entities does not scale. Each federation relationship requires a business/legal agreement, meta-data exchange, determination of protocol usage, user mapping, etc. While these issues are manageable "in the small", this complexity grows exponentially as the variety of federation protocols and number of federation partners increases.

The federation router architecture offered by HP Select Federation aims to address the scaling and management issues of tomorrow's federation deployments. Just as a network router simplifies the relationships between network entities by directing traffic, ensuring message delivery, providing protocol translation, and allowing for special handling of requests, a federation router simplifies the relationships between federated identity entities. The federation router will enable identity to be a more pervasive aspect of the enterprise infrastructure – transforming the enterprise and blurring the lines between the enterprise and extended enterprise.

Adopting the HP federation router architecture will allow enterprises to be more ready for organizational change; to be better integrated with customers, partners and suppliers; and to easily scale these capabilities as there electronic business relationships grow

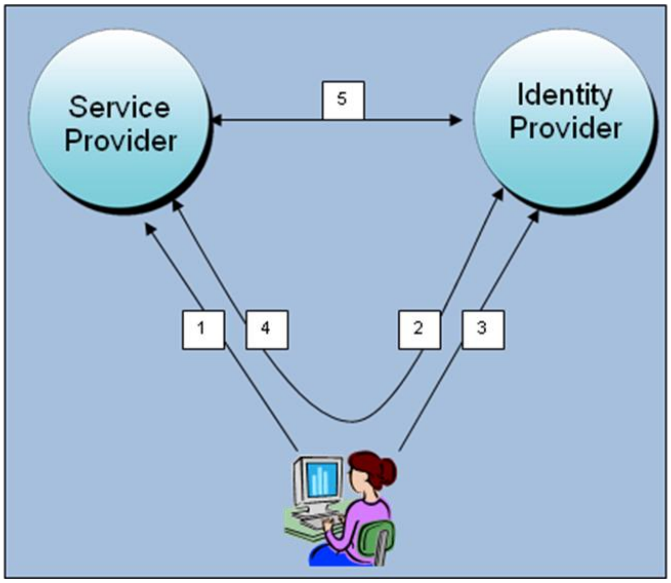
What is federation

Federation is the combination of business and technology practices to enable identities to span systems, networks, and domains in a secure and trustworthy fashion. This is analogous to how passports are used to assert our identity as we travel between countries. An important thing to note is that these domains may exist both within and between enterprises. The main purpose of federation is to share identity information across heterogeneous systems and identity platforms. Communication between these domains is based on industry-wide communication standards such as SAML, Liberty or Active Directory Federation Services (ADFS).

How does federation work

A federated identity system puts the real world trust between cooperating organizations into digital action. Using time honored security techniques of SSL and digital signatures it enables a user to benefit from single sign-on across organizational boundaries without requiring either a central user repository or any additional technology at the user end. In a federated identity system, an organizational entity (typically by means of a server) asserts the identity of an authenticated user. This entity is known as the Identity Provider or IDP. The assertion is conveyed to an application which needs to know the user's identity before providing whatever service it is meant to provide. This application is called the Service Provider or SP. **Error! Reference source not found.** depicts the relationship of these federated entities and the data flows.

Figure 1: Relationship between federated identities



1. User request for application access at the SP
2. SP redirects the request/user to the IDP
3. User logs in locally at IDP (if not already authenticated)
4. IDP generates an assertion and redirects user back to SP with either a:
   - Signed assertion(s)
     (or)
   - Artifact reference
5. *(Optional)* If the artifact reference was used in step 4, the SP will make SOAP based request to the IDP for the assertion using the artifact. The following security options can be used during this step:
   - Signed assertions
   - SSL client authentication
   - SSL with basic auth

Once the SP receives an assertion of the user's identity, it verifies the security of the process in accordance with its policies and if all is well, allows access to the application. The verification of the assertion (or the process of acquiring it) is based upon commonly accepted security principles such as digital signatures and mutually authenticated server-to-server SSL/TLS. In the case of Liberty and

SAML standards, they both have gone through a couple of iterations and extensive review by individuals, companies, and governments, making this conveyance of identity information secure.

