augustschell

CASE STUDY

U.S. Department of Defense Defeats Limitations of Legacy PKI

Executive Summary

One of our highest-value U.S. DoD customers was facing a Public Key Infrastructure (PKI) that was aging, unstable, and performing poorly. The PKI architecture, being a "system-of-systems" consisting of multiple Certificate Authorities (CAs) and Directory Servers (DSs), had grown to become unduly complex and extremely difficult and expensive to support. For redundancy and performance reasons, system components were deployed to multiple geographic locations.

Challenges

- The PKI systems were in dire need of modernization to meet current security standards and to improve overall performance and stability.
- Experiencing difficulties with the limitations of a legacy PKI system, including poor scalability and deficient security, running on operating systems that were beyond end-of-life for vendor support.

Business Impacts

- ✓ The customer was able to take on the role of a common service provider for PKI for the agencies they support, while ultimately enhancing their overall security posture.
- ✓ Limitations of a legacy PKI were eliminated as a result of an entirely reengineered, state-of-the-art infrastructure.
- ✓ Secure mobility was made possible, thanks to effectively configured derived credentials.
- ✓ The customer was able to deploy simpler and more secure CAs.

Solutions

Primary:

- A major reengineering effort – including software, physical servers, networks, and load-balancers.
- Software from Red Hat, including updated Red Hat Certificate System, Red Hat Directory Server, and Red Hat Enterprise Linux

Supporting:

- Red Hat Satellite
- Red Hat Enterprise Virtualization
- Puppet

Component of the U.S. DoD Faced an Aging PKI and Resulting Security Challenges

Our customer was challenged with sophisticated technology, a complicated architecture, and a major security issue: their PKI systems were outdated, causing poor performance, a weakening security posture, and operations management difficulties.

Our customer was also challenged to accept the role of PKI common service provider for many non-DoD agencies. A new, updated system with a highly effective user interface would be required to effectively update, secure and enable our customer to deliver the desired service levels.

Bringing an aging PKI out of the Dark Ages with a New, Automated Infrastructure

Jonathon Petrovitch, PKI Team Lead at August Schell recalled, "They required their PKI to be totally rearchitected and reengineered. After the issuance of a million certificates, the old CAs consistently started to degrade. To move forward, we wanted to refresh their entire enclave using the latest Red Hat software to fix

our standing bugs and institute the use of modern automation. The customer desparately needed faster, more automated server builds."

Using the existing, out-of-date technology, would've taken the customer up to three years to deploy a new CA. Petrovitch explained, "We were able to shorten the deployment process significantly as a result of scripting and automating the entire server build process. This allowed the customer to stand up new CAs much faster than ever before. Streamlining the build process also provided increased scalability."

In addition, the customer needed a system to enable derived credentials for mobility support. "ASE was the first company to enable DoD PKI certificates for use on mobile devices," Jeff Flax, August Schell Program Manager, explained. "That's a fast, ever-growing technology initiative, and it's extremely beneficial that the software is the same across the board, yet it's configured to allow continued growth and expansion."

Overall, August Schell was able to introduce advanced features and capabilities that were never before seen within the DoD PKI. Petrovitch added, "We were able to address the customer's problems by reengineering the PKI system from the ground up! We engineered a web application firewall that sits in front of the CAs. Server Virtualization was an absolutely necessity. "

Fully Redesigning, Rebuilding, and Redeploying a Public Key Infrastructure to Keep Pace with Certificates and Enhance Security

Teaming for Success: Bill Schell, President of August Schell confesses "The customer's Chief PKI Engineer and his DoD resources were a critical component of the overall team. One didn't succeed without the other." With the August Schell engineering team on-board to rethink the outdated PKI, the project began. The undertaking was initiated by an excruciatingly detailed architecting and planning period. "For several months before we began the reconstruction from the ground up, we sat shoulder-to-shoulder, fleshing out detailed requirements, white boarding, and planning."

The next step was standing up a new network with new networking hardware, new physical and virtual servers, and then getting all components to communicate with each other safely and securely. "We had to install the updated Red Hat Enterprise Linux OS on all new servers. Then we had to start implementing all the tools available with Red Hat Certificate System to make sure everything was up and running cleanly," Petrovitch said.

The customer worked closely with August Schell to provide feedback and approvals. A number of changes were made along the way, but the team didn't let the modifications slow down the project. August Schell paired team members with tasks that best matched their strengths and leveraged multiple test sites and labs to ensure all components were tested and verified before finally going into production. "We rebuilt the hardware, made sure everything was communicating properly, and finished up executing on the OS we built," Flax explained.

Common Service Provider Capability Achieved. Next Generation CAs Deployed. Derived Credentials Configured.

Ultimately, the PKI project was a success as a result of the teamwork between August Schell and the DoD engineering teams. The result is that the DoD can now leverage this system to deliver certificates in a reliable and efficient manner for years to come. They were also given the ability to inject credentials onto smart devices, mobile phones and tablets, which made securing mobile devices easier.

Our DoD customer now enjoys simpler, more secure certificate authorities and a totally refreshed, state-of-the-art PKI.

Through better communications and project leadership, and a strict focus on security, the processes of planning and deploying the new PKI system were significantly easier and more collaborative. "The collaboration we achieved enabled us to refresh the entire PKI system on new hardware, update the software, and consolidate many racks and servers down to just a few—and with even more power, CAs, and a greater overall product," Flax concluded.

51 Monroe Street, Suite 1802
Rockville, MD 20850
301.838.9470 | www.augustschell.com