

SSO at 3M. Our story so far.

Bob Brandt

Security and Directory Architect

3M



Agenda

- About 3M
- IT Design Philosophy / Industry Model
- SSO at 3M
- Federation at 3M
- Current Challenges

About 3M

3M , a Global, Diversified Technology Company

- 3M is fundamentally a science-based company.
- We produce thousands of imaginative products, and we're a leader in scores of markets – from health care and highway safety to office products and optical films for LCD displays.
- Our success begins with our ability to apply our technologies – often in combination – to an endless array of real-world customer needs.

Our Values

- Act with uncompromising honesty and integrity in everything we do.
- Satisfy our customers with innovative technology and superior quality, value and service.
- Provide our investors an attractive return through sustainable, global growth.
- Respect our social and physical environment around the world.
- Value and develop our employees' diverse talents, initiative and leadership.
- Earn the admiration of all those associated with 3M worldwide.



About 3M



- Has been around for 106 years
- Dow 30 and S&P 500 Stock
- Dividends paid every quarter since 1916
- 66% of sales from outside the US
- Around 25B in revenue
- 55,000+ products
- 45 core technologies
- A company of powerful leading brands

3M Periodic Table of Technologies

Technologies

Ab								Pm	Se
Ac	Bi						Nt	Po	Sm
Ad	Ce	Ec	Fi			Mi	Nw	Pp	Su
Am	Dd	Em	Fl	In	Md	Mo	Op	Pr	Vp
An	Di	Fc	Fs	Is	Me	Mr	Pd	Rr	We
As	Do	Fe	Im	Lm	Mf		Pe	Rp	Wo

http://solutions.3m.com/wps/portal/3M/en_US/3M-Technologies/Home/



Secure Documents example. Use specialty films and adhesives, RFID tags, nanotechnology, & microreplication



Missing retroreflective patterns are an immediate visual indicator of potential simulation attempts. Possibilities include the substitution of conventional laminates or over-laminating the surface to disguise changes or additions.

Any disruption to the laminate's surface, however, will signal tampering attempts. 3M Confirm Laminate is resistant to the most common attacks:

- Retroreflective patterns that are not aligned can indicate an attempted alteration.
- Retroreflective patterns that are blocked when verified with a light source can mean that data has been added to the surface of the laminate.
- Dark spots or washed out retroreflective patterns can indicate attempts to tamper with the document using solvents.