Federation Growth Brings New Challenges and Barriers to adoption

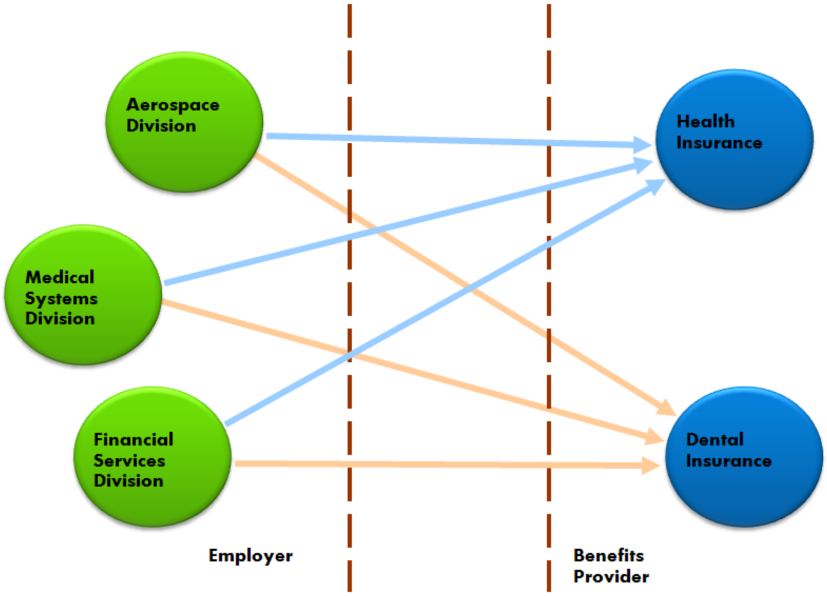
According to an IDC report1, federation is a rapidly growing market with projected sales of over $700 million by the year 2010. Adoption is growing among companies that use it today as a "perimeter" technology to connect with partner enterprises.

Common use cases of federation deployments today include allowing employees to seamlessly access their benefits information which is provided by independent benefits provider enterprises, or allowing consumers of to seamlessly access different services provided by independent divisions of the same enterprise.

Federated identity technology is rapidly growing in adoption. New management challenges that never existed before are resulting out of its early success. Federation depends upon trust relationships (business policy) between independent entities; Trust between an Identity Provider and Service Provider, Trust between Web Service Provider and Web Service Consumer. Adoption of Federation technology and the evolution of federation standards have introduced a need to deal with issues that are not necessarily new to an organization, but are in a different context. These issues are not apparent in small deployments, when the number of federation partners is fairly limited or very uniform. Complexity of the deployment grows exponentially as the number federation partners increases and/or the number of federation protocols supported increases.

[1] Market Analysis: Worldwide Identity and Access Management Federation 2006 – 2010 Forecast, *Sally Hudson and Allan Curry*, IDC Report Dec 2006

Figure 2. Potential multiple relationships required during federation.



Error! Reference source not found. demonstrates the sets of relationships that might be required between federating entities from an enterprise (Employer) and outsourced employee service provider (Benefits Provider). In this example a large engineering enterprise has an aeronautical division, medical systems division and a financial services division. The enterprise as a whole has contracted with a benefits provider for health and dental benefits. However, since each of the divisions in the enterprise is independent, each has its own identity management processes. Further, the Benefits Provider is actually a merger between two benefits providers, one which provides medical benefits and the other providing dental benefits. As a result, the systems within the benefits provider are also independent. The enterprise has now mandated that all employees must receive seamless access to their benefits information. This means that each division would have to explicitly trust each service of the benefits provider so that employees from each division get seamless access to their personal medical and dental benefits information.

For each of the federation relationships depicted in Figure 2, business and technical policy must be defined to address trust, protocol usage, attribute mapping, and security. Since trust agreements are based upon business and regulatory policies, they are typically legal documents requiring costly legal review. Thus, having a large number of legal agreements is less than desirable to simplify and reduce costs of governance and management of contracts. Furthermore, non-technology processes will lengthen the duration of federation IT projects adding further delay and uncertainty to the process. These issues become a hurdle for rapid adoption of federated identity management.

