MAGNet VPN Infrastructure Upgrade

June 28th, 2013
AGENDA

• 1. Team Introductions
• 2. What Is New?
• 3. Juniper SSL VPN- What has changed?
• 4. Universal Identity Service Overview
• 5. What to Expect During the Migration
  – Verizon’s Role
  – ITD’s Role
  – Agency Role
• 6. Ongoing Operations
• 7. Project Approach
• 8. Wrap Up
October 25, 2000

Verizon Captures Massachusetts VPN Contract

By Steve Towns
Government Technology Reseller (On-Line)

Oct 25, 2000 -- BOSTON -- Massachusetts awarded a three-year contract on Tuesday to Verizon Communications to provide virtual private network services for remote state workers and businesses that sell to the commonwealth, according to Verizon.

The new VPN services -- which are expected to reach 10,000 users this year -- will deliver key elements of the commonwealth’s electronic government strategy, according to Massachusetts CIO David Lewis. “We’ll improve our collaboration with business partners, increase access to state resources and give our mobile workers the tools they need -- all to better serve the public.”

Verizon says the VPN will provide remote access to databases for state employees who frequently work from field locations, offer site-to-site connections between agencies and businesses that need to exchange information, and link businesses such as insurance agents to appropriate government databases. Users may access the system via 56 Kbps dial-up service, ISDN or DSL.

Agencies and businesses will use their existing telecommunications services to gain access to the network. Cost for the minimum service configuration will range from $10 to $30 per month, Verizon says. More information is online at http://www.verizon.com.
What is Changing?

- Juniper High Availability MAG 6611s replaced End of Life Sonic Wall
- New VPN Mobile Client
- Good Bye Digital Certificates, Good Bye Hard Tokens! Hello OTP!
- New ITD Administrative Portal & New User Profile Management Portal
- New Ethernet Internet Access & New More Cost Effective Site to Site Design
- New UIS help desk for soft token and password issues
- Introducing Local Program Office Support
What Remains the Same?

• Client Based SSL Service

• Infrastructure Designed to Provide High Availability

• Ability to Access MAGNet from any Internet Accessible Device in a Secure Manner

• Remote Access Help Desk Support

• Gateway Groups, Configurations- will remain “As Is” during the migration

• ITD support role
New Environment
Proposed Design for MAGNet VPN
Site to Site IPSec Partner Connections

Public Internet

Business Partner Sites (Future)
Verizon Provided Managed Router

Business Partner Sites (ACS)
Verizon Provided Managed Router

Business Partner Sites (Perot Systems)
Verizon Provided Managed Router

IPSec Tunnels

Boston Data Center

MAGNet

SSL HA Gateway

ITD Provided Firewall (existing)

ITD Provided Switch (existing)

Business Partner Sites
(Perot Systems)
Verizon Provided Managed Router

Business Partner DNZ Site to Site IPSec
Verizon Provided Ethernet NID

Business Partner DNZ Site to Site IPSec
Verizon Provided Ethernet NID

Business Partner DNZ Site to Site IPSec
Verizon Provided Ethernet NID

Business Partner DNZ Site to Site IPSec
Verizon Provided Ethernet NID

ITD Provided Switch (existing)

ITD Provided Firewall (existing)

Business Partner Sites (Future)
Verizon Provided Managed Router

Each Partner Rents a small Cisco or Juniper Router at Chelsea Data Center (or at both Chelsea and Boston) and at each remote location. The IPSec Tunnels are terminated at the data center in the individual partner router.

Prepared by Rich Chiuve
06/05/2013
Juniper High Availability SSL VPN

Jayson McIvor and Vadim Starikov
Megapath
Architectural Design

- **User Accessibility**
  - **Current:** Two URL structure for end users (Boston and Chelsea)
  - **Planned:** Single dynamic URL which bases CPE traffic on load
  - **Benefit:** Simplified access and business continuity

- **User Authentication**
  - **Current:** User Management via Certificates and small Token base for 3rd party
  - **Planned:** High multi-phase authentication via UIS
  - **Benefit:** Stronger and More Flexible User authentication

- **SSL VPN Platform Environment**
  - **Current:** Complex Solution – F5 Load Balancers, Switches, LDAP servers
  - **Planned:** Simplified Solution – HA Design to scale to 10k users. No dedicated switches or LDAP servers.
  - **Benefit:** Robust Platform, Easily scalable
Improved Technology Functions

