

technology viewpoints

September 2008

TABLE OF CONTENTS

This issue of CGI's *Technology Viewpoints* takes a look at topic of identity and its role in business today. It examines the topic from five key viewpoints:

- Identity and the enterprise
- Identity and its uses
- The effect of Web 2.0
- Service oriented architecture (SOA)
- User-centric identity

The paper concludes with CGI's solutions for identity and access management (IAM).

To provide your perspectives on these topics and to learn more about CGI, contact us at info@cgi.com.

Effective Use of Identity in Today's Networked World

Identity is one of the largest business challenges today.

What was once a topic among academics and security professionals, the debate over identity and its proper use and protection is now within the public domain. The role of identity now stretches from immigration policy and how to prevent terrorism and other crimes to privacy and participation in social interaction and e-commerce.

And yet, despite that growing impact, our information technology (IT) solutions have failed to mature to deliver against contemporary challenges.

There has been dramatic growth in the size and value of e-commerce and its scope continues to broaden. Web 2.0 phenomena such as social networking and blogging introduced new arenas where people actually want to supply their identity. With more people visiting more sites – and more sites looking to offer personalized services – the number of logins is ever increasing, which leads to more entities storing more information about people.

The more identity and other private information that travels across the Internet, the more available it is for theft and other abuse. IT has been focused on how to manage these risks. In large part, this is why industry has not kept pace in understanding how to leverage the analysis and flow of identity information to enable the delivery of new business goals. Enterprises that use identity intelligently can generate significant gains in customer loyalty and reduce risks and administrative costs. As a result, enterprises need to strike a balance among security, ease of use, customer intelligence and privacy.

In this issue of *Technology Viewpoints*, we look at the evolution of identity and its role in business today. We dig into changing definitions and uses of identity and solutions that serve as catalysts for strategic growth from the following key viewpoints:


- **Identity and the enterprise:** Identity represents both opportunities and risks for enterprises. Enterprises need to strike a balance that works for them, their partners and their customers.
- **Identity and its uses:** In the beginning, identity opened doors, literally, such as to buildings or system access. As electronic uses have evolved, individuals have taken on multiple identities and how they are used has changed as well.
- **The effect of Web 2.0:** People want to engage and share their identity over the Internet. Greater information sharing generates greater concerns about security, privacy and reputation in the open networked world.
- **Service oriented architecture: SOA** creates a platform for tailored, right-time services, but it relies on enterprises to create new architectures for accessing services.
- **User-centric identity:** We are moving closer to standardized identity management with greater control for the individual over their own information.

The paper closes with CGI's solutions for identity and access management (IAM). CGI has developed a unified vision of how enterprises can leverage identity to build strategic gains, while being mindful of both the opportunities and challenges associated with it.

Identity and the enterprise

For an enterprise, identity represents a threat and an opportunity, a hindrance and an enabler. In recent years, identity theft has captured global headlines, such as the unfolding story of \$7 billion fraud at Société Générale and the associated costs of recovering from identity theft. As a result, COOs must make significant investments in protocols and compliance initiatives aimed at protecting information, and CIOs face constant maintenance costs and the lack of agility that results from overly complex identity management systems.

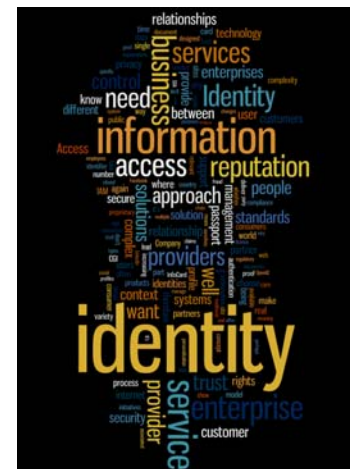
Effective identity management

Benefits		Challenges
<ul style="list-style-type: none"> • Improve customer satisfaction and support for new initiatives through <ul style="list-style-type: none"> ◦ Personalized service ◦ Improved usability ◦ User centricity • Reduce fraud and identity theft through <ul style="list-style-type: none"> ◦ Reduced complexity and redundancy in user management ◦ Trust relationships and standardization 		<ul style="list-style-type: none"> • Prevent fraud without compromising usability • Allow personalization without invading privacy • Meet compliance requirements but remain agile • Protect reputation without restricting liberty and creativity

Never more than today, an enterprise must incorporate how it defines and uses identity – for itself, its customers and its partners – from the earliest stages of both its business and IT architecture. Companies that get it right benefit from enormous opportunities, but the risks are just as big for those that get it wrong.

Identity and its uses

Identity is not just an identifier such as a user ID or passport. Identity reflects how we see ourselves and how others see us, which we can shape by the personal information we share. Identity is also a set of characteristics that uniquely identify us to the satisfaction of an authority or service provider. It depends on the context and one's viewpoint.