As new IDP's and SP's relationships are added to the federated environment, there will undoubtedly be new federation protocol requirements. **Error! Reference source not found.**

Figure 3. Complexity increases due to multiple relationships and federation protocols.

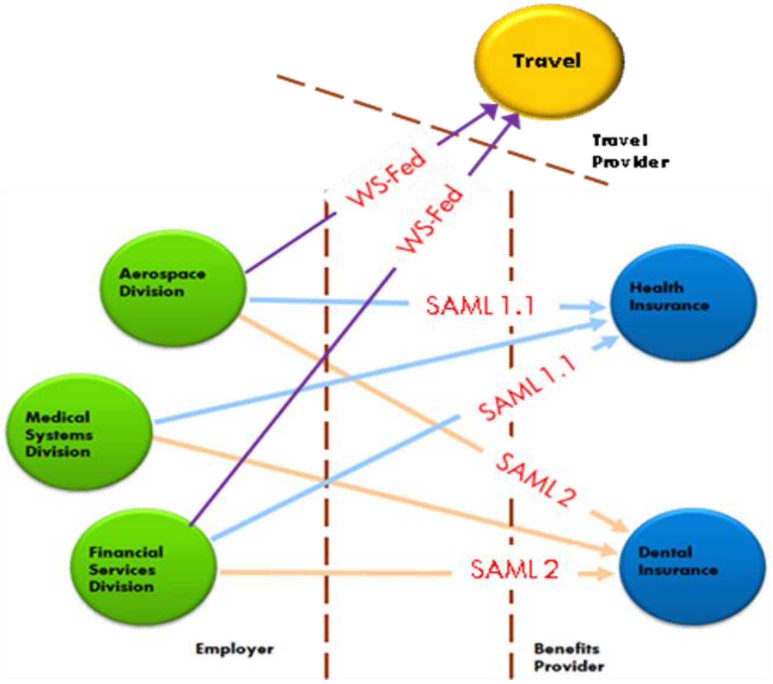


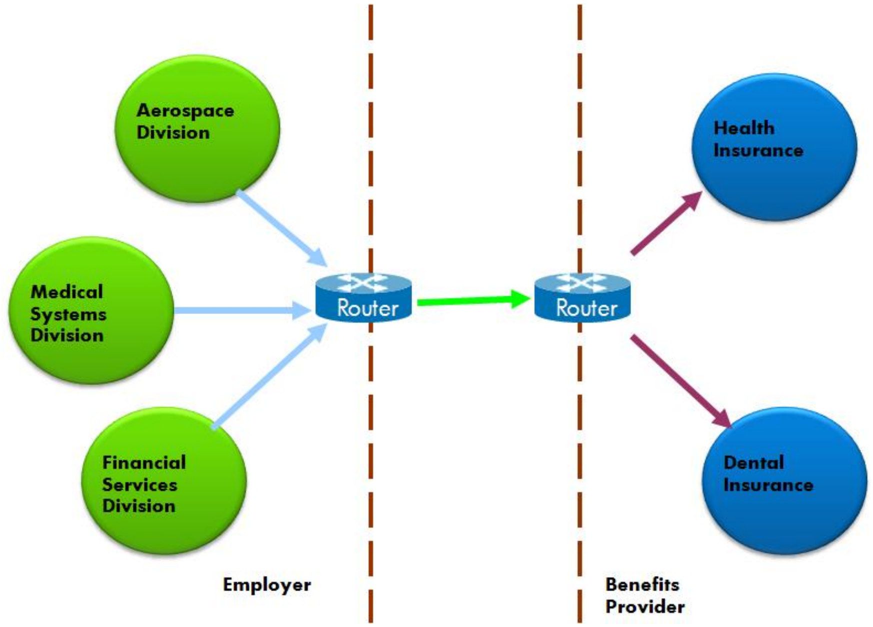
Figure 3 depicts the complexity that can arise related to federation protocols and the need to match the capabilities of your partner. Either an IPD will need to add support for an additional federation protocol when interacting with the new partner (e.g. Aerospace division uses WS-Fed when interacting with the Travel Service Provider), or the SP will need to add support for a protocol that the IDP(s) already supports. Either way, this can become a hindrance to doing business, not to mention complicates configuration and support of the environment for any particular federating entity.