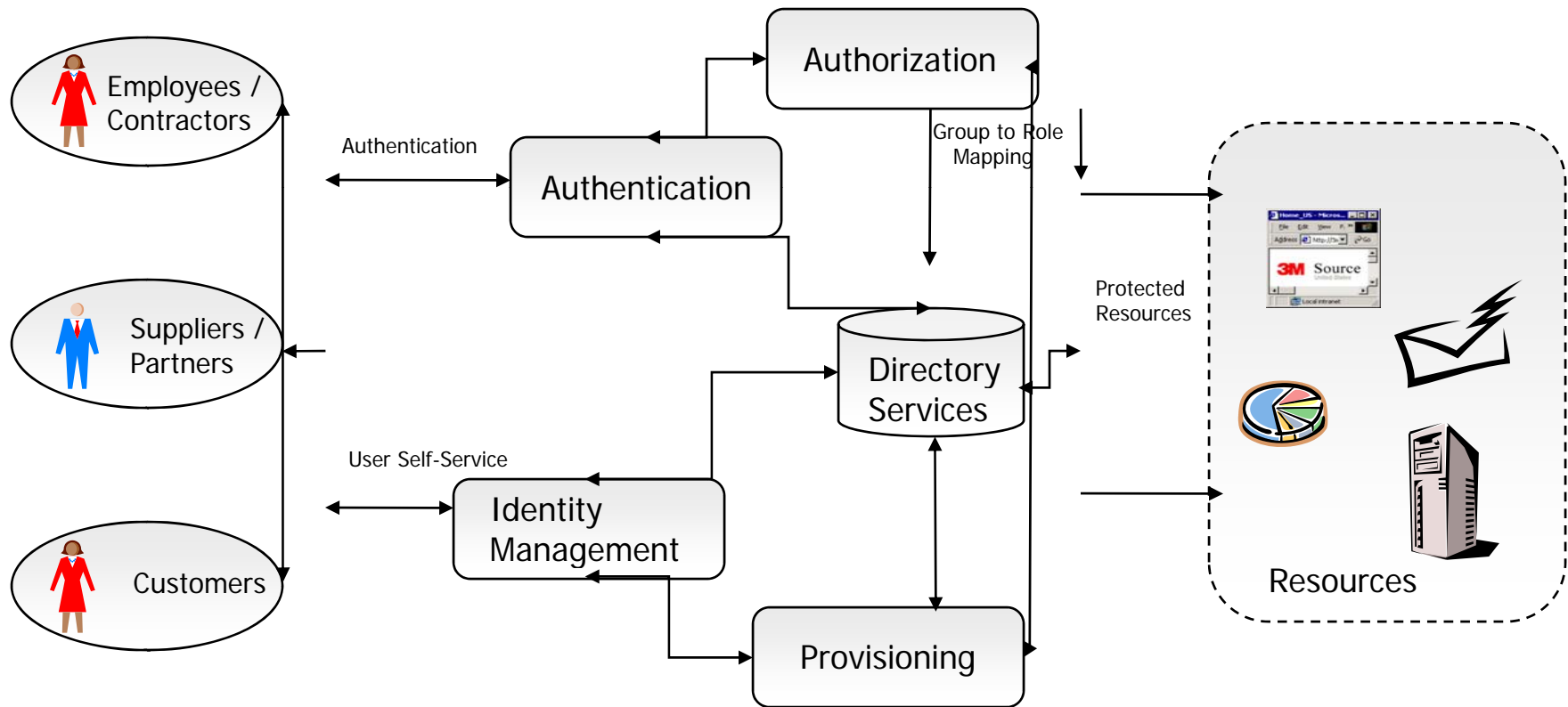
The proprietary technologies used in Confirm Laminates are the product of years of research in secure laboratories. Component materials are not commercially available, and the manufacturing expertise and equipment required to replicate the laminate make it extremely difficult for counterfeiters to pursue.