- Juniper SSL Appliance
  - Integrated with Verizon Business User Identity Service (UIS) using SAML
  - Dynamic access to resources (web, files, client/server) based on user group profiles.
  - Installer Service for agent deployment to restricted users
  - End user machine level checking and remediation support
  - Display End User Licensing Agreement (EULA) and Message of the Day (MOTD) notification support
  - Improved troubleshooting tools for client and server
Access Agents

- **Core / Browser Based Access**
  - Dynamic Portal (based on Access Policy) provide access to
    - Pre-defined web-application bookmarks
    - Network File Shares (Web-based network file explorer)
    - Telnet/SSH (Web-based terminal session emulation)
    - Terminal Services (Windows Terminal Services and Citrix)
  - Launching Mechanism for client based agents (below)

- **JunOS Pulse**
  - Network Layer Tunnel via Virtual Adapter
  - Session-based IP Assignment
  - TCP and UDP-based Client/Server Application Access
  - Supports Server-initiated Applications such as VoIP, X-Windows, NetMeeting
  - Provisioned via stand-alone installer service or installed via Web Access (requires admin rights)
Mobile Access

- **JunOS Pulse Mobile (downloaded from Mobile App Store)**
  - TCP-based Mobile Client/Server Application access
  - Windows Mobile Support:
    - Apple iOS Support
    - Android Support

- **Web Access Support**
  - Mobile-friendly SSL VPN Login Pages:
    - Pre-defined HTML pages customized for mobile devices, including Apple iPhones and iPad, Google Android, and Windows Mobile devices.
  - Supports Web & File Browsing
### Identity Management: A Business and Security Challenge

#### Market Driven By Fear
- FTC estimates identity theft leads to $50 billion in unnecessary costs to businesses each year; 10 mil US consumers affected each year\(^1\)
- Gallup poll: 66% consumers more concerned with ID theft vs. terrorism\(^2\)
- Verizon Data Breach Investigations: 900 million compromised records

#### Enterprises Move to the Cloud
- Services are leaving the company
- People are working outside the company
- Companies granting access to everyone (partners, associates, government, customers)

#### Regulations are Changing
- DEA and HIPAA
- ePrescribing of controlled substances requires strong assurance ID
- Financial services requesting stronger ID assurance
- PCI
- Required Digital Signatures

#### National Identity Assurance
- More governments are investigating national identities for their citizens
- Privacy and security are top concerns

---

How can identity and authentication be simple, less risky, and cost efficient?

---

Identity Reality today

People/Patients

Provider Applications and Gateways

<table>
<thead>
<tr>
<th>Service</th>
<th>Domain</th>
<th>Authenticator/Mechanism</th>
</tr>
</thead>
<tbody>
<tr>
<td>Gmail/MSGT Mail</td>
<td>Email address</td>
<td>Password</td>
</tr>
<tr>
<td>Bank Account</td>
<td>Account number</td>
<td>Password (Shared Secret)</td>
</tr>
<tr>
<td>AT&amp;T</td>
<td>Account number</td>
<td>Password (Shared Secret)</td>
</tr>
<tr>
<td>Brokerage</td>
<td>Account number</td>
<td>Password (Shared Secret)</td>
</tr>
<tr>
<td>Cell phone</td>
<td>Email address</td>
<td>Password (Shared Secret)</td>
</tr>
<tr>
<td>Phone Insurance</td>
<td>Account number</td>
<td>Password (Shared Secret)</td>
</tr>
<tr>
<td>Email/Cable and Phone</td>
<td>Email address</td>
<td>Password (Shared Secret)</td>
</tr>
<tr>
<td>Facebook</td>
<td>Email address</td>
<td>Password (Shared Secret)</td>
</tr>
<tr>
<td>Twitter</td>
<td>Email address</td>
<td>Password (Shared Secret)</td>
</tr>
<tr>
<td>MyXoom</td>
<td>Account number</td>
<td>Password (Shared Secret)</td>
</tr>
<tr>
<td>LinkedIn</td>
<td>Email address</td>
<td>Password (Shared Secret)</td>
</tr>
<tr>
<td>Enroll</td>
<td>Email address</td>
<td>Password (Shared Secret)</td>
</tr>
<tr>
<td>PayPal</td>
<td>Email address</td>
<td>Password (Shared Secret)</td>
</tr>
<tr>
<td>Continental</td>
<td>Account number</td>
<td>Password (Shared Secret)</td>
</tr>
<tr>
<td>AXA/XOM</td>
<td>Email address</td>
<td>Password (Shared Secret)</td>
</tr>
<tr>
<td>Work Portal</td>
<td>UserID</td>
<td>Password (Taken)</td>
</tr>
<tr>
<td>Work email</td>
<td>UserID</td>
<td>Password (Taken)</td>
</tr>
<tr>
<td>Work Partner Portal</td>
<td>UserID</td>
<td>Password (Taken)</td>
</tr>
<tr>
<td>Workday</td>
<td>UserID</td>
<td>Password (Taken)</td>
</tr>
</tbody>
</table>

