

Identity and Web Services MIX AT OGILVY

Ogilvy & Mather is one of the most recognized names in advertising. But they had struggled to find a way to securely and rapidly move the large media files they use daily between offices in a way that fit their creative staff, planners, and support personnel's work methods. Then they hit on combining web services, identity, and email. It fit the company's work methods, reduced delivery time dramatically, reduced storage requirements, improved business productivity, while simultaneously reducing network loading and increasing security and accountability

The term "Madison Avenue" is synonymous with the advertising business. In 1948, David Ogilvy founded Ogilvy & Mather in New York, in an office on Madison Avenue. Ogilvy began its climb to prominence with the "Man in the Hathaway Shirt" campaign. That campaign – featuring a graying mustachioed gentleman in a starched white shirt and tie with a black eye patch – appealed to the reader's intelligence to raise the profile of the brand and ran for 25 years. David Ogilvy also began the elevation of the Rolls Royce brand with a campaign noting that "At 60 miles an hour the loudest noise in this new Rolls Royce comes from the electric clock." That campaign began building an image for Rolls Royce that made the name a synonym for extreme quality.

Today, Ogilvy & Mather Worldwide is one of the most recognized names in advertising. Ogilvy continues to produce memorable campaigns for its clients, who now include a majority of the companies in the Fortune 500.

Ogilvy has grown far beyond its Madison Avenue origins – to nearly 400 offices in 113 countries – and therein lay the origins of an IT problem. For while the company may not still be the intimate organization it once was, the act of creating and managing branding, advertising, and PR still is. To allow easy collaboration among a team of creative professionals with partners and clients ranging worldwide, Ogilvy needed a way to move extremely large media files rapidly and securely.

As far back as late 2001, Ogilvy started building custom web applications to allow authenticated access to their databases with a web browser. According to Andres Andreu, Technical Director of Web Engineering and Applications at Ogilvy, "We started writing [web applications] to meet some client needs to tap into sources of data and provide them some functionality in return. One of the distinct needs that came out of those [early] relationships was that we had to have these clients pump their data into our LDAP sources. So we were actually



“We never had a breach, but you can’t sleep at night the right way, when you know that there’s some points of exposure.”

storing their user data on our side so that they could use the applications that we host here at Ogilvy.”

The browser based applications, however, didn’t work out as had been hoped. “You start exposing some data, then it kind of grows,” said Andreu. “We found ourselves writing web based apps to facilitate these needs and I sat down one day and said ‘this is not efficient.’ It’s fine if you’re doing it for one client. But when the second, and the third, and the fourth start asking for the same thing, yet they all want it customized to their needs, that’s certainly not the right approach.”

Enter Web Services

Soon Ogilvy began to experiment with Web Services. “About three years ago is when we started going live with the Web Services,” said Andreu. “And we saw a great level of success with the Web Services. It was very exciting for us and for the clients as well. The integration points became so much more seamless than the old way. We started doing everything based on open source models of Web Services.”

Once they were familiar with web services, Ogilvy began to look into using them to handle their growing LDAP export/import issues. “We used the web services framework to abstract the access to our entire directory space,” said Andreu. “Prior to that, the other side of the world had to be in tune with our schema. Just the move to the Web Services simplified all that. It was a nice clean layer of abstraction between them and us.” They were still importing data into their LDAP directories, “but now it was transactional. So there was no bulk import once a week. The other challenge we had was

that the data that was coming into our directory was not always from another LDAP source. So we also abstracted a lot of that based on the services. Now somebody can send over a CSV file and we’ll parse through it and process the data accordingly. We bought ourselves a lot of flexibility, or loose coupling if you will, of the systems.”

Using web services had now allowed Ogilvy to create a transaction based directory system with an abstracted external interface, but it brought with it significant security risks. Because the only real security their web services had was that the end points and formats were not published – security through obscurity. “In the beginning we just kind of accepted the risk,” said Andreu. “We were doing Web Services over HTTPS, so there was no risk in the transmission part of it, but there was nothing on our end points to authenticate the source or the consumer.”

Moving Large Content

Throughout this period, the company’s Lotus Notes email system continued to be what the account executives, creative staff, and support personnel used most for communications. In 2003, Ogilvy decided to deploy an email file attachment management system from Accellion which would allow the easy interface of authenticated sending and receiving of extremely large email attachments. Combined with their web services applications this system could do the job of tracking and billing while making authenticated large file transfers interface easily into sending or receiving email.

Growing Risk

As usage of this new system ramped up, however, the security issues of the lack of

identity enabled web services became more clear. “We never had a breach,” said Andreu. “But you can’t sleep at night the right way, when you know that there’s some points of exposure. I distinctly remember going to our bosses here and showing them what could possibly happen if somebody ran across the URL endpoint for one of our services. I told them: one day, if somebody pumps 20,000 bogus objects into our directory, we don’t say ‘just clean them up.’ Once they realized that there was a distinct business impact, that clients could start losing trust in us, they were on board with the fact that it had to be fixed.”