Federation Router – Simplifying federation management and accelerating deployments

In today's TCP/IP networking environment, much of the work to get a message from one computer to another is done by routers, because they're the crucial devices that let messages transit between networking domains. These routers play the critical role of directing traffic, ensuring message delivery, providing protocol translation, and allowing for special handling of requests.

With HP Select Federation, HP is applying the same principles behind network routers to the processing of identity federation. HP Select Federation has introduced a new capability that allows for its deployment as a federation router.

Figure 4. Federation router simplifies relationships between federated identities.



Error! Reference source not found. depicts how the federation relationships between federating entities from an enterprise (Employer) and outsourced employee service provider (Benefits Provider) have now been condensed, as compared to the pair-wise deployment without a router shown in Figure 2. With the federation router, not only are there less trust relationships, but the management of the relationships, including the information conveyed about users, authentication policies, etc. can move away from the individual divisions to being managed at the enterprise level.

Simply put, a federation router acts as an SP to an IDP on one side and then turns around and acts as an IDP to an SP on the other side. The Liberty specifications proposed the use of such "identity proxies" first in its Liberty ID-FF 1.2 specification, and it is now a part of the SAML 2.0 specification. However, the HP federation routers architecture takes the idea of identity proxies further by fulfilling the following purposes:

- Acts as an intermediary between multiple organizations, some of which are on the "inside" and others on the "outside".
- Abstracts the details of each side for the other. Hides backend infrastructure (various Federation protocols, agreements, multiple IDPs, etc.)
- Maintains trust relationship with identity components on the inside and outside. This reduces the overall number of trust relationships that need to be managed.
- Maintains policy about which users on one side have access to which applications on the other side
- Transforms user identity representation so that applications can get all information they need about a user in the format they expect.
- Performs protocol translation, ensuring that federating entities receive messages in the format they support

- Possible to make internal changes without requiring communication to or coordination with external partners