Who we are

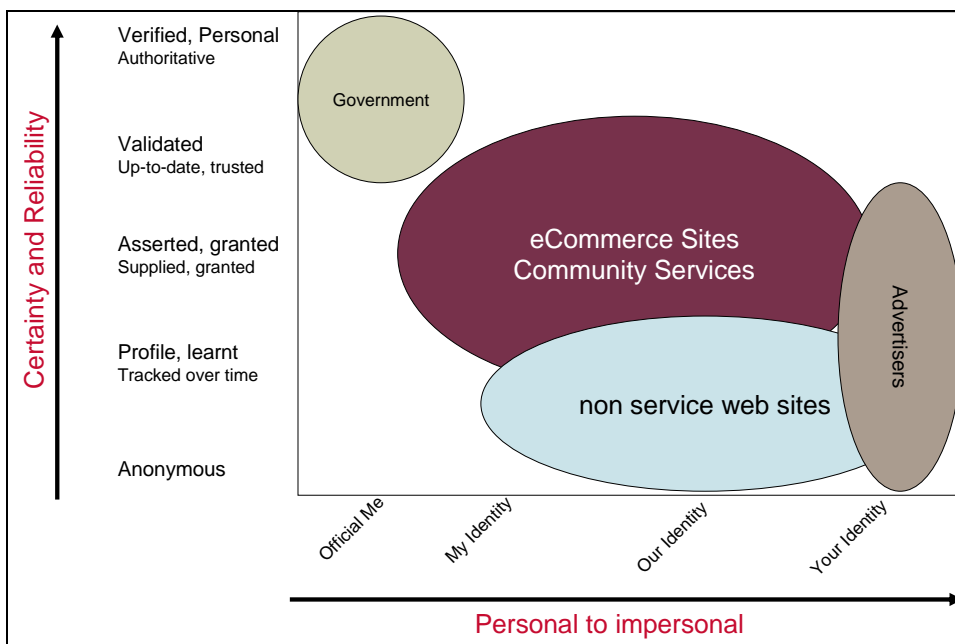
Most contexts involve a lot less information than what constitutes our complete personal identity. In fact, when someone asks us to identify ourselves, the question is to provide reasonable proof that we legitimately own an identification form that is relevant to that situation, such as a passport and photo, credit card and signature, user ID and password. In addition to great variation among types of identifiers and proof, we have numerous identity attributes, which may not be relevant to a proof of identity but are valuable to our personal identity.

What we can do

Identity can be used to grant or deny us access to something – a country, a building, a computer system, some information or a bottle of wine. Enterprises also can use their understanding of our identity to define our interests, including how they match us to certain products they think we will like. Identity can determine our reputation or that of our employer. Some aspects of our identity are official, verified and controlled by the government, a bank or our employer. Some are entirely under our own control and may not even be capable of verification.

Who says it's true

How people view their identity most likely isn't identical to what interests their government, local liquor store or employers' human resources departments. That identity may be part of how others, including a service provider, such as Amazon, or a social networking site, such as Facebook, sees and groups individuals with those of similar traits. The below illustration – "Aspects of Identity" – demonstrates how different groups have different perspectives of an individual based upon their business.



Privacy, reputation and trust

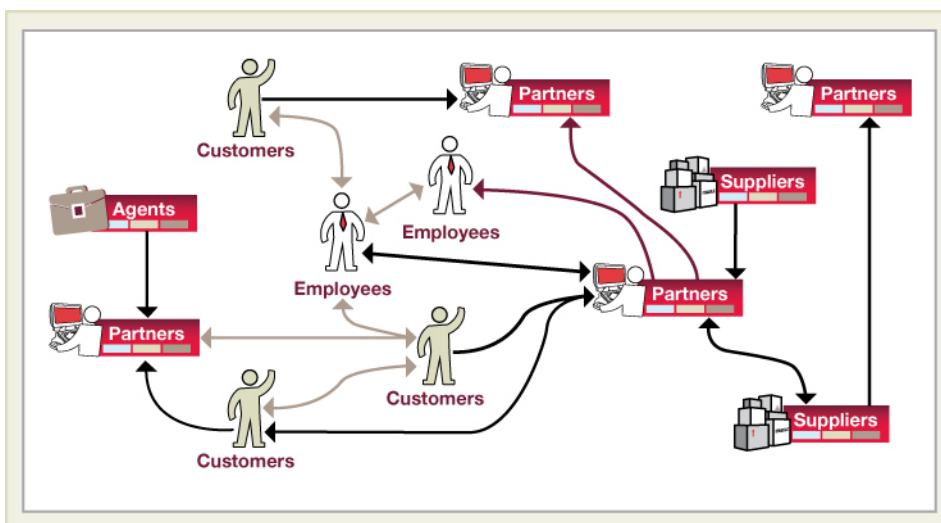
Identity and its uses and abuses today influences personal and organizational reputations, shaping how we relate to others and interact in the market, such as how we market products or receive services. Because of its sensitivity to theft and fraud, identity requires security and control. However, safeguarding identity can generate complexity in operations and even invade freedom and privacy. Therefore, the right model should allow individuals to control their own identity, leading to trusted relationships that make that possible and safe for all parties.

