

What Microsoft's Identity Metasystem Means to Developers

Laurianne McLaughlin

Every day we use a bevy of identity technologies to prove who we are to various systems, whether we're logging on to a virtual private network or buying from an online store. For users, this means an increasing number of passwords and routines, leading to security fatigue and occasional confusion. For developers, it means working with a hodgepodge of different identity technologies—a situation that doesn't help with maintenance, ongoing security risk analysis, or innovation. Microsoft's proposed answer to this problem is an identity metasystem—a framework that lets varying identity technologies communicate and interoperate using common standards.

Microsoft likens the metasystem's role to the role IP plays for varying network technologies.

InfoCard, the end-user software piece of Microsoft's framework, will give Windows users a visual portfolio of digital identities. Behind the scenes, protocols for messaging and security token services will let various identity technologies communicate with each other, negotiating requests and exchanging information. If Microsoft's identity metasystem gains wide acceptance, how will it affect software developers?

Could it save development time, promote improved technology, or ease some security maintenance woes, for example? Just how well the system works will reveal itself over time, as companies write to the common standards and tap into Microsoft's framework.

The need for some sort of identity metasys-

tem has become real, says Phillip Windley, an associate professor of computer science at Brigham Young University and former CIO for the state of Utah, who recently authored *Digital Identity* (O'Reilly, 2005).

"We're never going to get to one identity system for everyone," Windley says. "So we need a way for them all to operate together."

"I don't like the name 'identity metasystem'," says Mike Neuenschwander, VP and research director of identity and privacy strategies for the research and consulting firm Burton Group. "I like the concept very much. We do need better interoperability for identity information. We need to have a better set of standards around this."

Developers should take an interest in Microsoft's proposed set of standards, keeping in mind that the proposal is still a work in progress and that only time will tell whether the framework wins widespread adoption, Neuenschwander says.

How it works

Microsoft is careful to say that its identity metasystem is not Passport, Microsoft's controversial attempt to manage digital identities for end users. Passport was meant to serve as an identity service itself, managing password and purchase-related data for consumers and passing it to Microsoft e-commerce sites and other e-commerce partners, originally with charges to those partners for participating.

But in the identity metasystem, Microsoft

has helped construct a framework within which various online identity services and e-commerce sites can operate without paying Microsoft. The identity metasytem encourages companies to build to common standards.

The need for such a system became clear to Microsoft as it worked on its next-generation Indigo Web services technology, says John Shewchuk, Microsoft CTO for distributed systems and an architect of Indigo. For users, the password problem only continues to grow. For developers, the workload intensifies as new identity technologies hit the market, he says.

“What we as computer scientists have always done for this sort of challenge is build an abstraction,” Shewchuk says. For example, PC file systems solved a similar problem, he says. “For developers, they can program against the abstraction without worrying about those details.”

Today, developers must deal with such identity technologies as public-key technologies, Kerberos (used with Active Directory and in some Unix environments), and X.509 (used with smart cards). There’s also the Security Assertion Markup Language, an XML standard for authentication and authorization. SAML was developed by the OASIS (Organization for the Advancement of Structured Information Standards, www.oasis-open.org/home/index.php) Security Services Technical Committee, which is tackling the issue of single-sign-on technologies.

“This means different sets of APIs for each, and a lot of work supporting all these different models,” Shewchuk says.

The common specs are known as the WS-* Web services architecture. There’s also an encapsulating protocol known as WS-Trust, and negotiation tools called WS-MetadataExchange and WS-SecurityPolicy. Microsoft’s goal is that new technologies plug into the architecture as they arrive, using the common specs, which it notes are freely available and traveling through open-standards groups.

Microsoft’s identity metasytem starts with the idea that you need a way to associate claims (such as “I am John”)

with messages. Next, you need a way to tell users that to process their claim, you need a credential from a respected party.

Finally, you need a security token service. “This serves as a kind of cool universal translator,” Shewchuk says. “You give me X.509, I give you a Kerberos ticket. Because it’s designed with open protocols, anyone can run a security token service. Sun, Yahoo, Google could all wrap their own identity tokens. An IBM mainframe with Kerberos can work with a SAML token.”

You can also think of the metasytem as a triangle, with the WS-* protocols inside. At one corner is Indigo, Microsoft’s next-generation Web services technology, which knows how to associate credentials with messages. Indigo also serves as Microsoft’s messaging infrastructure for developers.

At corner two is Microsoft’s Active Directory product, which lets IT professionals create rules regarding access and security, among others. It’s Microsoft’s implementation of WS-Trust. The third corner is the end-user piece of software. In Microsoft’s case, this is InfoCard.