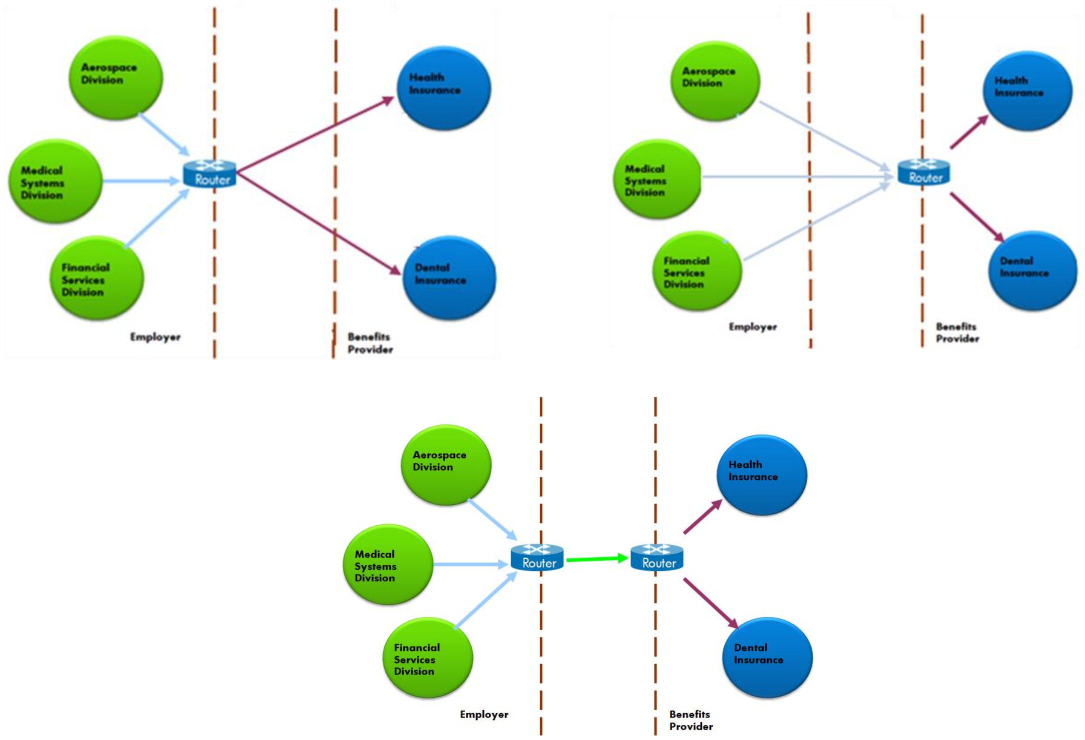
Deployment Models

There are a number of differing scenarios for which federation routers can be deployed. Obviously, which deployment model is employed will be largely dictated by the business model of the federated entities. In all cases the same federation router technology is used, it is just configured and deployed differently. This section will explore a few of the deployment models.

Edge Router

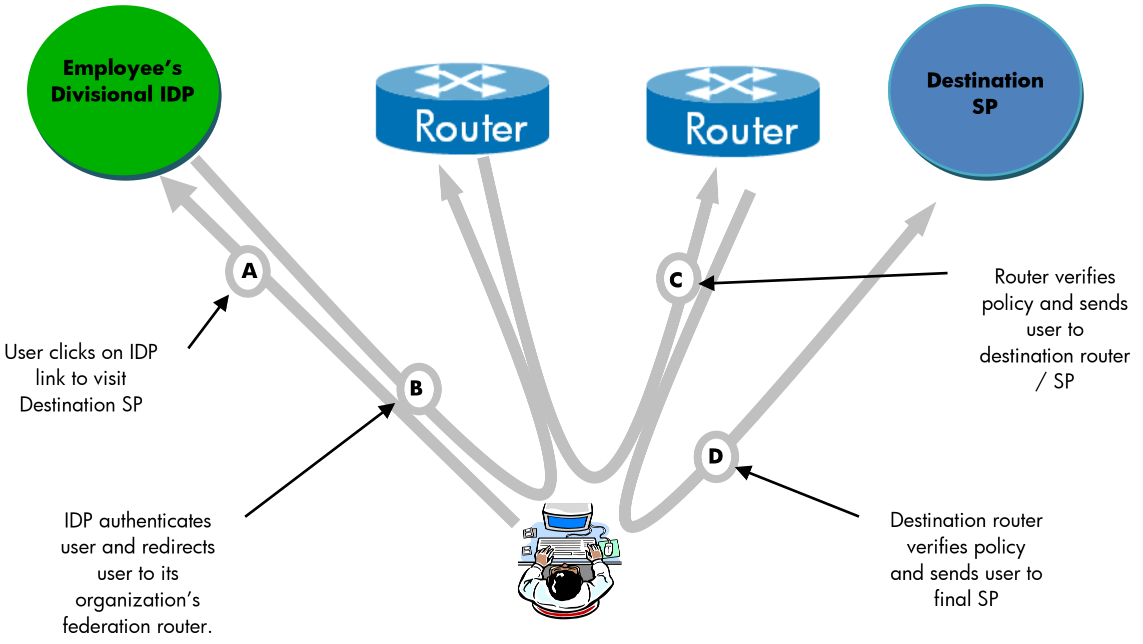
A typical deployment scenario for a federation router is for it to be located at the edge of an enterprise, thereby isolating actual applications and/or authorities from partners and vice-versa.

Figure 5. Edge router being used to front-end multiple federated identities.



As shown in **Error! Reference source not found.**, an edge router can be used to front-end multiple IDPs, SPs or both. Multiple IDPs can be seen quite often in situations where the enterprise does not have a centralized user data-store or has acquired other organizations. This was the case with the earlier example where multiple divisions within an enterprise had their own identity provider and needed to interact with a benefits provider services.

Figure 6. Edge router federation steps.