Identity in the networked world

As we have seen, more enterprises have transformed their former manual or closed-system processes into functions now performed on the public Internet. We call this the networked world.

While operations have evolved, our model and use of identity in this new environment has failed to evolve; our IT structure is simply inadequate for today's challenges. We are used to closed systems available only to people (and other systems) connecting from inside the corporate firewall – and even that's inadequate these days. The enterprise defines and controls the tasks people perform on these systems, which may be unrelated to any other IT function.

Today, those same activities also are performed by people who are customers or partners. An enterprise's employees may also be customers of its partners; blog and have Facebook and LinkedIn accounts; buy products from Amazon or via Craigslist; and complete their tax returns online. The below illustration reflects how our new approach to identity must reflect this environment. Patching up the old approach to add new complexities isn't an option. We need a new approach, which is perhaps the most important element of using identity today.



Access control

Historically, identity (or rather the possession of an identifier) was used primarily to control who is allowed to be where, do what, read what, use what or carry what at any given time. This usage of identity has become commonplace. From border controls to information security, we are used to carrying passports or memorizing PINs and passwords. Without these identifiers, we face some limits in our work and private lives.

Access control uses identity in two ways. The first is authentication: *Does the requester appear to be who he/she/it claims to be?* The second is authorization: *Is the authenticated requester authorized to get access to a particular service, information or location?*

We care about access control from the perspectives of both a provider and a consumer. As a provider, I care who can do what with which of my services. While I want to ensure that I get paid, my care extends to the privacy of my data and the protection of my assets. As a consumer, I care passionately about who can see and use my data – particularly my money, but also personal information that can influence my reputation.

Personalization and profiles

An increasing number of Web sites allow users to personalize their landing page. Some personal pages may be simple recognition (“Hello ...”) while others, such as iGoogle, allow users to fully configure their page. Users like the ability to quickly access what they want while eliminating what they find unimportant.

With the growing numbers of e-commerce transactions, providers want to provide personalized experiences for all shoppers, drawing on customer profiles built from past visits and comparing them with others’ behaviors. Unlike traditional, physical retail stores, these online shops can create the appearance of a separate store for every customer, from shelf order and product presentation, to ads and even pricing. The more a store can be tailored, the better the business can enhance the customer experience to increase revenue.

Profiles can provide a long-term advantage to providers. Effectively offering recommendations based on users’ past experiences will deepen the relationship, particularly as the provider enriches that profile every time the user visits. Smart and consistent profile management can secure the provider’s relationship and reputation.

In business-network platforms such as LinkedIn or Xing and in platforms like Facebook and Myspace, transactions are based directly on profiles. Both users and providers rely on the ongoing evolution of the profile to drive the site’s value. Connecting with friends, creating relationships and enhancing reputations with comments or recommendations builds user profiles, which are valuable for visitors, other users and providers. Think about it. Are you more likely to follow a recommendation of someone you’ve never heard of or from someone who is known?

Another aspect of personalization is the ability to create a recognizable persona – an image you want to portray. This can be achieved using your “personal” identity or a chosen avatar. The attraction is partly that you can choose a different “identity” for every site you use; for example, you may want to be a space cowboy on Facebook

but a serious professional on LinkedIn. In some cases, you can have multiple identities on one site. You also can associate a profile (both structured and unstructured information) with each persona, so that you are eventually represented by multiple personalities. There does not have to be a single entity that knows they are all you.

Audit and control

Enterprises must be able to monitor, control and report on the integrity and correctness of their transactions. While a sound business approach, this also reinforces best legal, regulatory and ethical practices. Legislation in this area, such as Sarbanes-Oxley and Basel II, has been much in the news.

Identifying all parties in a transaction is core information for these purposes. But just as with everything else that changes in the networked world, the use and meaning of identity in this case is far more complex than in the case of former, closed systems. The openness of modern systems and the variety of entry points, payment types and internal services used make audit and control more complex – *unless* those processes are designed to reflect the new reality.

The effect of Web 2.0

Social networking and reputation

While reputation has always been a vital element of how we do business and interact with people, social networking and e-commerce are making it even more significant on the Internet. We've already looked at reputation in the context of Amazon, Facebook or eBay. But whose reputation is it? You can't take it with you from one site to the other because your identity on each site is only meaningful there. People may know that both "identities" are the same but that's unreliable.

Another aspect with direct relevance to enterprises is blogging. Blogs are increasingly used as a form of advertising or promotion with a pseudo-objective gloss. The identity of the blogger and association to an enterprise (and therefore to the image of the enterprise) is therefore vital. The reputation of the individual becomes the reputation of the enterprise. Suppose Company X has a blogger that consistently produces quotable material. That blogger may well be seen as a Company X blogger, acting on behalf of Company X. That's good for Company X's reputation and good for the individual's reputation. Then this person changes employers and starts a blog on behalf of Company Y. Is Company X able to keep the blog content's reputation? Is the blogger able to keep the past reputation?

