

Putting Trust in the Web

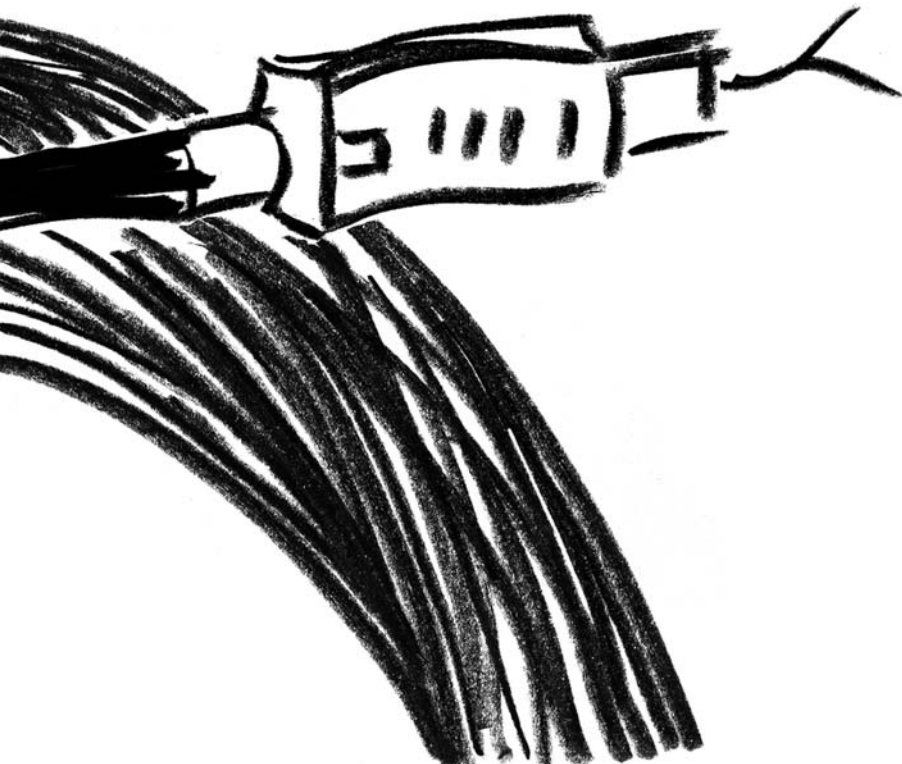
Identity theft is crime's greatest growth sector. The FBI says that 27.3 million Americans had their identities stolen between 1998 and 2003 – more than one third of them in the last 12 months of that period alone. Mafia-like gangs of organised criminals are increasingly engaged in “phishing” schemes which use e-mail messages to lure unwitting consumers to websites masquerading as home pages of trusted banks and credit card issuers, where visitors are incited to reveal passwords and other sensitive personal information. Security analysts and law enforcement officials are deeply worried, while Internet pundits fear that users may start to turn their backs on what they perceive as an unsafe system. In fact, 44 percent of computer users have already reduced their use of e-mail and the Internet in the last 12 months, according to findings of a survey conducted by Osterman Research early this year.

*Is there a
way out?*

“Yes,” says Dr. Hellmuth Broda, European head of the Liberty Alliance, a consortium of more than 150 technology companies (including HP) and consumer organisations dedicated to a concept called Identity Federation, or IF for short.

“Today's acceptance of Web-based services is hampered by the lack of consumers' trust in the system,”

says Broda. “Also, network identity nowadays exists for each user in numerous unrelated “information silos” that cannot interoperate. Users have to remember hundreds of user IDs and passwords or pin codes.” An interoperable federated approach for Network Identity and Trust Management that would also guarantee privacy and security of the consumer's information could help the public to gain trust into these systems and finally increase the acceptance for network delivered services, he believes.



The charm of IF, many experts feel, lies in the fact that the information about a person's identity remains in its original location at all times. Instead, it relies on sharing information using computer systems based on industry standards developed by the Liberty Alliance, the most remarkable feature of which is that the person whose identity is being shared maintains complete control over his or her personal information.

IF requires organisations to form so-called "circles of trust" based on common rules as well as contractual agreements. Naturally enough, the most trustworthy environment of all, and therefore the one in which IF is almost certain to take root first, is within the enterprise itself. Since employee identities can be managed centrally and brought online and offline quickly, deployment of IF promises to limit the company's vulnerability to security attacks by current or former staff members and contractors, while providing the ability to outsource certain applications and tasks in a more secure manner.