Employee's Divisional IDP
Router
Router
Destination SP
A
B
C
D
User clicks on IDP link to visit Destination SP
IDP authenticates user and redirects user to its organization's federation router.
Router verifies policy and sends user to destination router / SP
Destination router verifies policy and sends user to final SP

In this edge router deployment model, the federation router works as follows:

A. The user visits an IDP portal (at the divisional level) and clicks a link to an external benefits provider.

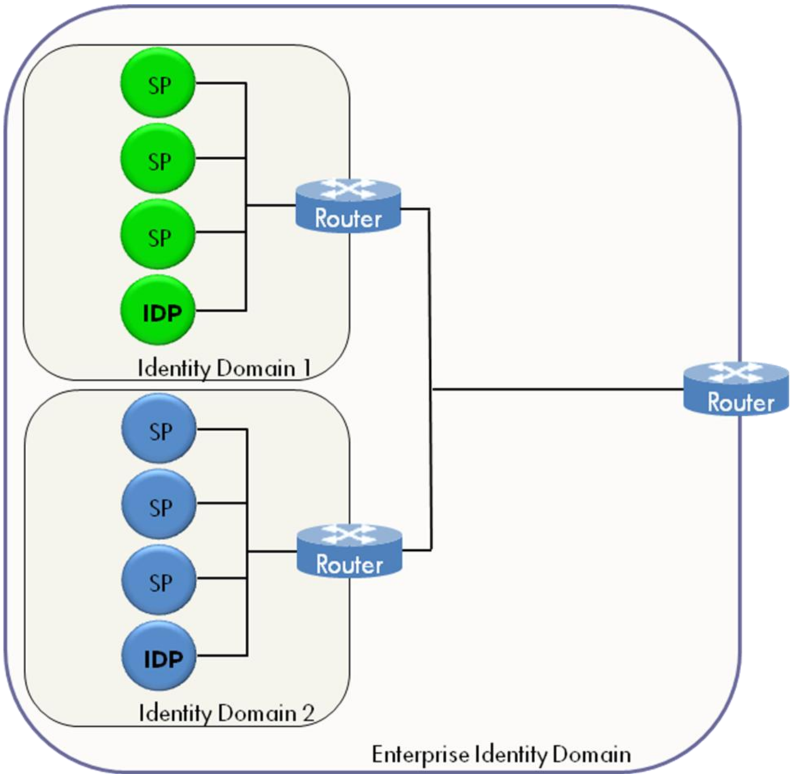
B. The IDP authenticates the user (if not already authenticated) and redirects her to the router at the enterprise level.

C. The router verifies that the user has permissions to visit the external benefits provider (e.g. he is an employee and not a contractor), transforms the user representation so that only information required by benefits providers is revealed, and redirects the user to the router at the benefits provider (Note: the router may not know that the SP at the benefits provider is actually a router. It just thinks of the benefits provider as a single SP). The router will also translate the request into the appropriate protocol to meet SP/router requirements.

D. The router at the benefits provider finds out which services the user is signed up for in its enterprise and verifies that the user is accessing a service she is subscribed to. If she is, it redirects her to the SP which is the benefits application translating to the appropriate federation protocol for that SP.

Enterprise Tiered Router

Figure 7. Enterprise tiered router gives business units more control over specific user population.