But you can replace any point on the triangle with another non-Microsoft implementation, so long as the provider adheres to the WS-* specifications, Shewchuk says. (For more information, see <http://msdn.microsoft.com/webservices/default.aspx?pull=/library/en-us/dnwebsrv/html/identitymetasytem.asp>.)

Microsoft is attempting to deal with some important security issues, Neuenschwander says, such as exchanging different kinds of tokens. “But whether all this needs to be done in the WS-* stack remains to be seen,” he says.

“The entire world isn’t going to

switch over to WS-*,” Neuenschwander says. “The best we can hope for is better interoperability. The promise of interoperability is quite good.”

The upshot for developers

For developers, the first result is that this metasytem lets them link existing identity-related systems with new systems as they emerge.

“By placing security token services into your systems, it lets you stitch things together—quickly. Fortune 500 companies are excited about that,” Shewchuk says.

Also, Microsoft proposes that developers should like the metasytem because it will eliminate some learning curves. “I don’t have to learn Kerberos, X.509; I just learn how the metasytem works. There should be a lot less learning required overall, and with the learning you do, you could achieve more,” Shewchuk says.

Some longer-term maintenance and security benefits could accrue as well, says Kal Toth, associate professor of computer science at Portland State University and associate director of the Oregon Master of Software Engineering program.

“A lot of people don’t understand identity management very well,” Toth says. “A lot of IT departments are using fragmented systems; usually it’s a patchwork, even in sophisticated organizations. In that kind of patchwork environment, it’s easy to make mistakes and it’s hard to maintain security.”

For example, when people leave a company, many different identity-related holes must be closed, he notes.

There are many details to manage, from high-level policy statements to lower-level implementation details, Toth says. “Simply integrating the range of applications is not trivial,” he says. “Plus, a complete analysis of risks is often not done.” InfoCard will automate more, presumably eliminating errors, he says.

For example, Toth feels InfoCard could be of particular help with Web services security policies. The best examples, he says, are security policies where people change status. The security policy might block that person

**For developers,
the workload
intensifies as new
identity technologies
hit the market.**

from accessing certain databases, but the person might be able to break in via another application.

“Developers are aware there’s a problem but often don’t understand all the vulnerability points,” Toth says. “Automated systems enforce things that are easy to overlook, or make up for people who are missing training.”

But Toth notes that the full picture on the WS-* standards won’t emerge until more people have a chance to work with the tools directly.

How much time might the identity metasytem save developers? For an analogy, Windley suggests thinking back to the Web’s early days when everyone wrote CGI programs. Then a couple of years later, developers could just pick whatever they needed from CGI libraries.

“Once the metasytem is defined, a lot of identity issues could become library options we include instead of software we develop,” he says.

Another benefit: “Developers potentially have access to richer sets of data, without having to plan for it,” Windley says.

For example, the metasytem could make it easier to work with credit card numbers for businesses who don’t want to have to store them.

“I can stop storing as much personally identifiable information, which lessens my security concerns,” Windley says.

More attack protection?

Microsoft argues its metasytem will also promote innovation in identity technology and help developers quickly adapt to new attack methods. Of course, many technologies aspire to those broad goals.

“What we have developed over the past 20 years of computing security is a siege mentality,” Windley says. “That doesn’t work with Web services. With Web services, people need to get into my network. I can’t keep everything on the edge anymore. I can’t just let partners handle the identity information. Now the question is an identity problem.”

Moreover, Windley says some sort of identity metasytem must come to pass for e-commerce to remain trustworthy. As clever as developers have

been at fighting certain e-commerce threats, problems such as phishing just keep getting worse.

“If you extrapolate where we are now with phishing, do we get to the point where the Web is only good for valueless transactions?” Windley says. “My bank can’t communicate with me via email [because it’s too hard to tell the real bank emails from the fakes]. The only viable answer to this question is an identity system upon which people can build trust technologies.”

Rivals weigh in

Some developers might see more immediate benefit from the identity metasytem than others. Who can take advantage of an identity metasytem quickly, and who can’t?

“Microsoft is very good at building developer tools. I suspect if you’re a .NET programmer, things will happen fairly easily,” Windley says. “Whether it’s easy in other languages depends on the community developing tools.” So, the ball is partly in the developer court with regard to creating and sharing these tools, he says.

The metasytem’s heavy dependence on Web services based on SOAP (Simple Object Access Protocol) might hamper it, Windley notes. That’s fine for Java developers, but not so great for other developers—say, PERL developers—he says.