- Too many passwords
- Too much complexity
- Too much risk
- Simply too hard
- Identity fraud

- Highly complex
- Expensive
- Too much risk
- Not enough flexibility
- No scalability

Success Requires Addressing Both Sides
The Evolution of Identity Management

Identity Management Growth Path

Simple Usernames and Passwords
- Provides no identity assurance or control and can be easily hacked

Hardware Tokens
- Provides better assurance, but is expensive and not flexible or user friendly

Identity-as-a-Service and Bring Your Own Device
- Provides an efficient and cost effective approach to enforce security policies
UIS Portfolio of Services

ID Proofing:
- Enterprise Antecedent
- 3rd Party Antecedent
- Trusted Agent
- Dispatched Notary
- Self Service Notary
- Self Asserted Attributes
- Verified Attributes

Registration/Enrollment:
- Self-service
- CSV File Bulk Upload
- External Authentication
- Completely customizable

Identity Broker:
- Complete Sun OpenAM
- Risk Engine
- Mobile Services Gateway
- SAML 1.x-2.0
- LDAP
- Active Directory®

Profile Manager:
- Web management interface
- Read/Write – customizable
- Upgrade Identity Proofing
- Register new form factors

Digital Signature Services

Form Factors:
- User Identifier
- Password
- PIN
- Email OTP
- SMS OTP
- IVR OTP/ack
- SW OATH
- HW OATH
- SAFE Roaming (ZFR)
- IP Malice
- IP Geolocation
- And Growing

Mobile Application & ID Message Center
Universal Identity Services (UIS)
Purpose-built for Government Agencies

Built to Federal Standards to Meet FISMA Moderate Requirements
including meeting all 18 security control families and each individual security control

Platform is Housed in Hardened Data Centers
that exceed physical and environmental controls of FISMA high, and protected 24X7 by armed guards in hardened enclaves that are under continuous surveillance

Same Standards as Verizon’s Most Sensitive Government Customers
and is monitored using the strictest Government processes and procedures

Follows Best-Practice Risk Management Methodologies
that identify sensitive information and users with elevated access privileges

Protected by Verizon’s Government Network Operations and Security Operations Center
that is FISMA high, providing security management, real time security event correlation and in-depth analysis of the UIS environment
UIS is ICAM-certified under the Kantara Trust Framework as an identity provider for LOA 1, 2 and 3 credentials

### FAST FACTS ABOUT ICAM

- ICAM (Identity, Credential and Access Management) was established by the Federal CIO
- Chaired by GSA and DoD, ICAM's task is to align the IAM activities of Government agencies
- Is a key enabler for the National Strategy for Trusted Identities in Cyberspace (NSTIC)
- Supports E-Government activities by leveraging industry-based credentials
- Seeks to enable trust in online transactions through common IAM policies and approaches
- Aligns Federal agencies around common IAM practices
- Reduces the IAM burden for individual agencies by fostering a common approach
Demonstration of User Self Registration
End-User E-Mail and Registration Workflow
Reduce risks and address compliance by ensuring that only the right people have access to the right resources.
Problem: How do we ensure users are who they say they are?
Solution: High assurance identity verification

Product
• Universal Identity Services

Capabilities
• Enterprises can bulk upload
• Online Identity verification
• NIST Level of Assurance 1-3
• Options for in person vetting
CoMA CSV generated spreadsheet used for bulk uploading candidate users to UIS.

Example Bulk Upload Below

| A   | B       | C       | D       | E       | F       | G       | H       | I       | J       | K       | L       | M       | N       | O       | P       | Q       | R       | S       | T       | U       | V       | W       |
|-----|---------|---------|---------|---------|---------|---------|---------|---------|---------|---------|---------|---------|---------|---------|---------|---------|---------|---------|---------|---------|---------|---------|---------|---------|

Please Note

- Existing users will continue to maintain their current VPN Username
- E-Mail address, First Name and Last Name are mandatory fields
- Enterprise Security Policy States that every VPN account must be unique
Post Bulk Upload, End Users will receive an enrollment E-mail containing a URL link that will take them through the UIS registration process.