3M IT Design Philosophy

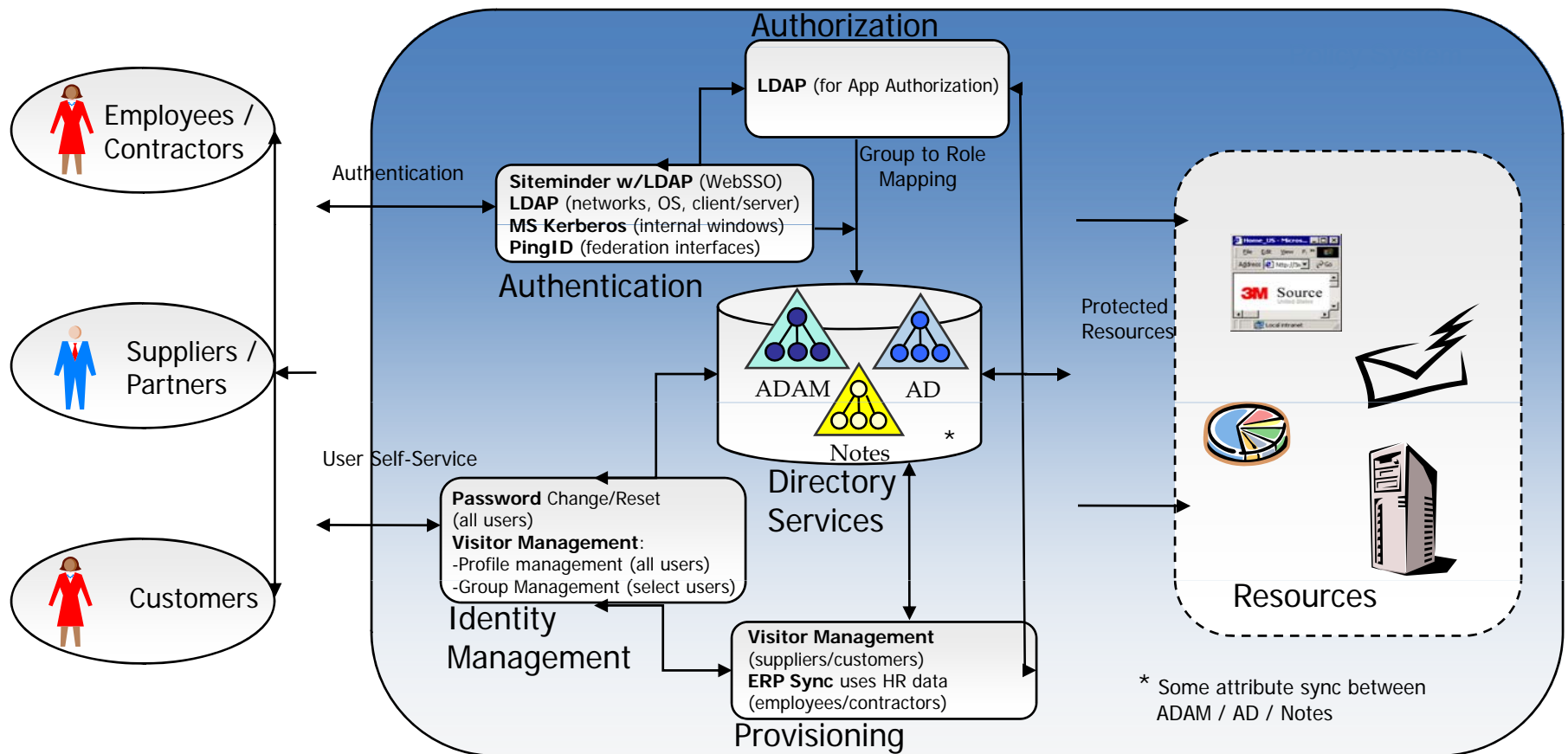
- Standards based wherever possible
- Component based
 - Stereo model. Interchangeable parts (vendors)
- Layered
 - Supports new features without breaking existing model, e.g. adding Strong AuthN does not break downstream security.
- Keep it Simple.
 - This isn't rocket science, no matter what you tell your boss.
- Collaborate with vendors and peers.
- Call your mother.

Industry Model – Cap Gemini Framework



Security Architecture Components

Industry Model – 3M Implementation



Runtime Deployment

SSO at 3M

- **5 years ago 3M...**
 - **Harvested our corporate DCE cell** along with many silos of **application specific logins.**
 - Moved to an enterprise LDAP approach based on Microsoft ADAM as the directory.
 - Overlaid CA Siteminder for Web SSO using ADAM LDAP as the backing user & group store.
- **Since then..**
 - 200+ Web apps working with SSO together including: J2EE, ERP, CRM, Portals, WIKIs and 3rd Party apps.
 - 50+ nonWeb classes of apps also handled with this design:
 - e.g. client/server, network (VPNs, iPass, Firewalls, wireless), OS (Windows/Linux), federation (~19), hw/sw/services.

SSO at 3M

- Today.. 95% of our users manage a single password in a single location.
 - Customers/Suppliers as native accounts in ADAM, with an extranet password policy.
 - Employees as AD accounts (using a bindproxy User class that ties ADAM to AD), and using a corporate SOX-controlled password policy.
- When we implemented:
 - A prevalent selling point for using Sync tools, and Virtual Directories, was to address the “too many passwords” problem.
 - With the approach we took we did not need password Sync tools or vDirs. (We convinced our vendor to ship a bindproxy instead).
 - Virtual Directories and Sync tools are still very interesting for many reasons, we just did not need them at the time we moved to this current design.