People who are using other programming languages might choose something other than Microsoft’s architecture, Windley says. But if the Microsoft client piece drives ubiquitous adoption, and developers find it compelling, modules could appear in every programming language, he claims.

Will a direct, broad competitor to Microsoft’s vision emerge? Perhaps. Some companies are marketing proprietary systems. For example, Sxip Identity (www.sxip.com) has its own vision of identity management.

“Sxip’s point of view is that what Microsoft has constructed still looks a lot like corporate standard, but it’s not Internet-enough,” Neuenschwander says. “How open is it? Whether Microsoft has gone far enough remains to be seen.”

Some companies would like to see the WS-* specs published to standards bodies earlier than they have been, Neuenschwander notes, a sore spot that has caused some grief for Microsoft with the developer community.

Also, some companies wonder if the WS-* stack is overly complex, Neuenschwander says. “That WS-* stack could be heavy if you’re just doing consumer apps on the Net,” he says. “Is it too much of a requirement once you get outside of corporate environments?”

Dick Hardt, Sxip CEO, says the WS-* stack could be overkill for some applications. “InfoCard is great for securing the desktop,” Hardt says. “I think that WS-* is too heavy for most identity requirements and too rigid.”

How does Hardt’s broad vision for identity technology differ from Microsoft’s identity metasytem?

In Microsoft’s vision for the metasytem, companies such as Sxip could become part of the competitive playing field within the metasytem, but whether that comes to pass depends on how the competition plays out.

“At a high level, we are aligned,” Hardt says. “We think it is important that a user is able to participate without having to install new software on the client, so we differ there.”

Another rival group, the Liberty Alliance (www.projectliberty.org), which represents 150-plus corporate, nonprofit, and governmental groups, is also working on industry standards for identity technology.

“I don’t think we’ve arrived yet at the right architecture” for an identity metasytem, says Neuenschwander. “I wonder if Microsoft has gone too far in decentralization. We’ll get there. There’s a conversation happening. The market has to decide what will work for it.”

Negotiation technology, for example, is a hot topic to watch, Windley says. “Negotiation is one of these things that people are still doing a lot of research on,” he says. “We’re not at the end of that. We’ll see new ideas come out. It’s a different and interesting place, where people could get some leverage building systems.”

Security and privacy ideals

Perhaps the most complex issues surrounding the identity metasytem aren't technical; they're broader social concerns regarding identity and security.

Microsoft's identity metasytem plans include a sort of ethical manifesto, called the Laws of Identity (see <http://msdn.microsoft.com/webservices/default.aspx?pull=/library/en-us/dnwebsrv/html/lawsofidentity.asp>), spearheaded by Kim Cameron, Microsoft's "chief architect of identity and access," and developed via online debate with input from many parties interested in identity technology. See Cameron's blog (www.identityblog.com)

for a look at the ongoing discussion on identity issues. The Laws of Identity touch on user control and consent, minimal disclosure, and related topics.

Will Microsoft's vision succeed? "Kim Cameron has been particularly adept at managing the political challenges internally and externally," Windley says. "He took great lessons from the earlier Passport experience. This system in general is a reasonable proposition. There's no technology reason that it won't work. But people are always fearful of Microsoft.

"In general, the Laws of Identity set a high hurdle for how systems should

work," Windley says, adding he thinks that's a good hurdle. "The impact on developers comes down to an architecture question. It may be a matter of business advantage to choose an architecture other than Microsoft's ... or it may just be easier."

For example, some companies really are trying to control information because it gives them lock-in with customers, Windley says. Consider how tightly cell phone companies like to control customer data, he suggests. So ultimately, the metasytem's impact on developers will vary greatly by industry as well, he notes.

Open Source and Government Systems: Goscon 2005

Bart Massey

It's always fun to witness the founding of a new tradition. The First International Government Open Source Conference, sponsored by Oregon State University's Open Source Laboratory, took place on 13–14 October 2005. After watching the positive experiences of the organizers, presenters, and attendees, I'm sure GOSCON was the first of what will be a long, successful conference series.

Enthusiastic attendance

For a first-time conference, GOSCON did extremely well at attracting national and international government participants. IT folks from the State of Oregon formed one of the largest contingents, and there were many Western US participants. That said, Massachusetts, which is in the throes of its own government open source revolution (more on that in a bit), had several speakers and attendees, and partici-

pants came from as far away as Europe and Argentina.