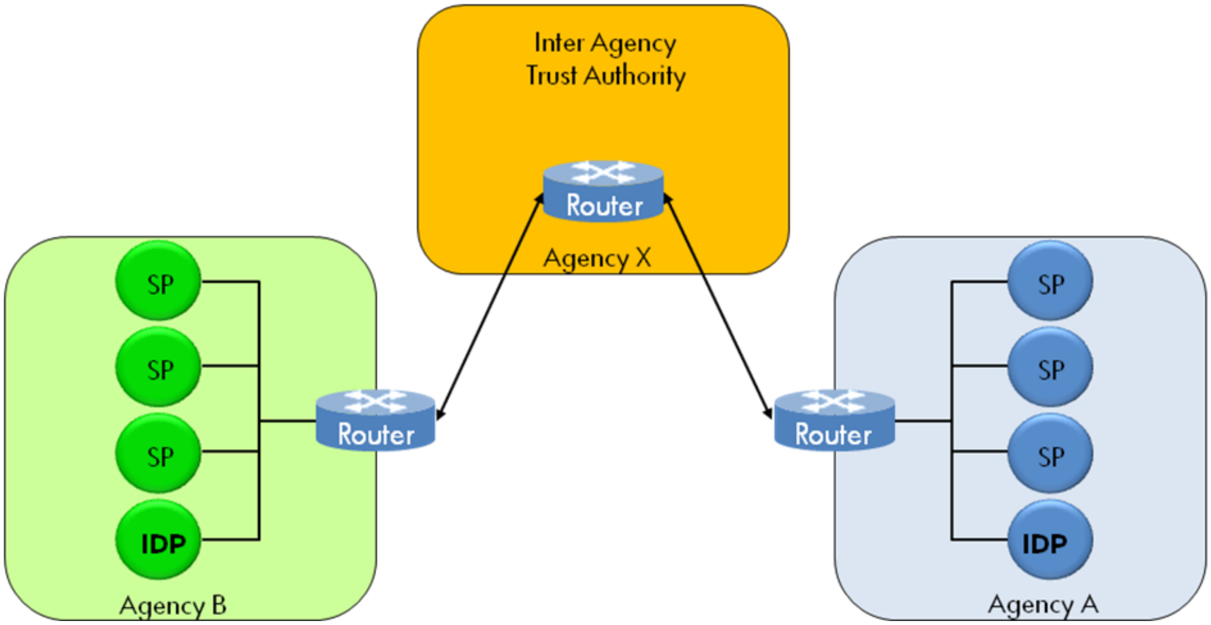


This type of deployment scenario is particularly useful within a large enterprise where businesses want to retain a certain amount of autonomy over their user population and the access requirements to its applications, while still conforming to enterprise level IT policies. For example, at a large financial institution, a private client business (Identity Domain 1) and an institutional investor business (Identity Domain 2) may have differing requirements of authentication, authorization and application access policies for their respective users. Interactions between these domains would be governed by the local polices of the routers in those domains. However, for interactions with either of those domains that come via the enterprise domain, enterprise level policy can be applied. As an example, an enterprise level policy might be applied that transforms or removes certain identity information (e.g. employee ID) from requests originating in internal domains and transiting outside the enterprise.

Trust Authority Router

In another deployment model the router is deployed by a separate business entity, acting in the role of a trust authority. The goal is essentially the same: reduce the number of trust relationships. One example of a trust authority router deployment is an inter-agency access broker.

Figure 8. Trust authority routers are deployed by separate business entities.



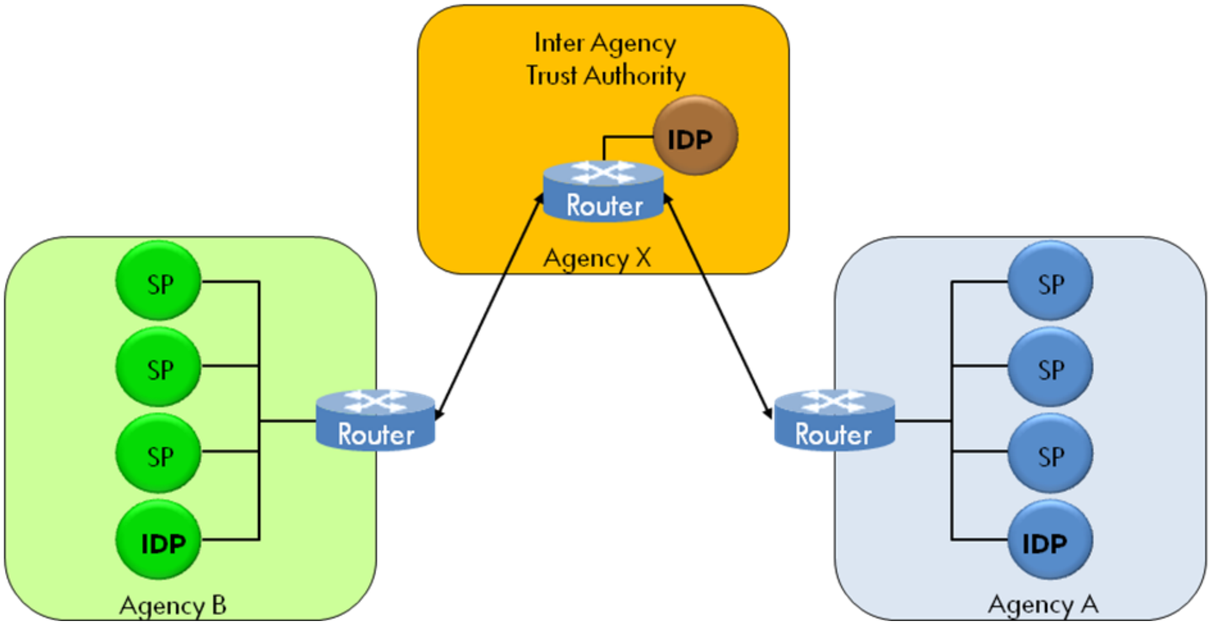
In this example deployment scenario users from a government agency "Agency A" need access to applications in another government agency "Agency B" (and vice-versa). However, there is an overall government authority "Agency X" that sets policies regarding such inter-agency access. One logical way of implementing this is to setup a federation router at Agency X. Employees from Agency A are authenticated locally within that agency and are conveyed via the desired federation protocol to the router at Agency X. Agency X acts as a SP and receives the request. It then verifies that the incoming user from Agency A has the privileges to access the particular application (SP) at Agency B. If the policies are met, it then becomes the IDP and generates a new request that is then conveyed to the SP Agency B. Since Agency B trusts Agency X, it verifies that the assertion has indeed come from X and lets the user in to the requested application.