Mashups and access

Mashups provide a relatively easy way to create added value out of pre-existing applications or services. If I create a public mashup of services between Google and Craigslist, am I blurring the reputation of those providers with my own? That's just a risk of doing business publicly – I'm not touching their protected data. If, however, I then couple that information to the secure services of another enterprise, I am introducing a new risk because that enterprise potentially has to rely on me to ensure secure access to their services. They don't know the identities or reputations of my

WEB 2.0 AND IDENTITY 2.0

With so much media coverage, Web 2.0 has its share of definitions. So what is it really? Web 2.0 is a convenient term for the current stage of the continuing evolution of IT and communication as applied to the Internet – a key feature of which is user-centricity.

In much the same way, Identity 2.0 – although yet to be defined in any formal context – revolves around principles of users being in control of how, when and where they provide information. It also contains a business opportunity, whereby enterprises strike a balance among security, ease of use, customer intelligence and privacy.

There are technical, commercial and most likely regulatory issues to be addressed before Identity 2.0 becomes standard. In the meantime, organizations need to create a trusted environment that also balances the need to provide enough consumer choices without creating an overly complex environment.

users and they certainly don't want to maintain a vastly increased amount of identity information anyway. Processes and standards are needed to prevent these types of scenarios.

Mobility

Being constantly connected is part of Web 2.0. People want use to the same services and sites from any device – such as a computer, cell phone, games console or car navigation system – whenever it is convenient for them.

However, many newer devices are not well suited to traditional identity authentication screens and processes. In the case of mobile phones, the traditional identifier is hardware based – such as a SIM card or MSISDN – which is not reliable for access to secure services. The challenge for mobile service providers is to develop new, secure mechanisms that don't undercut service.

Mobility also introduces the concepts of location and presence, which can influence an identity's access control and profiles. It's also likely that each device comes with different profiles and personalization. Bringing these factors together means that ways to authenticate and authorize users based on context must be created.

Trust

While trust is a fundamental requirement of any significant transaction between people and organizations, it has traditionally had little impact on IT systems. In the closed system that manages and controls all identities and access rules, trust has little role. The open networked world cannot work without trust. To understand why, let's look at some real-world examples.

The official identity document for most is a passport. When immigration officers check a passport, they can see whether the photo and description match the appearance of the owner and whether the document appears to be genuine. That sounds authoritative, doesn't it? But underlying this authentication process is an assumption that the country that issued the passport checked all the necessary papers and is not itself actively engaged in smuggling people illegally into the visited country. That assumption is based on a trust relationship between the governments of the visited country and the issuing country.

That is a fairly simple example involving trust between two equivalent bodies, governments, which may or may not have a diplomatic relationship. Here's something a little more complex. It's possible to use a driver's license as proof of identity when renting a car or joining a video club or even as official identification in some countries. There is a trust relationship (usually implicit) between the authenticating party and the issuing party, which might be a local authority. The local authority requires specific documents to be presented and validated before issuing a license. It has trust relationships with those documented issuers, and so the chain usually continues until a national government agency is involved. This trust chain can be quite long, and – even if each link involves an explicit trust relationship – there is usually no direct relationship between the authenticating party and the party that issued the original, identity source document.

Now, because more real-world transactions are carried out over the Internet, we see trust relationships, both formal and implicit, acquiring a steadily more important role.

Service oriented architecture (SOA)

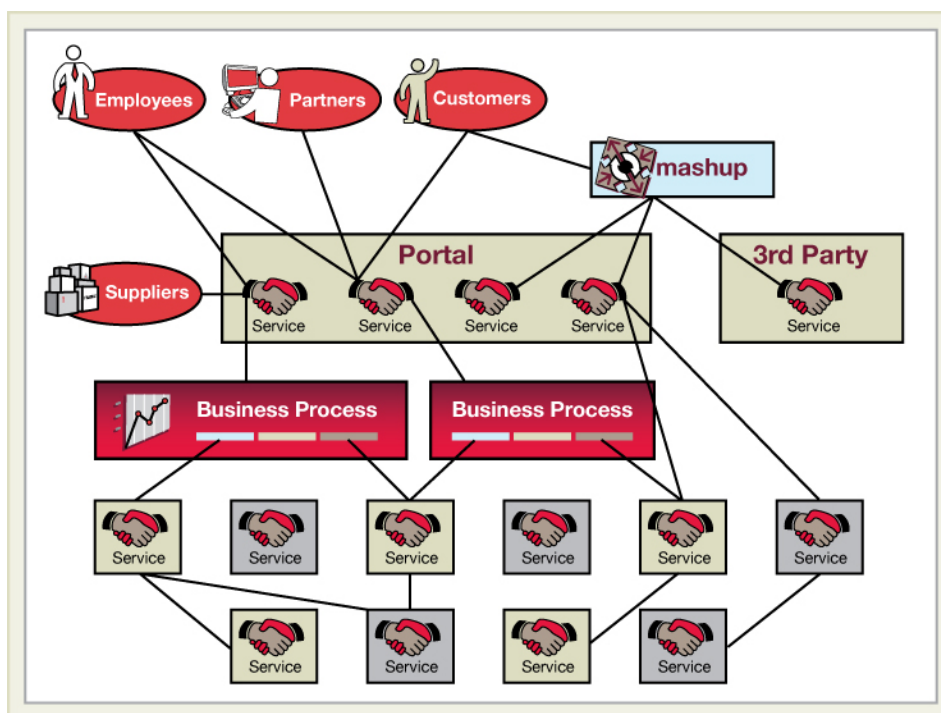
SOA is becoming the standard architecture in both enterprise IT and on the Internet. At its most fundamental level, SOA promises reusability. Enterprises can define specific services that can be used in multiple scenarios and in combination with other services. Loose coupling means that we can combine and recombine services to relate them only in the current content being used. Every new context comes with a new set of relationships.

