SSO Case Study:

The USPS Gives SSO Its Stamp of Approval

Wayne Grimes,
Manager, Customer Care Operations, USPS

May 10, 2005

Today's topics

- **An overview of the USPS**
- **USPS SSO efforts**
- **Lessons we learned along the way**
  - **Technical**
  - **Organizational**
  - **Implementation**

Secrets to a successful SSO project?

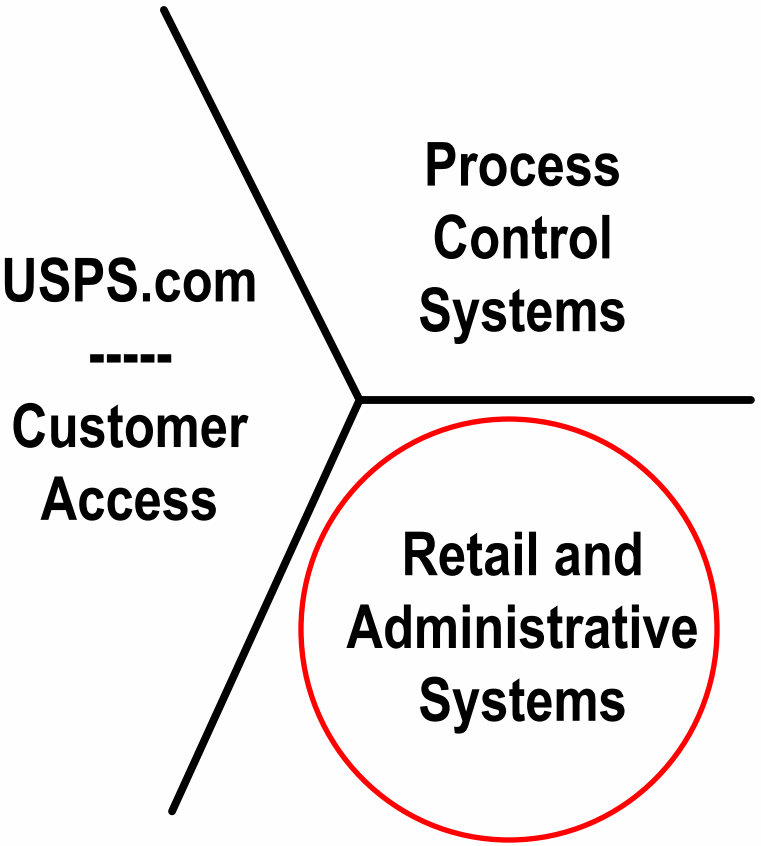
- **First rule – Get someone else to do it!**
- **Things to remember if you fail at rule #1**
  - **There is no silver bullet for a complex enterprise – You'll need more than one tool in your SSO tool chest**
  - **Pay attention to organizational issues – They can kill the project**
  - **Tune your solutions and processes to fit your organizational culture**

USPS – An overview

Business

- **Annual revenue – $69 billion**
- **Career employees – 700,000**
- **Mail volume – 206 billion pieces per year**
- **Delivery points – 142 million per day growing by 1.8 million per year**
- **Retail outlets – Serve 7 million customers a day via 37,000 outlets**
- **Vehicle fleet – over 208,000**

Technical Divisions



USPS retail and administrative systems

- **People – 150,000 admin and 70,000 retail**
- **Devices – 140,000 admin wkst and 43,000 retail terminals**
- **Mainframe – 96,000 user accounts**
- **Infrastructure – based on Active Directory (AD) and Windows**
- **Business apps – 600 plus**
- **Client software – Web, Win32, terminal emulators, client side Java, etc.**
- **Server platforms – Windows, Solaris, mainframe, etc.**
- **Applications – COTS, Oracle, Websphere, ColdFusion, etc.**
- **Authorization management – eAccess (Home grown)**

USPS internal environment (cont.)

- **eAccess – Requesting access to our systems**
  - **A home grown Identity Management System to manage user system access requests and approval workflow**
- **User identity**
  - **Hundreds of applications that maintain their own specific User IDs with no common user naming standard**
  - **No easy way to align all of the accounts that belong to a given individual**

SSO business drivers

- **Administration for 150,000 users averaging 10 IDs and passwords**
- **Over 100,000 password reset calls per year**
- **No way to disable all of a users accounts**
- **User were unhappy with the situation**
- **Problem was getting worse, not better**
- **Security issues with passwords on paper**

Our original charter and limits

- **Original Charter – Single Sign On (SSO)**
  - **Build transparent logons based on the Windows credentials**
  - **Improve the end user experience – make their lives better**
  - **Reduce administrative and help desk costs**
- **Focus on authentication not authorization**
- **Maintain eAccess to request and grant system access privileges**
- **No internal portal**
  - **No single point of failure**
  - **Applications were building e-mail enabled interfaces to their applications that required direct application access**