Such deployments are under way in a small scale today, and are expected to grow.

Router plus IDP

A variant that can be applied to any of the deployment models previously discussed is to include an IDP with the router. This allows the router to not only route to and from external IDPs, but to also interact with its own IDP without having to introduce additional infrastructure within that identity domain. **Error! Reference source not found.** shows the Trust Authority deployment model but with the router plus IDP variant. This type of deployment would be used when the Trust Authority (Agency X), has its own user population that may need access to the applications of Agency A or Agency B. In such a case, the users at Agency X requesting access to Agency A or B applications would be authenticated by the routers local IDP.

Figure 9. Including IDP with router deployment allows router to interact with its own IDP.



Summary

Inefficiencies, disparate technologies, and complexity drive enterprises towards federated identity management solutions that address heterogeneity issues and allow them to integrate with their business partners. Privacy concerns, conformity with a long list of compliance standards, and increasing demands by customers for seamless end-user interaction are also reasons many organizations are looking to federated identity management for the answer.

The federation router architecture eliminates this complexity. It allows an organization to have a single interface to the partners. With a single negotiation of technical and legal agreements, organizations can establish a partnership that may optionally be leveraged by various business units. Additionally those business units may interact with each other through a single interface without the need to support multiple protocols or to negotiate beyond the granting of access to the application to the business unit partner.   The federation router architecture helps reduce the number of partnerships that need to be set up, while improving oversight, monitoring, controls and audit of the partnerships. It helps reduce the time-to-market and legal and planning costs, while insulating the organization's partners from the inevitable change that occur in its IT environment. The result is improved business continuity at a reduced cost.

The federation router architecture offered by HP Select Federation addresses the scaling and management issues of large federation deployments. Federation routing simplifies trust relationships between federated entities and opens the door for many different federation deployment scenarios to meet your business needs.

Adopting the HP federation router architecture with HP Select Federation allows enterprises to be equipped for organizational change; to be efficient integration with partners and suppliers; and to easily scale these capabilities as there electronic business relationships grow.

HP Select Federation effectively enables extranet identity management, web single sign-on and cross-domain identity management without requiring a centralized data repository or synchronization between repositories. Using Select Federation, you easily achieve single sign-on and federated session management while leveraging your existing identity management deployments. HP Select Federation is designed to work with HP Software Identity Center products, as well as integrate for use with other vendors' systems. HP Select Federation allows federation to be achieved via SAML (1.0/1.1/2.0), Liberty ID-FF (1.1/1.2), ADFS, CardSpace, and Liberty ID-WSF (1.0/2.0) protocols. Additionally, Liberty Personal Profile, Liberty Employee Profile and the LECP (Liberty Enabled Client Proxy) services are provided.

For additional information, access the HP Web site at http://h10078.www1.hp.com/cda/hpms/display/main/hpms_content.jsp?zn=bto&cp=1-11-85-131_4000_100__

Oct 2007

invent