This means that the relevance of a consumer's identity can only be determined in context to the current service used. Access rules vary according to how critical the business process is for that service. In turn, this means – with a few exceptions – we can't give consumers direct access rights to services. Even if we could, we probably wouldn't want to manage access rights in this ever-evolving blend of customers, partner's employees and service-based interactions.

We need to take a similar view on mashups. Here again, the mashup layer means that consumers are leveraging services through another, remote channel rather than directly from the original provider. Often, the mashup itself belongs to a third party – a partner that may not actually be a consumer of the root enterprise's services. Or is it?

The concept of service consumers and providers should drive us to think carefully about our meaning of consumer identity. If a service is consumed by another service as part of a business process, what is the relevant identity: the consuming service or the ultimate consumer of that business process? Our answer has deep implications for identity and access management within a provider's domain.

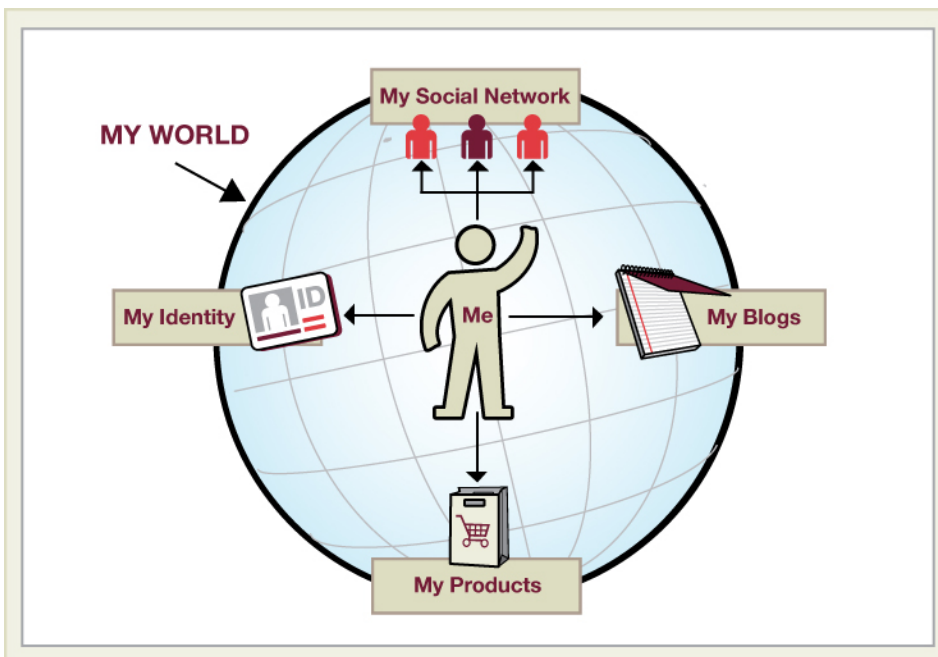
The below illustration demonstrates the potential complexities of these situations.



Not surprisingly, this discussion leads to solutions involving high degrees of trust among enterprise networks. Some relationships will be formal and supported by technology and standards. Others, such as our passport examples, will remain largely informal and dependent on the reputation of the identity provider.

User-centric identity

In today's world, each of us carries various forms of identification, such as a passport, driver's license and membership and credit cards, which are issued by different identity providers and carry different amounts of personal information. Within certain limits, we can choose which document to use in different circumstances. We might choose a document based on how much information we want to disclose when requested for identification. When asked to provide evidence of age at a liquor store, for instance, people might not want to present their drivers' licenses, which includes an address, which the retailer doesn't need to know, or a passport, because they may not be in the habit of carrying it or don't want to reveal recent travels. So instead, they may opt to show the minimum document needed – perhaps a student ID card. This is a user-centric model; all the documents are in their possession and they decide which one to use and the exchange takes place solely between the individual and the service provider.