**Example E-mail Below**

UIS_INT: Your UIS account is ready for activation

test@icsl.net

Jun 7 (13 days ago)

Mass.Gov

Your Universal Identity Services (UIS) account is ready for activation to be used for Commonwealth of Massachusetts.

Please click [here](#) to complete the registration process to activate your account.

Please contact your support if you have any questions.
The Contact Information setup screen will allow users to create their initial contract information.

**Example Contact Info Setup Below**
Users must create a compliant password, based on password rules, and create a PIN used for profile management and to enable certain Mobile App functions. **Example User Password and Pin setup Below**
The Knowledge Based Security questions are required for Forgot Password or Helpdesk functions when users call.

**Example Security Questions Setup Below**
This screen allows the user to verify the contact information entered so far and prepares for the next step to **bind the users profile to a credential**

**Example Verification of User Profile Below**
Verizon Universal Identity Services
End-User Registration – Credential

Problem: How can we simplify credential issuance?
Solution: Online, self-service credential provisioning service

Credential

Product
• Universal Identity Services

Capabilities
• Credentials can be quickly, easily issued to a variety of form factors
• Employees, customer, partners
• Mass scale end-user credentialing
• Cloud-based – no CPE
Assigning of Initial Credential – i.e. Form Factors

- Form factors are devices or methods used to bind a User to a Credential
- I.E. – Soft Token, Smart App, Text Message, Any phone, Your voice, etc.

Windows Desktop
- Soft Token

Mobile Phone
- Tablet OATH OTP Application

SMS Text Messaging

IVR callback
- All Phone Types
This screen shows the initial step of binding the user profile to a credential by utilizing a form-factor associated with the user.

**Example of Credential Binding to E-Mail Below**
This screen details the step required for confirming the credential binding to the user. User enters one-time password (OTP) that went to E-Mail

**Example of Credential Binding Confirmation Below**

![Contact Device Verification](image-url)

- **A password has been sent to your Email - [redacted].**
- If you do not have your contact device with you, you can click the Close button below and come back to this screen at a later time.
- Please type in the 6-digit password sent to you, in the password box below, and click Verify.

Password: [Redacted]  Time Left: 4:57
Here the check mark shows the users that their profile has been bound to the users E-Mail address. E-mail used to get OTP

**Example of Credential Bound to Profile Below**
Screen indicates the completion of UIS End-User Registration and provides a summary of information entered by the user.

**Example of Registration Completion Below**

![Example of Registration Completion](image_url)
An E-Mail link will be sent to the End-User for profile management which allows for self-management of form-factors, contact information, etc…

**Example of End-User Profile Management Below**
Problem: Are the right users gaining access to systems and data?
Solution: Multi-factor authentication mitigates identity risks

Product
- Universal Identity Services

Capabilities
- **Bring Your Own Device** by using mobile phone, SMS, OTP generator, IVR, etc. as credentials
- Multiple NIST compliant options
- Approve transactions with mobile app
Demonstrates the UIS authentication screens that a user will see when going through Juniper SSL VPN multi-factor authentication connection.

**Authentication Request Example Below**
Demonstrates the UIS authentication screens that a user will go through during Juniper SSL VPN multi-factor authentication connection.

**Authentication Request Example Below**

- **User Enters E-Mailed OTP**
  - The following password is valid for the next 5 minutes: 443171
  - Please enter this value into Universal Identity Services (US) to complete the authentication.
  - Please contact your support if you have any questions.

- **Submit**
Verizon Universal Identity Services
End-User SSL VPN Login – Profile Management

Demonstrates the completed authentication request to the UIS Profile Management screen.

**Completed Authentication Request Example Below**
The new access method includes a self-service password reset feature that allows users to reset a forgotten password via the KBA questions setup in their UIS profile. OTP will still be required to confirm the password reset.
FAQ – Learn More -
https://universalid.verizon.com/uid//resources/pdf/UniversalIDServiceHelpCenterFAQ.pdf

General
Why do I need to set up a user profile?
The creation of a user profile will permit you to be issued a personal, secure password to verify your identity each time you attempt to log in. The delivery of this password to you will confirm your identity and grant you access your personal information; making sure that someone else is not trying to access your account.