Early research identified six application methods

Solutions we use

- **Logon ID and password management – (Application changes not needed)**
- **Native integration with MS protocols**
- **LDAP based "Single Log On" (SLO) – (User challenged for their AD ID and password)**
- **AD integration via MIT Kerberos**

Solutions we don't use

- **CA/PKI based integration – Key management, cost and workstation integration problems**
- **Application integration middleware – No internal portal, no desire to delegate administration, and application integration problems**

Bad news we learned early on

- **We had a very complicated legacy application environment**
- **Industry provides very limited interoperability and standards**
- **Product vendors don't help much**
  - **Strong bias for proprietary APIs and hooks**
  - **Staff not trained in the standards based features of their products**
- **Weak IT consulting support for standards based integration solutions**
  - **Staff is trained in one or two proprietary solutions**
  - **'Joint Marketing Agreements' with product vendors**
- **We as customers haven't demanded interoperability**

Our SSO charter today

- **Evolved charter – SSO & Single Log On (SLO)**
  - **All application user authentication, both transparent and interactive, must be tied to the users Active Directory ID and password**
  - **Improve the end user experience – make their lives better**
  - **Improve security by improving our ability to disable a user access to our systems**
  - **Reduce administrative and help desk costs**
  - **Its ok to challenge the user for their AD ID and password (SLO)**
  - **Good enough is good enough**

USPS progress so far

- **Over 75,000 users use v-GO to manage their IDs and passwords into hundreds and hundreds of applications**
- **We've converted over 50 applications to full AD integration via SSO or SLO**
- **Developed templates that can be used for developing new SSO apps**
- **Virtually all of our application access requests are managed via eAccess**
- **We've automated the process of account creation and management in AD and our high profile applications**
- **We've pushed many of our password reset calls off of the help desk to an automated password reset system**

Technology problems with SSO

- **Most non-Microsoft applications can't use native MS credentials**
  - **SPNEGO (Simple and Protected GSS-API Negotiation) tools can do the job**
- **The valves are there but the plumbing is missing**
  - **Many applications advertise a Kerberos interface**
  - **Few tools to read credentials from the desktop and pass them through the browser to the website and application**
- **Moving credentials to the web site isn't enough**
  - **Credentials must be passed to the application server**

User and application owner objections

- **End user resistance**
  - **Many users don't think Single Sign On is secure**
  - **They also don't trust programs that remember and submit their IDs and passwords**
- **But I'm special…**
  - **Many application sponsors don't understand or trust SSO**
  - **Some applications may be to sensitive for SSO**
  - **SLO solutions are often a good compromise for applications with a high level of business or personal sensitivity**

Users don't do what we think they do

- **Users often 'loan' application IDs and passwords as a way of sharing or delegating work**
- **High profile users are often involved in this behavior**
- **SSO or SLO means they can't share just one password anymore**
- **Applications may need to be modified to allow delegated authority from within the application**

People who are paid to stay on there feet

- **Our design was on the users Windows/AD logon**
- **The design works for people who stay in a chair**
- **The logon/logoff process is to slow for people who work on their feet (KIOSK)**
- **This problem is very real in the medical community**
- **The Health Insurance Portability and Accountability Act (HIPPA) helped to forced the issue**
- **Look at a vendors HIPPA compliant tools for solutions**

Matching directory accounts to application accounts

- **A user's ID often varies from system to system**
- **These IDs must be matched to the users directory identity as the application is converted to SSO**
- **Applications must have a conversion routine that asks users to supply both their old application ID and password and their directory based ID and password**
- **Once validated, the application can convert its old ID or maintain a crosswalk table**

Building an SSO project team

- **SSO infrastructure engineering team**
  - **Builds shared SSO components**
  - **Develops and publishes SSO integration templates for specific application environments**
  - **Provides technical support to application development teams**
- **Line of business sponsor**
  - **Funds the conversion work**
  - **Commissions the application development team to do the conversion work**
- **Application development team(s)**
  - **Take the lead role in building a solution for their application(s)**

Building an SSO project team (cont.)

- **Senior management**
  - **Promotes the goal of a SSO enabled enterprise**
  - **Reviews and rewards progress**
- **Internal marketing team**
  - **Promotes the idea of SSO to line of business managers and development organizations**
  - **Help line of business managers promote and explain SSO to the end user community**

Other implementation issues

- **Don't promise until you can deliver**
  - **Develop the SSO infrastructure before you approach line of business managers – It may take longer than you think**
- **Pick the right systems to convert first**
  - **Driven by the technology solutions you have ready**
  - **High profile systems with lots of users build buzz**
  - **A few big successes are better than a lot of little successes – or failures**
- **Keep your users informed and trained**

Audience Response

- **Questions**