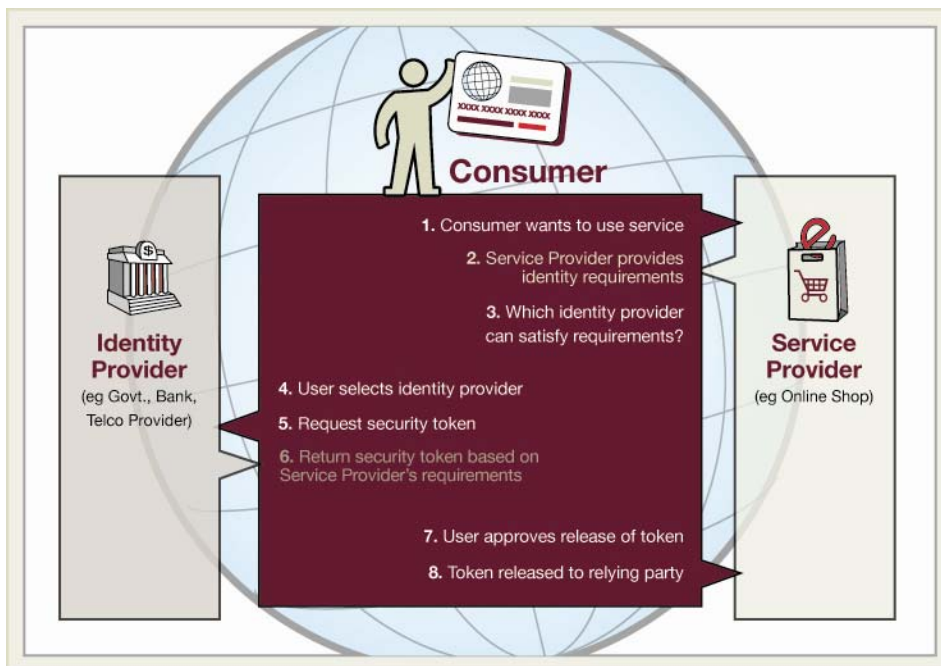
User-centric identity extends that model to support access to computerized systems. In the new Web 2.0 environment, this model is more than a concept; it is a logical operational response. As the illustration depicts, the relationship of the individual has changed from a passive consumer to an increasingly active participant. Therefore, it's probably not a coincidence that user-centric identity is sometimes also referred to as Identity 2.0.

UID standards and solutions

In addition to proprietary and semi-proprietary solutions, an evolving mix of UID standards and solutions are entering the public space, including:

- **OpenID:** A free, open-source solution offered by many providers, including some large enterprises such as Yahoo. Increasing numbers of sites accept OpenIDs, mostly for social networking or blogging. Because it does not transmit identity data securely or verify user-supplied information, the solution is not yet ready for secure services.
- **InfoCard:** A specification largely developed and implemented by Microsoft. Known as CardSpace, this solution is built into the Vista operating system and more recent releases of XP. InfoCard supports secure transmission and includes the concept of a “managed card,” which is select identity information, such as date of birth and passport number, which could reasonably be verified. An identity provider is obliged to verify this information before issuing a card and the user is not able to change it without re-verification. Additionally, the user may store unmanaged information, such as preferences and other profile information. (Refer to the below illustration – User-Centric Identity: The InfoCard Model – for more information.)
- **Higgins:** A specification related to the InfoCard structure. This approach incorporates an interface layer that allows mapping to CardSpace, OpenID or any other standard or proprietary approach.

The common factor across the above solutions is that consumers directly own and manage their identities and profile information – not the service providers. That means that identity and service providers must build implicit and explicit trust relationships.



THE VALUE OF USER-CENTRIC IDENTITY

User-centric identity can significantly reduce the number of user IDs and passwords to remember. It won't deliver single sign-on but will allow the same sign-on – perhaps ultimately part of a genuine Web single sign-on.

User-centric identity helps protect privacy because service providers don't get more personal data than we agree to provide. The benefits for enterprises include reduced complexity in their requirements to manage external users' access rights.

User-centric identity also can help to make reputation portable, because the reputation is associated with the same “identity” across multiple sites – if the owner wishes to enable that.

There are technical, commercial and probable regulatory issues to be addressed before Identity 2.0 becomes standard. These include setting up trust relationships, relinquishing proprietary control of user information and acceptance of common standards.

Identity providers and trust

Identity providers are central to the success of Identity 2.0. However, we need balance to provide enough consumer choices without creating an environment that is even more complex.

Identity providers need to be trusted – by service consumers and by service providers. Amidst the evolution of building trust relationships, we must be mindful of resulting complications where different identity providers are needed for different service providers. Ideally an identity provider should be an enterprise with a public and reliable reputation. Up to now, most identity providers have been small, Internet-friendly organizations without the capabilities to verify and manage critical information. Larger Internet enterprises have opted for proprietary solutions where, perhaps, they use standards such as OpenID but do not accept anyone else's OpenIDs. For the time being at least, we should look to traditional enterprises as authoritative providers.