Why do I need another password to log in?
By requesting an additional password, a significantly higher level security can be provided to you and your personal information when you log in. By using a second password delivered to contact information that you provided, a higher level of assurance can be established that you personally are logging in, as opposed to an unauthorized person attempting to gain access your account and information.

Why do I need to provide you with my contact information?
Personal, secure passwords can be delivered to you in a variety of ways, based on the information you submit. These methods can be a voice call to one of your phone numbers, a text message sent to a cell phone you possess or provided directly to you by your smart phone, if you installed the mobile application.

Why are you asking for multiple contacts?
It is recommended that you enter several different contacts in your profile. A password will be sent to you each time you
Project Approach
Project Schedule

- July/August – Provisioning
- August – Testing
- Early September – Begin Migration
- Late October – End Migration
- Mid November – Turn down Legacy SSL VPN

Note: The above dates are subject to change based on equipment deployment and production system test results. Any date changes would be later than the dates above, not earlier.
Test Phase

1) Timing – August
2) Begins after install of Juniper routers at:
   a) 1 Ashburton Pl
   b) 200 Arlington St
3) Test UIS Enrollment Process
4) Test access to various MAGNet resources
5) Testers:
   a) Select group of ITD users
   b) Expand to select users in various agencies
### Project Approach

#### Migration Phases

<table>
<thead>
<tr>
<th>Group</th>
<th>Agencies</th>
<th>Users</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>ITD</td>
<td>226</td>
</tr>
<tr>
<td>2</td>
<td>ADD thru DMR plus TRE</td>
<td>1021</td>
</tr>
<tr>
<td>3</td>
<td>DOB thru EAS</td>
<td>994</td>
</tr>
<tr>
<td>4</td>
<td>EEC thru ETH</td>
<td>999</td>
</tr>
<tr>
<td>5</td>
<td>FAD thru RMV Employees</td>
<td>1000</td>
</tr>
<tr>
<td>6</td>
<td>RMV Mainframe</td>
<td>1257</td>
</tr>
<tr>
<td>7</td>
<td>SAO thru XMTA (less TRE)</td>
<td>840</td>
</tr>
</tbody>
</table>

**Total Users (as of 06/10/13)**  6337
## Project Approach

### Typical Agency Migration Time Line

<table>
<thead>
<tr>
<th>Week 1</th>
<th>Agency Technical Contacts Migrate &amp; Test</th>
</tr>
</thead>
</table>
| Weeks 2 & 3 | • Users Migrate  
             • Resolve Migration Issues |
| Weeks 4 & 5 | Maintain dual VPN service for 2 weeks |
| Week 6 | Disable legacy SSL VPN Connection |
Call To Action-You Are A Critical Part of the Project’s Success

- **Testing- Technical Contact Testers Needed.**
  - To Volunteer Contact Ed Maher ITD VPN Service Manager
    Ed.Maher@state.ma.us

- **Attend Training Offered Prior to Migration**

- **Migrate Agency Based on Schedule**

- **Final Note-** ITD will post these slides on the Intranet.
Step 1: Access Juniper URL, and the user is redirected to UIS for login:
Password Reset Continued
End User Self Management - Password Reset


test@icsl.net

The following password is valid for the next 5 minutes: 784212 Please...

test@icsl.net
to me

Mass.Gov

The following password is valid for the next 5 minutes: 906661

Please enter this value into Universal Identity Services (UIS) to complete the authentication.

Please contact your support if you have any questions.

Powered by Verizon

Click here to Reply, Reply to all, or Forward
Password Reset Continued
Please wait...

Launching Junos Pulse. This may take from a few seconds to a couple of minutes, depending on your bandwidth.

If an error prevents the Junos Pulse from loading properly, you can:
- Check browser accessibility.
- Continue. Not all functionality may be available.
Password Reset Continued
End User Self-Management Password Change

Manage Your Profile
Universal ID Profile Manager provides a secure electronic environment where individuals and organizations can manage their profiles.

Enter your credentials to manage your profile.

Username
Password
Login

Forgot Password?
End-User Self-Management- Password Change

Manage Your Profile
Universal ID Profile Manager provides a secure electronic environment where individuals and organizations can manage their profiles.

Enter your credentials to manage your profile.

Username: [Enter Username]
Submit

Powered by Verizon
Password Change Continued

Security Questions

Enter the answers to your chosen security questions.

What was the make of your first car?

What is your favorite movie?

Who is your favorite person from history?

Submit
Password Change Continued

Password successfully changed. You will be automatically redirected to login using your new password.