yorktel
Making complicated simple.

A Primer on Federated Communications

By Vishal Brown, Vice President of Professional Services, Yorktel

The concept of federated identity management, or identity federation, encompasses solutions in which enterprises coordinate for the purpose of authenticating and permitting users to traverse firewalls to access applications within the networks of participating organizations.

For a number of years, federation has been a hot topic in the enterprise communications market. At a high level, federated communications occurs when multiple computing and/or networking providers agree on standards of operation that allow otherwise disparate applications to communicate. Most enterprises have traditionally used a variety of applications and devices to communicate with their suppliers, partners, and customers. Federation solutions promise to meet those growing demands, while simultaneously requiring fewer devices and applications.

One of the challenges proponents of federation face is a myriad of philosophies regarding how federation should be achieved. The single common theme among the various viewpoints, however, is the goal of federation, which is to provide secure, reliable, and seamless communications capabilities across multiple platforms and networks.

Federation leverages trust relationships that allow information sharing across domains. It provides inter-company or business-to-business (B2B) interactions that enable enterprise users to securely communicate and share information with colleagues, partners, and customers that are outside the corporate firewall.[1]

True Enterprise Federation goes beyond interoperability among applications and devices — it allows distinct applications (such as voice, instant messaging (IM)/ presence, and conferencing) to work together to deliver a seamless user experience. Examples of secure, inter-company federated communications capabilities include allowing users from different organizations to:

- Share dial plans and directories
- Access shared databases and content libraries
- Utilize shared applications or team spaces, and
- Share real-time user information such as rich presence status and availability.[2]

THE IMPORTANCE OF UC&C FEDERATION

Constructing multi-platform, multi-modal solutions presents a number of challenges, namely, the integration, interoperability, control, and security of communications sessions between end points across platforms and networks. To enable a seamless user experience, unified communications and collaboration (UC&C) solutions have to go beyond the traditional model of siloed user authorization and authentication processes for each application and leverage common directory information. To this end, tightly integrated UC&C solutions, whether premises-based, cloud-based, or hybrid must support common directories and recognize the same user identities.

FEDERATED IDENTITY

One of the essential prerequisites for achieving federated communications is a federated user identity. In essence, a federated user identity facilitates a single sign-on to multiple applications and services. The distinct applications of a solution must utilize common data verification points (name, password, SIP address, e-mail address, phone number, and location) for individual users. A single sign-on improves user experience by making all relevant integrated applications readily available. Microsoft's Active Directory, which already plays a critical role in many UC&C solutions by acting as the central database for user data, is an example of an identity management solution.

The concept of federated identity management, or identity federation, encompasses solutions in which enterprises coordinate for the purpose of authenticating and permitting users to traverse firewalls to access applications within the networks of participating organizations. Identity federation allows users from participating companies to utilize the same instance of an application (such as project management software, work spaces, logistics, and supply chain), and also allows users to directly connect for interactions (that is, via voice or video communications) and to share information (such as IM and real-time status/availability).

FEDERATED DIRECTORY

From a user perspective, support for a common user identity among a range of distinct applications (e.g. telephony, IM/presence, unified messaging, audio and video conferencing, and social business) enables a single sign-on to the various applications in the UC&C stack. This allows users to authenticate on the system once and then access any of their provisioned applications when needed throughout their work day. A common directory allows

> Federated Presence is intended to allow users of different platforms to communicate via IM and share their presence/availability with constituents inside the same organization as well as those from other companies. Today we are seeing a greater degree of intra-company Federated Presence.

user information to be shared across applications. Leveraging Active Directory for user information allows distinct applications to interoperate more tightly. For example, a common directory for presence/IM and telephony enables a user's availability status for phones calls to be displayed in a desktop UC client. The common directory also enables users to have a single phone number for voice and video communication.

FEDERATED PRESENCE

The ability to federate multi-vendor presence engines has been available for years in the consumer world. In 2005, AOL launched its IM Federation Initiative and introduced the AOL Federation Gateway to connect users of AOL, Jabber, and several other IM/presence platforms. In 2006, Google opened up its APIs to enable third parties to integrate and federate their XMPP-based IM/presence applications with Google Talk.[3]

Federated Presence is intended to allow users of different platforms to communicate via IM and share their presence/availability with constituents inside the same organization as well as those from other companies. Today we are seeing a greater degree of intra-company Federated Presence (e.g. Lync, Lotus Sametime, Jabber). There are also IM and presence aggregators that allow multiple enterprise and consumer platforms to exchange XMPP information.

FEDERATION TODAY

Tighter integration across vendor platforms and the creation of multi-modal, multi-vendor Federation provides the ability to track user identities and contact information across different UC&C tools.[4] Capabilities include a single contacts view that lists users' corporate contact information (name, e-mail, and phone number) as well as their contact details from third-party social applications such as Facebook and Twitter. Interaction history includes a time stamp and the type of session (voice, IM, video, e-mail, Tweet, and Facebook message).

CONCLUSION

Enterprises are increasingly viewing federated communication as a strategic business decision that can provide them with a competitive edge. Businesses expect to integrate communications into workflows and processes, following the examples already set by consumer-focused companies such as AOL and Google. Tight integration and federated user identities across IT and communications applications are an important prerequisite to building powerful solutions that will help users become more productive and efficient. Federated Identity Management for Secure B2B communications is a second prerequisite to compel more companies to adopt certain applications in the UC stack, such as videoconferencing. Those who are able to overcome potential philosophical differences in how federated communication should be implemented will gain the ability to securely communicate with parties outside of their enterprise, achieving increased productivity and collaboration, customer satisfaction, and a myriad of other business benefits as well.

[1] Source: Frost & Sullivan Analysis
[2] Source: Frost & Sullivan Analysis
[3] Source: Frost & Sullivan Analysis
[4] Source: Frost & Sullivan Analysis