Governments are well-placed to become identity providers. In delivering on their primary mission, they already collect and archive much personal information and, in principle, people view them as accountable and reliable. Larger financial institutions also have the public visibility and the necessary relationships to make this work. Telecommunications enterprises could also step into this space because they already maintain identity information and often serve as ISPs.

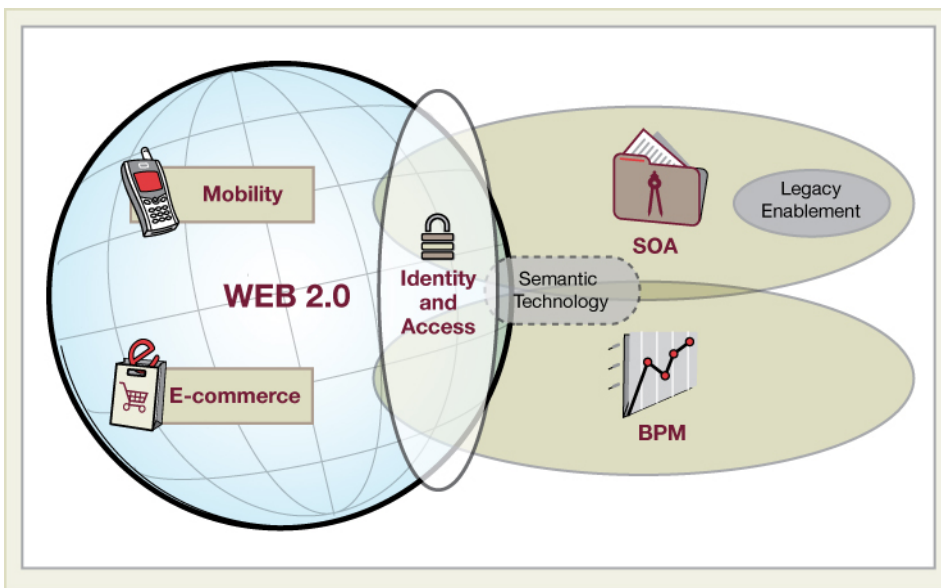
In the end, the key factors will be a mixture of willingness, reputation and trust.

CGI solutions for identity and access management (IAM)

Authentication and authorization remain the most widespread and demanding uses of identity. Implementing these functions efficiently, effectively and reliably is essential for data protection, privacy, security and regulatory compliance. As a result, any successful, new approach to identity must satisfy the authentication and authorization requirements of a wide variety of types of enterprise.

The revolution under way in how people and businesses embrace IT is driving the need to look beyond these two core functions. At the heart of all IT transactions today, enterprises need a new approach that reflects emerging opportunities and risks associated with individual identity.

CGI believes that IAM solutions must be designed for the networked world, open systems, Web 2.0 and SOA. Even within a single enterprise, this can reduce complexity and deliver agile solutions. To deliver the optimal benefits, IAM must be designed as a business solution – not a technology afterthought. That is why, as the below illustration (“Architecture for the Agile Enterprise”) demonstrates, CGI positions IAM as a key enabling technology. Our approach combines that strategic vision with a practical implementation approach that delivers benefits quickly while allowing for incremental investments and added flexibility to build and adapt for the future.



Features of our solutions

CGI regards Identity 2.0 as the ideal model for an IAM architecture. It is not a one-size-fits-all solution, but rather provides the framework for adapting to the concrete realities of a specific enterprise. Identity 2.0 comes with guiding principles, which are described in more detail below.

Within the enterprise

Authentication and authorization should be agent-based, using the model of policy enforcement points (PEP) and policy decision points (PDP). The main advantages include:

- Services and applications concentrate on their functionality and don't have to know anything about the access management infrastructure. Thus, both can evolve independently. This simple separation of concerns is a basic principle of any good design.
- Management and maintenance are simplified because, at most, only one PDP per domain is needed and all access rules are stored only in the PDP. PEPs are deployable (i.e. as many as we need, where we need them, when we need them) and do not require maintenance. Even redundancy for a PEP is a minor issue.

Access rights to business processes must be applied at the initiating service – not in a chain of other services to which users have no natural rights. In particular, as legacy applications transform to service structures, we should move away from individual user access rights. Access depends on the business process in use. If we don't adapt to the current context, we end up with unnecessarily complex user provisioning and hard-to-maintain identity propagation and mapping. When you take into account access by customers and partners, the benefit of transitioning to this model is even more obvious.

Role based access control (RBAC) should and can be drastically simplified, because too much irrelevant information is often used in the initial assignment – including geographic, job and department differences. Applying the principle of separation of concerns provides a framework for streamlining complexity while managing different functionality in different places.

Customer-facing IAM

CGI believes that user-centric identity is the right approach for enterprises to take for their customers. Enterprises need to look outward and capitalize on available information, which, in turn, can deliver the optimum experience for their customers. To be ready, enterprises need to ensure the following:

- IAM solutions must support OpenID and/or InfoCard and be ready for new initiatives. The Higgins framework provides the best option for a catch-all solution, allowing enterprises to incrementally extend their support range without undermining the underlying logic. There are also proprietary products, which often lead the way, while standards and interoperability between standards are developing.
- There are trust relationships with their identity providers. These providers must be trustworthy and their implementation of designated standards must involve verifying critical customer information. They must also support secure transmission of data.