SSO at 3M

- **IT Benefits** of the current system

- Single LDAP DIT

- J2EE (Websphere, JBOSS, Weblogic), WIKIs, and Portal authorization references port easily across Test, QA, Production systems because LDAP DNs do not change.
- They typically would change with AD, on a common network, because of DNS linkage to AD names.

- Referralsless

- Works with least capable LDAP clients. nonMicrosoft LDAP clients (non ADSI) do not work well with Multi-domain forests.
- For multi-vendor shops it is important to work with lots of clients.

- Works with load balancers and wildcard SSL

- Works with Strong AuthN (e.g. OATH tokens)

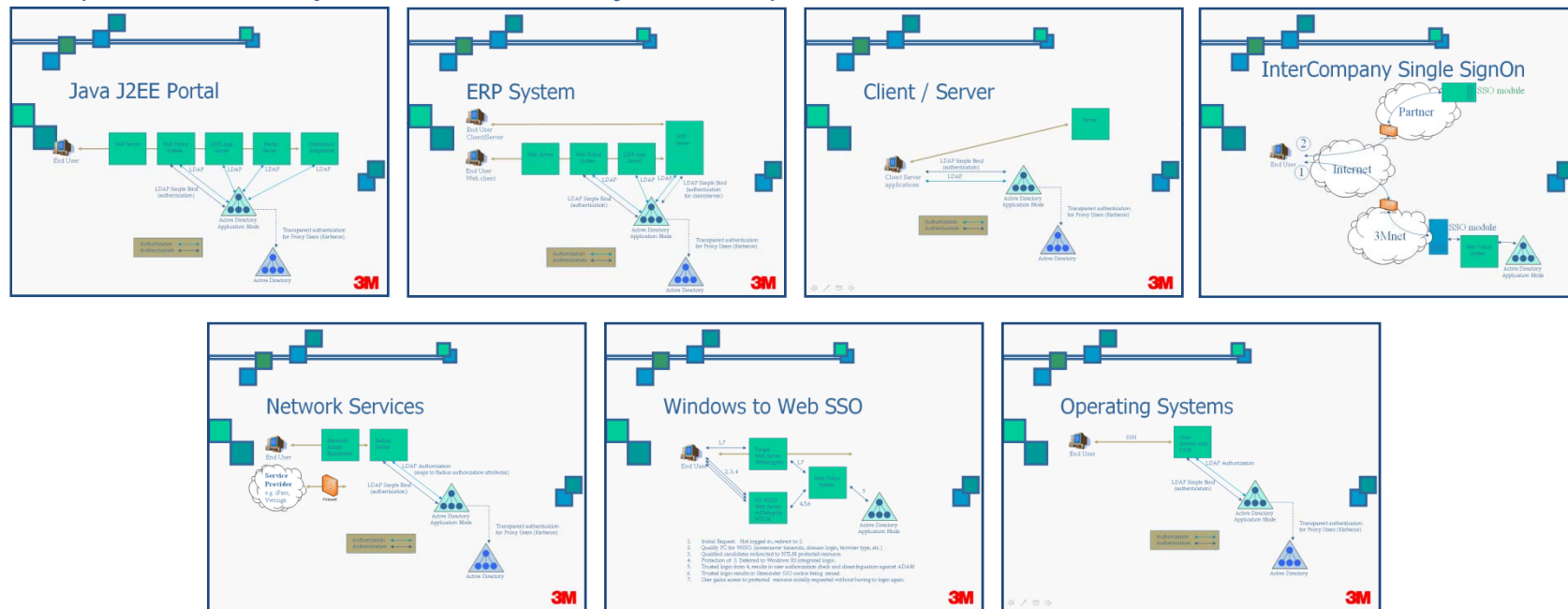
- Works cross domain (mmm.com, 3m.com, 3m.com.cn, ...)

