

Secure Identity Management for HSPD-12

Certificate-based Authentication Hastens Compliance with Security Directive Innovative Identity Management Solution Built on Legacy Systems

With mounting concerns surrounding homeland and network security, federal agencies are looking for ways to enhance both physical and computer security that are cost effective, easy to deploy and that meet prevailing security standards.

Effectively managing the identity of users is germane to ensuring security for agency officials and network administrators. Recognizing the identity of each person requesting

information maintains data integrity and protects sensitive information from unauthorized access.

Standards Initiative Driving Identity Management

The federal government has been moving in the direction of standardizing identity management for some time. One initiative pushing aspects of this forward is the Homeland Security Presidential Directive-12 (HSPD-12), which outlines a policy for a common identification standard for federal employees and contractors. Agencies must have a program in place by October 2005.

With identity management taking a front-row seat, agencies are looking for a commercial solution that incorporates the use of smart cards. The solution they select to augment the authentication process must meet several requirements. A well designed solution should ease the burden of already-

“Having one common method for accessing the network improves security and reduces the complexity of what users are required to do.”

—Carl Vercio
OSD/WHS Program Manager

stretched system of administrators, and above all, it must be transparent to users.

Certificate-Based Network Login Addresses Shortfalls of Other Solutions

The Novell® Certificate-Based Network Login (CBNL), an off-the-shelf solution already deployed in the Department of Defense, may be the answer federal agencies are looking for to meet the requirements of HSPD-12. It provides secure access to network resources using standard X.509 Public Key Infrastructure (PKI) certificates and smart cards.

It's no secret that managing user names and passwords is tricky and time consuming. Federal employees have multiple passwords to commit to memory.

Adopting Novell's solution will result in "reduced sign-on." Coupling additional Novell technology with the CBNL solution, will significantly reduce the number of required passwords. By eliminating reliance on user names and passwords, the solution helps drive down the total cost of ownership, too. Because users won't have to call the help desk to get their passwords reset, the number of calls for assistance will be dramatically reduced, freeing up the help desk personnel for more important matters.

With Novell's CBNL, users who forget their HSPD-12 ID card can be issued temporary smart cards after completing an identity verification process. The software has the capability to extend a certificate revocation list (CRL) validity period or disable CRL checking, as appropriate.

CBNL Simplifies Security and Enhances Productivity

Another benefit of the Novell solution is "zero-day start" and "zero-day stop," according to Doug Rossie, Federal Government Sales Executive for Novell. When new

employees or contractors start, the system activates their status, giving them immediate access to all applications for which they have been approved based on their defined role.

Similarly, when someone leaves the agency, their access authority is automatically removed from the system. This capability is especially significant within the Defense Department, which has large numbers of people continually changing locations or leaving military service.

Authentication Solution Coexists with Many Products

"The beauty of the Novell authentication solution is that users don't have to be NetWare customers," said Rossie, adding that the software can be dropped into existing Windows*, Linux*, UNIX*, mainframe and other IT environments.

Many of the federal agencies use Microsoft's Active Directory. The Novell solution automatically synchronizes user names and passwords with Active Directory*, freeing up the administrators for other important IT matters.

In addition to supporting a variety of open standards, Novell's solution is highly scalable, very capable of managing millions of objects without negatively affecting the performance of the authentication process.