While the issue of open source crosses all levels of governments worldwide, most GOSCON participants were either IT officials in US state and municipal governments or employees of government-related commercial concerns. I spotted few US federal officials and even fewer politicians and policymakers. This might be due partly to GOSCON's newness; these latter groups are fairly risk-averse. On the basis of this inaugural event's success, however, I expect to see a broader representation next year.

Notably, GOSCON 2005 was completely sold out, and the initial registration had to be expanded. In the end, around 200 people attended in some capacity. This is somewhat remarkable for a first conference. Although the venue was quite nice, next year's conference will need a larger space.

Of course, the conference achieved

such enthusiastic attendance because the attendees perceive that government open source is successful, or at least headed in that direction. Many folks believe that open source addresses a lot of government IT concerns in ways that proprietary solutions don't. GOSCON provided a good forum for comparing notes on these issues.

Is open source for government different?

The most spectacular ways that open source is being fielded in government aren't necessarily the most common ways. For example, open source polling systems have received a lot of attention. This is a great idea on several levels, but I heard little mention of it at GOSCON. Instead, the focus was on traditional IT. (For more on this, see the "GOSCON 2005 Panels" sidebar.)

Government IT organizations have many of the same problems as their

Goscon 2005 Panels

The conference featured four panel discussions: Open Source Implementation, Open Source Strategy, CIO Perspectives, and Open Source IT Skills.

Strong panels require strong panelists; GOSCON did well in this regard. Several open source business leaders participated, including Bernard Golden, Navica CEO and popular columnist and blogger. Government and university IT directors were well represented—for example, Portland State University CIO Mark Gregory, Oregon State University CIO (and conference chair) Curt Pederson, Oregon Department of Human Services CIO Bill Crowell, and City of Newport News, Virginia, CIO Andy Stein. Their frank discussions of their organizations' internal open source technical and political issues brought an air of realism to the proceedings. However, one of the few actual open source development folks participating was Tim Ney, executive director of the GNOME Foundation, which oversees work on the GNOME (GNU Network Object Model Environment) desktop environment. Portland, Oregon's eminence as a leading open source city eased the recruiting of top panelists. Local talent contributed substantially to the discussions, with employees and directors of organizations such as the Oregon Department of Transportation and Department of Administrative Services giving ground-level explanations of how open source was being used in their environments and how well it was working.

Of course, a major point of the panel format is to represent a variety of perspectives. While the panels were well run and most panelists provided a unique take on at least some issues, overall there seemed to be more consensus than disagreement about the current state of affairs and about future directions. The general inclination seemed to be to treat government open source IT issues as "ordinary" open source IT issues by default; panelists only occasionally highlighted the differences. Many participants expressed concern about cost, planning, and deployment strategies. One particularly challenging problem appears to be how to maintain and reuse legacy government systems containing proprietary code during a transition to open source. Participants occasionally discussed and debated retraining costs, with some agreement that the desktop would move toward open source last in most government organizations.

sure both to adopt open source for its imputed benefits and to reject it for its imputed risks.

Open source and procurement

Open source is changing government procurement. Government (almost any government) is driven by legendarily arcane and complex processes for purchasing outside goods and services. There are good reasons for this, rooted in fairness to citizens and suppliers, the desire to avoid waste and corruption at all costs, and the complexity of government itself. Open source gives government IT personnel the opportunity to circumvent the procurement process. Software freely downloadable in source form isn't just free of charge. As several GOSCON participants noted, by circumventing the procurement process, it can provide something even more valuable: freedom from hassle and delay.

Of course, several concerns constrain this potential. For example, many government officials still poorly understand open source licensing and its risks. Also, the lack of official, paid support for most open source products is a problem in an environment that must balance in-house development and support with the need to purchase outside assistance. Indeed, several GOSCON speakers and participants indicated that the lack of credible outside organizations to take the lead in providing open source through the normal government procurement process is a serious problem. Solid business opportunities in this space seem to exist for those savvy in the ways of government contracting and of open source.

Saving money and effort

As with any IT organization, much government IT software is produced in-house. GOSCON participants report that much of this software is becoming open source. Many people believe that software produced with taxpayer dollars should be made available to taxpayers. While some would suggest that this could be a revenue opportunity for cash-strapped governments, the open source model has its own attractions in the form of low distribution cost, community sup-

nongovernmental counterparts, but they also have unique concerns. First, they tend to be more cost-sensitive than most corporations. They're also accountable to taxpayers, sometimes a fickle and finicky bunch. Finally, they have big legacy systems on a scale that you don't see in younger organizations.