One path could be for enterprises themselves to become identity providers. While some enterprises do this on their own, many often involve a partner. This partner may be an integrator, such as CGI, the enterprise's own business partners or a complementary branch. This approach allows enterprises to provide identity as a customer offering and employee protection. This solution delivers the optimal leverage of profiles and reputation, as well as providing enterprises with support for multi-channel access ("always on" connectivity) and context-driven services.

Enterprises can still choose to maintain their own customer registry. If the prescribed approach to access management has been implemented, user provisioning for customers does not have to be complex. The question is rather whether this will be a viable long-term solution.

Partner-facing IAM

Access management for partners may require a different approach for two main reasons:

- We cannot assume that a partner enterprise is ready or able to support user-centric identities for its own employees.

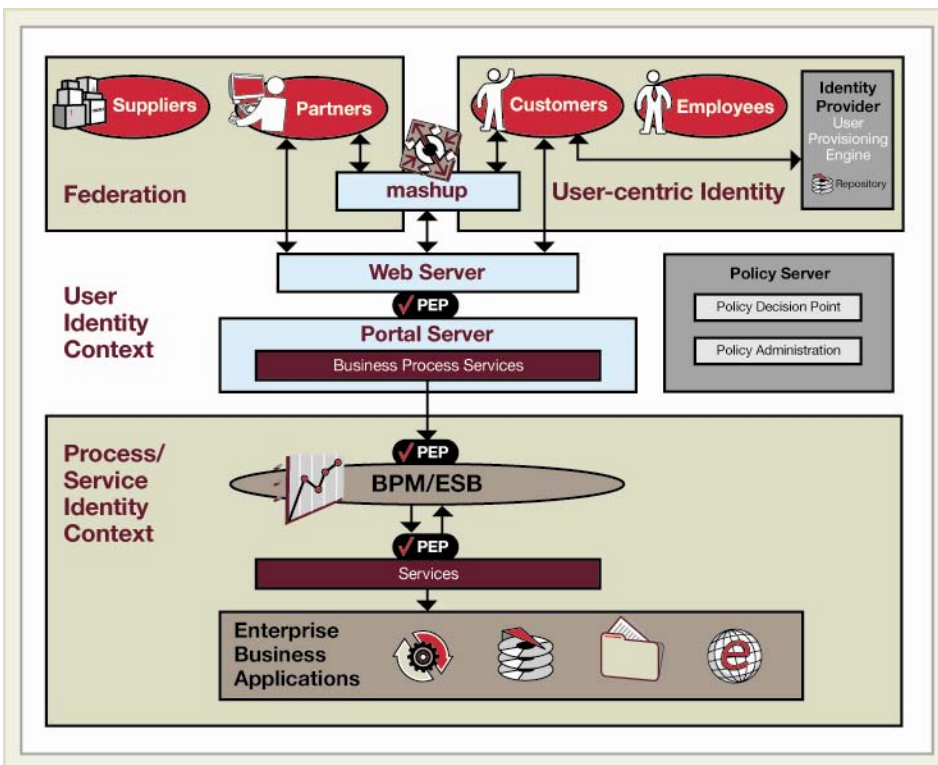
- When dealing with access by partner employees, enterprises may be more interested in their role in core business processes – something the partner enterprise can control. Those employees' actual identities are not directly relevant to the work.

In this case the right solution may be federation, a mature technology with well-established standards, such as SAML and ID-FF. Federation allows enterprises to accept identity tokens and associated claims from partner organizations with which they hold established trust relationships. The standards allow the received token to be validated by the partner. Thus there is no requirement to provision identities or identity associated rights.

In addition to these and other standards – such as WS-Federation, which is useful in a Microsoft environment – mature products are available that support those standards and may offer additional interoperability functionality.

Putting it all together

The below illustration demonstrates one possible architecture, which uses the technologies and architectural approach that has been discussed to deliver a secure and agile solution. With established vendor relationships and through appropriate standards and an agile approach, CGI delivers tailored IAM solutions that allow clients to successfully execute their business strategy.



ABOUT CGI

At CGI, we're in the business of satisfying clients. For more than 30 years, we've operated upon the principles of sharing in clients' challenges and delivering quality services to address them.

A leading IT and business process services provider, CGI has approximately 27,000 professionals operating in 100+ offices worldwide, giving us close proximity to our clients. Through these offices, we offer local partnerships and a balanced blend of global delivery options to ensure clients receive the combination of value and expertise they require.

In the area of technology leadership, CGI helps organizations achieve the promises of new technologies and business approaches through a practical approach to transformation. We define success by exceeding clients' expectations and helping clients achieve superior performance.