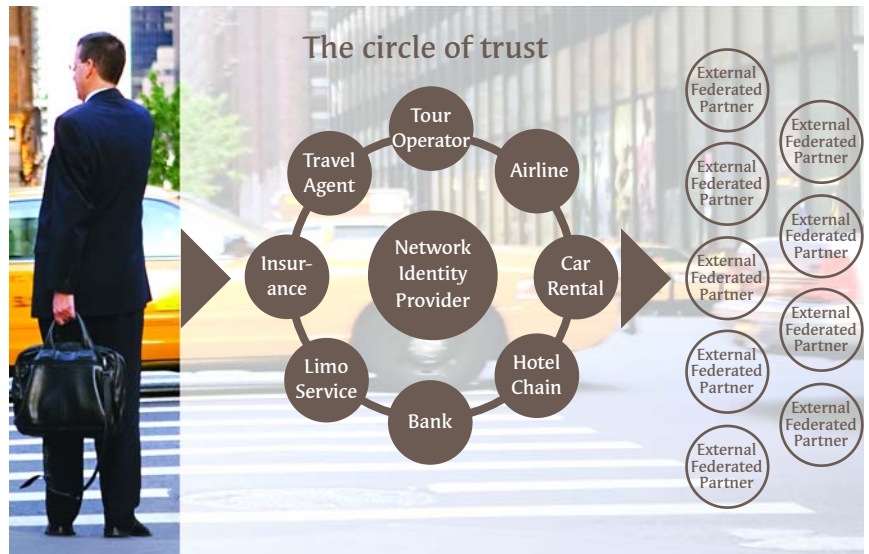
Companies like General Motors use IF in their employee portals to reduce gridlock caused by the constant need to type in user names and passwords for dozens or even hundreds of applications. According to John Jackson, GM's director of software technology, federated single-sign on has been such a huge success "that we didn't even try to calculate return on investment on this project – it was just too obvious!"

IF's pot of gold at the end of the rainbow, however, is enabling different companies and agencies to manage and share the identities of customers or citizens within such a circle of trust. Financial services such as Visa or BankAmerica in the U.S. have announced their intention to team up with major airlines, hotel chains and car rental companies, allowing mutual customers to deal with any or all members of the circle without having to manage separate access routines or update personal data for different accounts. In Britain, regional government agencies are pooling their information in order to provide a much wider range of online services to citizens. According to Helmuth Broda, future "e-government" projects will eventually cross national borders and may lead to public/private partnerships with administrations and companies cooperating to better serve both citizens and customers.

Key to IF, is the way requests for information are handled within an established circle of trust. Physically, the information remains on the computer system of the company or authority that "owns" it. Other members of the circle can "borrow" the information in order to perform certain clearly defined tasks, and each transfer must be approved by the user himself.

To take an example: Say that Visa and Lufthansa share membership in a circle of trust and a customer buys a flight ticket. Visa would handle the financial transaction itself and "lend" the customer's address to Lufthansa so that they can mail the ticket to the purchaser. However, this information is not stored on the Lufthansa system; in fact, if the hardware and software components conform to the Liberty specifications, they can't store it because the system won't allow it. Given the huge acceptance of such Liberty standards as SAML (Security Assertion Markup Language) or ID-FF (Identity Federation Framework) within the computer industry, the concept appears to be gathering steam, especially since Microsoft and the Liberty Alliance recently buried the hatchet on their competing schemes for IF, agreeing instead to aim for full interoperability between Liberty and Microsoft's own WS-Federation standard.

The future looks bright for IF, it seems, as more and more companies climb on the bandwagon. AOL recently joined D-Link, a major player in the digital home entertainment market, to extend AOL's Internet broadcasting service (Radio@AOL) beyond the computer and into any room with a TV or stereo. Liberty Alliance specifications allow AOL and D-Link to share information about both users and devices to provide instant authentication and billing. Using standard protocols works in favour of both customers and partners, says Conor Cahill, Chief Architect with AOL. His verdict: "Federation pays!"



The circle of trust concept
Source: Liberty Alliance