The question is whether differences in government IT imply differences in open source strategies and process. GOSCON governmental IT participants seemed genuinely interested in open source experiences outside government and clearly appeared to believe that many strategies and processes would transfer. At the same time, the participants noted some novel aspects of open source for government. For example,

because governments generally don't compete for customers, the incentive to keep information and tools proprietary is much less strong. Indeed, governments generally aren't entitled to hold intellectual-property rights to their works on their own behalf. On the other hand, government development tends to be less agile than development in the commercial world. There can be a lot of inertia to overcome in such venerable, people-intensive organizations. In addition, taxpayers scrutinize government software development methods and processes more intensely than commercial customers monitor proprietary products' development. This difference can cut both ways: government organizations have reported pres-

port and development, and transparency to government constituents.

Furthermore, the formation of inter-governmental open source consortia around specific missions could distribute the production costs of some kinds of governmental applications across multiple governments. Scott Kveton and Jason McKerr of the OSU OSL held a nice tutorial on this topic at GOSCON. One of the largest groups participating consisted of Corrections Office IT personnel from several western states who have formed a consortium to produce an open source corrections-related application package. GOSCON gave this group a nice venue for meeting, discussion, learning, and dissemination.

Open source could save the taxpayer money. Consequently, proprietary government solution vendors are looking at open source with increasing interest and concern. While even “free” software has real costs, there’s a hidden wild card here. In the next few months, Microsoft will release Windows Vista, its first OS upgrade in many years, and a new version of Microsoft Office that uses a document format unreadable by older Office versions. (Reportedly, the Gartner Group recommends that organizations delay upgrading to the new Microsoft software until around 2008.) As organizations consider upgrading their existing Microsoft software, including purchasing new hardware and retraining, the costs and risks of moving instead to open source solutions look less intimidating.

Indeed, the pressure is on for proprietary software developers. One of the most-talked-about news items at GOSCON was the recent Massachusetts decision that software for managing government documents must support open document formats. Linda Hamel, general counsel for Massachusetts’ Information Technology Division, gave a nice account of the Massachusetts government’s reasoning and process (for a detailed account, see the “Massachusetts Moves to Open Formats” sidebar). Although opposition to the move (by a fairly predictable cast) is still developing, many others appreciate the benefits that can come from ending

Massachusetts Moves to Open Formats

One of the most interesting recent events in government open source has been the Massachusetts decision to require open formats for new state archival documents and to require that new software acquired by the state adopt these formats. This move resulted from an initiative begun in 2003 and supported by Governor Mitt Romney. While Microsoft attempted to have its new XML-based Office document format certified as open, ultimately the state decided that the documentation and intellectual-property concerns regarding the format made it unsuitable.

In an invited talk at GOSCON 2005, Massachusetts IT Division General Counsel Linda Hamel described the history and goals of the Massachusetts open-formats initiative. In 2003, a commission appointed by the State IT Division was charged with recommending an IT strategy for the state government. The result was a report concluding that adherence to common standards and avoidance of vendor lock-in was key to government organizations’ interoperability and government records’ long-term survival.

In January 2004 the commission produced a report recommending a new requirement of adherence to open standards for data management, with a documented Open Standards Policy. This policy requires future procurement of open-standards-based products, wherever possible. It requires selecting software by best value after considering open source, proprietary, and public-sector alternatives.

Of particular interest was a list of concerns regarding the new state policy, including

- current software’s ability to support open formats,
- current non-Microsoft software’s support for users with disabilities,
- the new rules’ range of applicability,
- what to do about data that legacy systems are producing,
- interoperability inside and outside the government, and
- migration costs.

These concerns have focused mostly on office document formats, with other kinds of data receiving less attention.

The Massachusetts initiative looks as if it will be a success, meeting its goals of document exchange and preservation. However, there has been political and industry pressure to derail it before it really starts. It will be interesting to see to what extent Massachusetts’ intellectual leadership on this issue continues.

document lock-in and permitting support for open source document management and processing.

The future of government open source is still being written. GOSCON is one place where this writing will happen. Kudos to conference organizer Deborah Bryant and all those who made this a truly important and enjoyable event. ☺

A disclaimer

While I wasn’t an official conference organizer, I did help the OSL folks prepare the conference and chaired a panel. Although I’m an open source developer, researcher, and advocate, I have no particular stake in the governmental arena.

Bart Massey is an assistant professor of computer science at Portland State University, where he teaches and researches open source, software engineering, and artificial intelligence. He’s also on the faculty of the Oregon Master of Software Engineering program. Contact him at bart@cs.pdx.edu.