SSO at 3M

- **Business Benefits of the current system:**
 - Reduced operations costs.
 - Web self-service and Single managed password have each reduced helpdesk calls.
 - SSO is in our DNA now, and rarely a discussion item anymore with business or applications people, even with external federations.
 - Improved employee productivity.
 - Proactively stated by employees
 - Delivering solutions more quickly
 - Web 2.0 Collaboration Center rolled out with out excessive efforts at 3M.
 - Helping address regulatory compliance
 - SOX, CFR Part 11, HIPPA, US Export, PCI

SSO at 3M

- What different apps/services looks like
(classes map to the Industry Model)



What our employees see

Illustrates multivendor SSO: Websphere, Sharepoint, WIKI, ERP, Conferencing, Federation, all through a common portal

The screenshot shows a Microsoft Internet Explorer browser window displaying the 3M Source Collaboration Center. The browser title is "Collaboration Center Home - Microsoft Internet Explorer provided by 3M/IE 6.0". The address bar shows the URL: http://3msource.mmm.com/wps/myportal/3M/en_US/Collaboration-Center/Collaboration-Center-Home/. The page features the 3M logo and "Source United States" branding. A search bar for "Search Workforce" and "Search Intranet" is present. A navigation menu includes "Home", "Work Center", "Life & Career", "Supervisor e-HR", "Collaboration" (highlighted), and "About 3M". The user is logged in as "Robert Brandt" with "Log Out" and "Preferences" links. The main content area is titled "3M Source Collaboration Center" and includes a welcome message, a breadcrumb trail, and a list of services: Team Places, Meetings, Social Networking, Collective Knowledge, Personal Productivity, and Content Services. A sidebar on the left lists navigation options like "Collaboration Center Home", "About 3M Source", and "Tool Finder". The right sidebar contains "In The News...", "Quick Links", and "Tool Finder" sections.

Collaboration Center Home - Microsoft Internet Explorer provided by 3M/IE 6.0

Address: http://3msource.mmm.com/wps/myportal/3M/en_US/Collaboration-Center/Collaboration-Center-Home/

3M Source
United States

Search Workforce: Last Name First Name >> [Advanced](#)

Search Intranet: >>

Home Work Center Life & Career Supervisor e-HR **Collaboration** About 3M

Robert Brandt
[Log Out](#) | [Preferences](#)

Collaboration Center > Collaboration Center > Collaboration Center Home

3M Source Collaboration Center

Welcome! The 3M Source Collaboration Center brings into one location a new generation of web tools for 3M's businesses. It provides web platforms to facilitate collaboration and information sharing by individuals and teams around the globe.

Attention: Be sure to read [3M Information and Security Policies](#).

Collaboration Center

- Collaboration Center Home
- About 3M Source
- Collaboration Center
- Tool Finder
- Glossary
- In the News...
- Contact Us
- 3M Information and Security Policies
- Team Places
- Collective Knowledge
- Meeting Center
- Personal Productivity
- Social Networking
- Content Services

Team Places

- [Sharepoint](#)
- [Teamroom](#)
- [Quickplace](#)

Meetings

- [Global Crossing Web](#)
- [Sametime Web](#)
- [Sametime Instant](#)
- [Video Conferencing](#)
- [Audio Conferencing](#)

Social Networking

Collective Knowledge

- [Wiki Enterprise \(WE\)](#)
- [Maven](#)

Personal Productivity

- [Lotus Notes](#)
- [Mobile Devices](#)
- [Mobile Software](#)

Content Services

- [RSS](#)
- [3M TV WebStream](#)

In The News...

- > [Wiki Enterprise \(WE\) Available Worldwide - June 2008](#)
- > [3M Launches Online Collaboration Center](#)
- > [R&D - D&G Qtrly Communications](#)

[More...](#)

Quick Links

- > [Glossary](#)
- > [About 3M Source Collaboration Center](#) provides overview information, benefits, best practices
- > [Contact Us](#)
- > [3M Security Policies](#)
- > [SharePoint: Tips and Tricks](#)
- > [SharePoint: General Discussion](#)
Collaborate with fellow 3Mers on SharePoint

Tool Finder

Not sure what to use? Access our tool finder here!