Beyond XML Firewalls

But identity-enabling web services didn’t turn out to be so simple. “I looked at some traditional XML firewalls,” said Andreu. “And the market was substantially limited – from my perspective at least. There was certainly nothing out there that met all of my needs. We actually even toyed with the idea of writing one ourselves, [since] we are an engineering team. We built a couple of prototypes, and saw how complicated it would be. I don’t think anybody was willing to invest the money and time to build that type of integration. We all realized that this was going to be a big effort, [and] we needed something that was far more flexible.”

It was during this search for an answer that Andreu ran across the Layer 7 SecureSpan Gateway and identity bridge. They obtained the gateway for evaluation in a proof of concept test. “I can’t stand PowerPoint presentations,” said Andreu. “Give me the box, and let’s get down. So they came, put the box in, left us with all the information we needed, and they went back home. We wrote

PERL scripts to become the consumer, and we verified everything before we exposed it to anybody else. We did that on our internal services, and we hammered this box. I threw our security team at it, and we just hammered away. And it held up. It was amazing to me, because we haven't seen a clean Proof of Concept like that in awhile."

"Once we verified everything internally," said Andreu, "we got an external application and an external client involved for a prototype. We had scheduled three days worth of integration time between them and us, and we were done in less than a day. Usually three days means two weeks, right? It was great because we all sat there, half a day in, [saying] 'this looks like it's going to finish today.' We were running through proxies at first, watching all the packets go back and forth. We were sitting there going 'this is too good to be true.' But it was true, and it's been a success ever since."

"At the end of the three month [Proof of Concept test] I documented the entire set of results," said Andreu. "I went to my bosses, and gave them a presentation on the results of both the internal and external testing. There was concern in the beginning, because we typically don't deal with small companies." But with the success of the pilot and time spent looking into the vendor, Ogilvy was able to gain the confidence to commit to the product in a production setting.

True Identity-Enabled Web Services

Ogilvy has now rolled their identity-enabled web services out to seven client locations. In the process, the flexibility of using the identity-enabled gateways has shown its value. "If we look at a scenario where we have a client that's already using our services, and they're willing to take the client-side agent, it's literally a matter of minutes," said Andreu.

"Because the agent for the gateway communication takes care of everything else."

"One of the challenges we were facing, [however,] is that we are dealing with a myriad of clients on the other side of the world," said Andreu. "Some of them have very rigid infrastructures, you know, Fortune 500 companies. I certainly can't ask a company like that to drop an agent on their side, and expect those types of transmissions to start taking place."

"Once they realized that there was a distinct business impact, that clients could start losing trust in us, they were on board with the fact that it had to be fixed."

"That was an aspect of the flexibility [of the SecureSpan Gateway] that was key to me," said Andreu. "I had to deal with both aspects of the client world – the ones that played, and the ones that didn't play. Within the realm of the rigid companies, some already have, for instance, their own SAML assertion generating systems, and some have nothing. The Layer 7 product can pretty much accept SAML assertions from any other environment. Maybe a line or two of code on our side and we're good to go."

"The challenge for us is the companies that are rigid but not robust enough yet to have their own signing authorities, etc.," said Andreu. "For them we've done a quasi-PKI model. We have our own signing authority that we built on open source technology. We cut them a cert, and they implement it on their side on the systems that make the calls to us. As long as their actual SOAP calls have references back to that certificate

we accept them. It's not the highest level of security, but it's certainly not open to the world either."

Federation, Identity & Web Services

But the evolution towards federation standards such as SAML and WS-* is what Andreu expects to see over time. "The SecureSpan Gateway allows us to accept both," Andreu said. "That was another flexible factor for us. I had to accept both, I couldn't just say we're purely SAML. As a matter of fact, one of our biggest clients is not a SAML shop. They were part of the WS-Security movement, so I had to be very cognizant of that."

It's taken them some time to put it all together, but today, Ogilvy has developed a solid framework for identity enabling their web services and allowing flexibility in how clients can integrate with it for authentication and authorization. In addition, they are using web services through this framework to integrate their own LDAP identity data stores. "It's one of the things we're doing radically different now," said Andreu. "Let's say an application in India has a database, and we want to keep their database synchronized with our LDAP. There's no more batch processing scheduled. If there's an application that triggers a change in LDAP, that will trigger a SOAP client call out to the service in India and update their database. This is one of the ways we're using this whole framework. And that buys us the flexibility out at the edge."

"It's even given us an advantage on Sarbanes-Oxley Compliance," said Andreu. "Because with the web services it's transactional, [and] you're auditing each [identity] transaction one by one. So it's simplified that entire reporting process. In 2005, we're going to go pretty wide in scope." ■