

GM DEPLOYS FEDERATED IDENTITY AND LEARNS

It's often said that there's no school like experience, and for GM that has proved true with identity. No enterprise has spent more time and effort to understand and deploy identity on a large scale. GM was a founding member of the Liberty Alliance because they knew that their collaborative business model would require them to understand and implement identity federation. Despite all this study and experience, however, actually traveling the road to federated identity deployment still had lessons to teach that would alter GM's perspective on identity.

General Motors is the world's largest automobile company, employing about 325,000 people globally. It has manufacturing operations in 32 countries and its vehicles are sold in 192 countries. In addition to automobiles, GM parts and accessories are sold under the GM, GM Goodwrench and AC Delco brands. GM engines and transmissions are marketed through GM Powertrain and the GM Electromotive Division manufactures diesel-electric locomotives and commercial diesel engines. Beyond automobiles, parts, and service, GM operates one of the world's leading financial services companies, GMAC Financial Services, which offers automotive and commercial financing along with an array of mortgage and insurance products. And GM's OnStar is the industry leader in vehicle safety, security and information services.

Learning While Leading

Whatever GM does in IT usually ends up being done on a huge scale

and crossing national boundaries. This has led GM on many "journeys of discovery" and over the past several years GM has learned a lot about how digital identity and IT fit together. Their early experiences with global directories and web access control drove GM to look at federated identity and become a founding member of the Liberty Alliance. In Spring of 2003 they launched their first internal federated identity projects, using Liberty compliant software, to learn about the technology in preparation for larger federated identity projects later in the year.

Last Fall GM began the pilot deployment of their first large scale federated identity project. This was a project to interface a benefits provider with their employee portal called mySocrates. The name is relevant, since the Socratic Method involves professing ignorance and asking obvious questions to bring understanding. And as GM asked questions during their first large



scale federation deployment, they learned a lot – enough that it is changing the company’s entire outlook on digital identity.

“It’s the classic IT story,” said Tony Scott, CTO of GM’s Information and Services organization. “If you think about the insertion strategy for the web in corporations, most corporations did-

Alliance protocols went very well. “We did a proof of concept on linking up our employee portal and benefits information with them,” said Scott. “[It was] very successful in that the technology part was easy and we actually used two different technology providers. We used Sun and they used something else which wasn’t Sun. We demonstrated and tested and even scale tested the Liberty based technologies, and it worked great.”

“Initially, they were a little more skeptical than we were,” said Scott, “but by the end of the pilot they have now decided, and we’ve agreed, we’re going forward into production on this. The software worked very well. We had in this pilot far fewer technology issues than I would have guessed. [It was] far less complex than when we try to interface to a vendor for other reasons, exchange other kinds of data, precisely because the Liberty spec was in place and we had software that complied with the spec. There’s been a lot of pre-thought [put] into how these things might work.”

Like many, GM initially saw federated identity as primarily a technology problem – an extension of their directory services and access control security. But as they rolled out their federated deployment project, they found there was much more involved. “What took a lot more work than we expected,” said Scott, “was we followed our internal methodology and created use cases in detail. We ended up with a lot more use cases than we thought we were going to have. That is, the ways in which people might come at this or intersect the point at which they needed digital identity were far more than we realized.”

n’t start off and say ‘we’re going to move everything to the web and it is the major platform on which we are going to base our applications.’ They started with some folks that were a little more visionary and were willing to try it and experiment. Then, with some success, you reach critical mass and pretty soon it becomes an area that you can start thinking about strategically. That same thing is happening in identity.”

Technology Was the Easy Part

At the technology level, federating identity between GM’s employee portal and the benefits provider using the Liberty

Disguised Opportunity

“We have a lot of different ways you can get to our portal,” said Scott. “When you start talking about digital identity



© 2004 General Motors. All rights reserved.

(above) General Assembly-Lansing Grand River Plant. (right) Standing next to some of the General Motors' vehicles the Hummer H2, Cadillac XLR and Chevrolet SSR, (L-R) Gary Cowger, GM President of North America, Bob Lutz, Vice Chairman Product Development and Chairman GM North America; Rick Wagoner, Chairman and CEO, and John Devine, Chief Financial Officer.



and then access to the personal information, all of a sudden you've got to care a lot more about 'how did this person get to this place in the portal?' Where are they accessing [it] from? Is it a secure environment? Do I really know who this person is, have they really been authenticated on my side? All kinds of stuff like that. And on the reverse side when they leave, when they shut down, when they close the window, do they really in fact log out? So we ended up, bottom line, with a lot more complexity in the use cases than we anticipated we were going to have going in."

"It caused us to do two things," said Scott. "One is we cleaned up some processes that IT sort of evolved but weren't architected over time. You see this all the time. People get systems and

they get incrementally adjusted and proved over a period of time. And pretty soon you have a Rube Goldberg contraption on your hands. It isn't what you originally intended in the first place. So [developing the use cases] pointed out some opportunities for us to clean up our access architecture and paths by which people could get to information in our portal. That was an interesting journey just going through that."