Federation at 3M

- Federation is just another class of application that maps to the model.
- We Federate with partners using:
 - Partner Standards. 4 integrations
 - “3M Standard” mechanism. ~10 integrations
 - Industry Standards. 5 integrations in production w/ others pending.
 - Sales CRM, eRecruiting, eLearning, eFullfillment, ...
- For standards we are using Ping Federate v5.1:
 - We act as an IDP currently, with offer to our businesses to offer SP services.
 - We integrate with PingID’s Siteminder token support.
 - We are using SAML 1.1, SAML 2.0, Artifact and Bind.
 - We’ve done some testing of PingID’s STS with our developers.
 - We now spec SAML in RFI/E reviews with all existing and new partners, with a goal of moving everyone to standards when reasonable.

Federation at 3M

- **GOOD NEWS.** Most outsourcers we talk to now appear to know about SAML.
 - This was NOT the case a year ago.
- This means SAML will probably be very prevalent a year from now, i.e. is becoming part of outsourced application offerings.

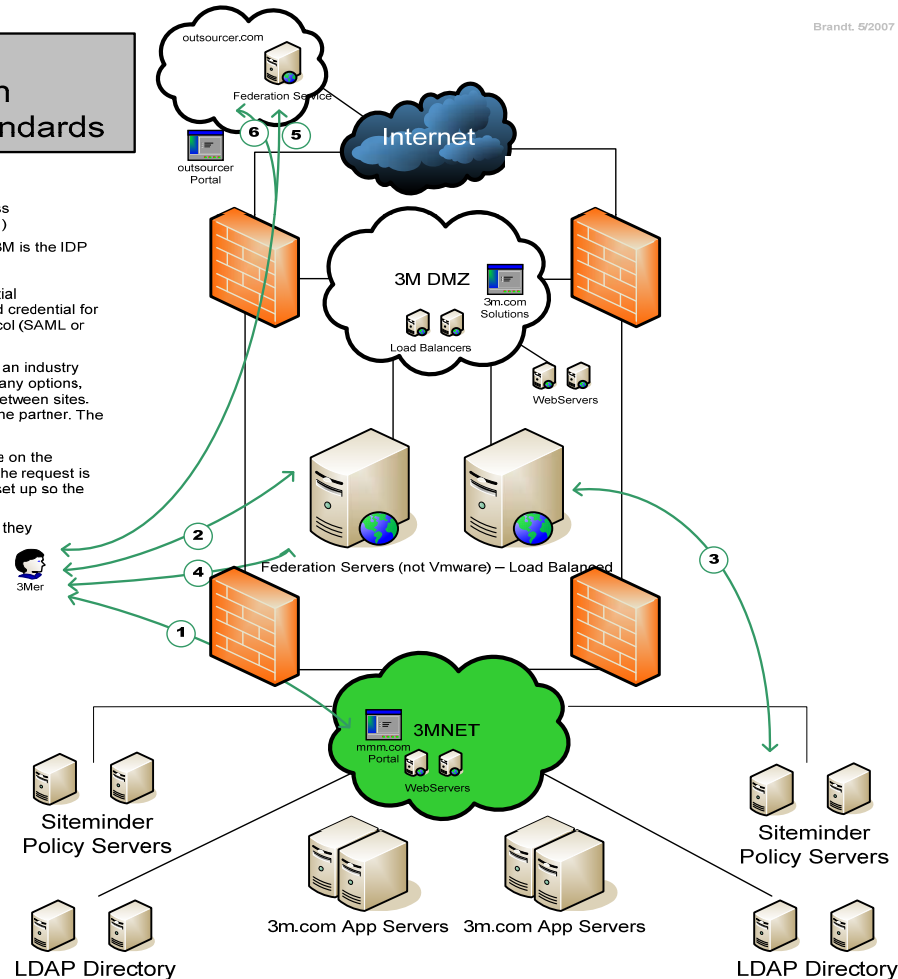
Federation at 3M

- What it looks like:

Example
Cross Company Single SignOn
with SOAP based Industry Standards

Federation - Outbound

- 1 Logged in 3Mer clicks link in mmm.com employee portal to access services at an outsourcer (401k, health, stock purchase plan, etc.)
- 2 3Mer gets directed to industry federation service hosted at 3M. 3M is the IDP (Identity Provider) in this scenario.
- 3 3M Federation server takes user's proprietary Siteminder credential (SMSESSION cookie), validates user, builds an industry standard credential for the user, and redirects the user using an industry standard protocol (SAML or WS-Fed) to the outsourced site.
- 4 Federation Server, redirects user browser to Customer site using an industry standard token and protocol (SAML or WS-Fed). Note: There many options, including web services (SOA) based ones, for passing the user between sites. The approach used depends upon the capability/preferences of the partner. The example shown is not atypical.
- 5 User arrives at customer federation service. 3M's digital signature on the request is verified. If DS is verified, the asserted user identity in the request is Mapped to an identity at the outsource and an SSO credential is set up so the user does not need to login.
- 6 User is redirected to the web application that provides the service they requested.

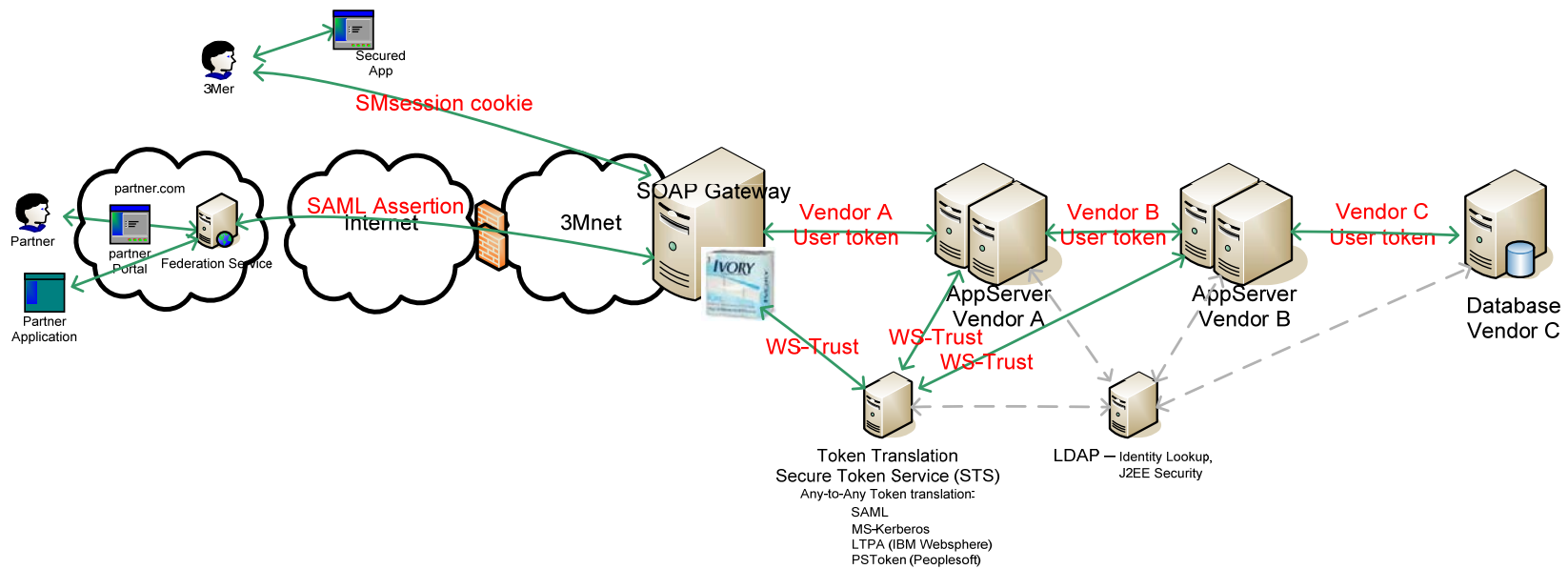


Current Challenges

- SOA Web Services
 - SOAP hardware firewall, or not.
 - Where/how to do token translation (SOAP firewall, app servers, standalone STS)?
 - Token Support, custom and standard tokens.
 - Most of this is likely to occur quickly only via a combination of vendor influence and platform upgrades.
 - Oracle, Psoft, JDEdwards, Websphere, Microsoft, SAP, WebMethods, Siebel, JBOSS ideally all need to be addressed.
 - Addressing discovery (UDDI) and Management legs of SOA.
 - Securing cross-company apps. Parts at 3M, parts running elsewhere.
- 3M as SP
 - How to best automate provisioning (SPML?)
- Database Tier SSO Security
 - Big pain point. Standard Token support not prevalent with database vendors.

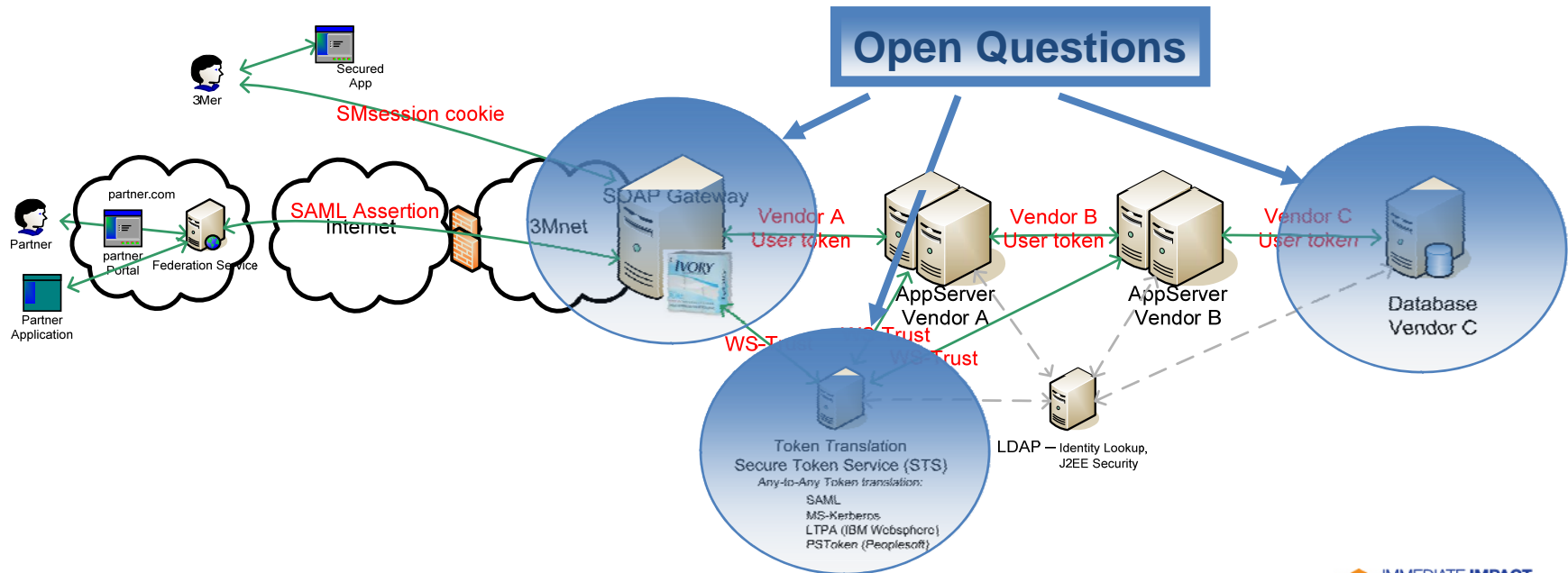
Current Challenges

Example
Browser Driven Web Service (multiple application tiers)



Current Challenges

Example
Browser Driven Web Service (multiple application tiers)



Can we solve this multi-vendor/company/platform security problem?

Thank You !