Trust and Liability

"More interesting were the conversations that took place around this [project]," said Scott. "All having to do with trust. What is trust, and what does it mean when you are trusting a third party or a partner?" These conversations became more involved than originally anticipated, and led both parties to

analyze how liability apportions in a federated identity setting. "What you end up with is some lines in the sand," said Scott. "You say 'I'll trust you up to this point, but beyond that, maybe not.' In the example of this benefits provider, viewing information in terms of account balances or positions, those kinds of things, [they said] 'OK, I'll trust your federated identity scheme to do that.' But when it comes time to take money out, transfer money, change beneficiaries or do things that have stronger legal implications [they said] 'maybe I won't trust you for that.'"

These issues were discovered during the extensive use case mapping process, and were addressed as they came up – sometimes with direct effect on the project's scope. "In these use cases you say, all right, I understand your point, you

think that you have legal liability in case something bad happens here, what are you proposing that we do?" said Scott. "Do you want the user to re-authenticate? Do they validate their login information? Are you going to ask them a security question? What are you going to do and how are we going to get those things resolved? And what is the user experience going to be around this?"

implementing federated identity in a changing corporate environment brought the concepts of digital identity into a new focus. "Three or four years ago when you talked about digital identity people would kind of go, 'Huh?'" said Scott. "What is that, why is it important, and why do I even care about this?" One of the interesting things I've seen here is that we've had this whole concern about Sarbanes-Oxley and the adequacy of IT controls. Do you have processes that are consistent enough that the results that those processes produce are reliable and can be counted on? All of that has sort of refocused attention on identity, and not coincidentally."

"So there's been a fresh interest in this topic beyond the sort of academic interest that might have existed," said Scott. "It's become very real and, at least in GM, has become right at the top of our agenda. We are going through an internal re-examination for all of those systems inside that we have and are re-looking at our identity scheme, our login and password management scheme, and so on. And [we are] realizing that there is a tremendous amount of work to be done. It's one thing to have this Liberty spec for the web space, but we've got lots of legacy systems that are client/server, that are mainframe, that are whatever. Certainly a smaller number than we had a few years ago – by fifty percent – but there are still a fair number of them around. And that needs to be addressed."

"[The] interest in [identity] and the scope of interest was primarily external facing up until now," said Scott. "Having to do with our collaborations and business partners and those kinds of things. We have now also begun to look inward, and realized that we probably have as much opportunity internally as we do externally. For the first



© 2004 General Motors. All rights reserved.

(above) Hummer H2 Assembly Plant, Mishawaka, Indiana. (right) On the eve of the Auto China 2004 auto show, a Cadillac SRX is parked along Juyong Pass, a section of the Great Wall north of Beijing.

"In some cases we backed off and we said, 'you know what, it really doesn't make any sense,'" said Scott. "In other cases we said, 'this is really important and we're just going to have to live with your PIN number or some additional level of security associated with the transaction.' Out of a total of about a seven month process it probably took us five months to have those discussions. We were working on the technology part in parallel, but those [discussions] were the long running thread in the process."

The Larger Perspective

Even after having focused on digital identity for many years, GM found that



time we have launched a corporate wide identity management program, and it's just now getting started. It has moved out of specific areas that we were interested in, such as the [federated portal project], and is now a company wide global program for GM this year. The conclusion of all that is [that] you can't look at digital identity myopically, in just the external web space. It's got to be a part of a bigger, more overarching architecture and plan that you have for the corporation."

Identity is Moving Front and Center

"We at GM have always thought that digital identity was something that would move to this more strategic focus," said Scott. "But you sort of had to prove it and you had to make it real for people. There's been this conver-

gence in the last two years of the push from a technology side – yes we can do this now, and there's a spec and there's a standard and so on – [and] the pull from the compliance and regulatory side and the worms, viruses, and spam that are acting as complementary forces in terms of making digital identity strategic – maybe even sooner than I would have guessed. As you get viruses and worms and spam and all that sort of stuff you start to get a lot more concerned about who am I interacting with, are they somebody I can trust, and are they validated. This has become a much bigger issue. It's kind of like Y2K (without the deadline.) People are starting to realize that there's a fairly significant problem out there and it's going to take real work to go fix, over some period of time. It's not an overnight sort of deal."

GM's experiences show that the move to extended-enterprise federated identity is one that demonstrates that it is no longer possible to ignore the strategic nature of digital identity. Even though the step itself seems relatively small, it is the point at which a company's IT systems must start to integrate not only identity, data but identity strategy. GM's experiences also show that once this perspective starts to take hold, a company sees that the same steps required by federated identity will also work to significantly moderate other pain points such as regulatory compliance, viruses, spam, and worm propagation.

The Socratic method has survived all these years because when you start by asking the obvious questions assuming you don't know the answers it can be surprising what you learn. GM's mySocrates federation project shows that it still works. ■