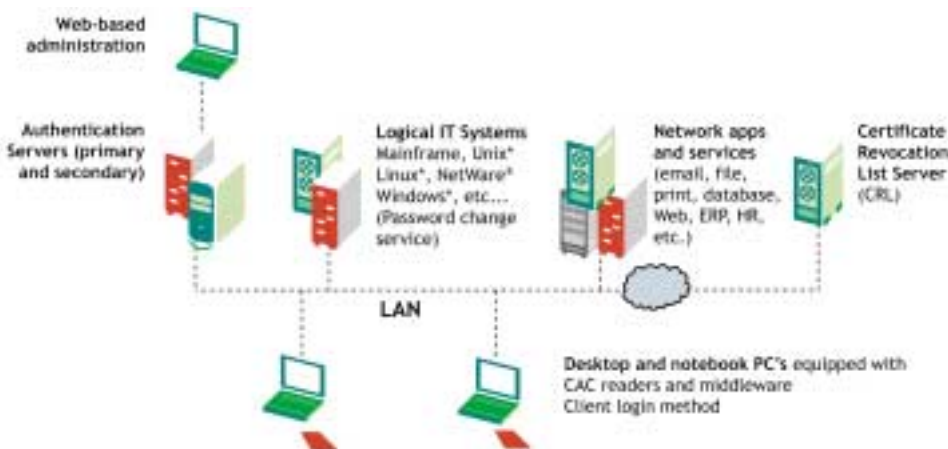
How do different users benefit from certificate-based authentication? The Novell solution provides the ability to connect many people to a single network. For example, in a veterans or military hospital scenario, doctors or nurses can insert their smart card to log on to the single network yet only access the applications appropriate to their role and identity. After they complete their work, they pull their card out which immediately logs them out. The "many-to-one" capability allows other people

the same access. Similarly, in a "one-to-many" scenario, one person may need and can be given access to multiple accounts

Novell's CBNL solution is already designed to incorporate the use of biometrics in areas demanding higher security. Any combination of the following elements can be used—smart card, PIN, biometric, and user name and password.

"We're anticipating a huge jump in interest for our certificate-based solution over the next two years because of the HSPD-12 requirement," concluded Rossie. "We see that organizations are becoming prepped to accept this technology. It's a matter of getting the technology in place." ●

The Novell Certificate-Based Network Login Solution Architecture



Certificate-Based Network Logon Improves Business Process and Network Security

New Solution Allows User Authentication Anytime, Anywhere

The Department of Defense (DOD) Washington Headquarters Services (WHS) faced the challenges of using the DOD Common Access Card (CAC) for secure network logon in a heterogeneous environment and meeting a diverse set of user requirements. Currently, military, civilian and contractor personnel all use the CAC for visual identification as well as for physical and logical access to DOD facilities and networks.

WHS provides a variety of administrative and operational services, including communications, human resource management, software development, and information technology for DOD services and agencies, including the Office of the Secretary of Defense (OSD). Under the direction of Carl Vercio, OSD/WHS Program Manager, the Identity Protection and Management Program provides comprehensive public key infrastructure, public key enabling, CAC and biometrics support for OSD, WHS and several other defense agencies and organizations within the National Capital Region.

WHS recognized that the ideal solution for improving its authentication process must leverage the DOD's significant investment in their CAC and PKI technology. "We initially looked at using the Microsoft Smart Card Logon solution but found a variety of network operating systems being used within the OSD and WHS," said Vercio. "At that time, many of the components were using Microsoft's NT operating system, which did not include the Smart Card Logon functionality. We finally realized we had to have a non-operating-system-specific solution."

WHS defined its requirements and sought a solution through the competitive acquisition process. It found a winning team in BearingPoint and Novell, which have been working side by side with WHS and other contractor personnel for the past 18 months to develop and deploy an operating-system-independent Certificate-Based Network Logon (CBNL) solution based on Novell off-the-shelf products.

CBNL provides a secure network authentication solution for federal agencies, which will be required to comply with Homeland Security Presidential Directive 12 (HSPD-12) mandating a common federal identification standard. CBNL is an open-standards authentication solution that uses CAC containing PKI certificates and will allow DOD to use HSPD-12 credentials from other federal agencies. Of major benefit to WHS is that hardware and software components of CBNL are added to the existing infrastructure; therefore, there is no need to replace or modify the current operating system, hardware or software within the environment.

"Supporting open standards, our technology helps authenticate those individuals to the appropriate computer systems to which they need access," said Doug Rossie, Novell's Federal Government Sales Executive. "Users insert their cards into the computer and enter a PIN [personal identification number], which allows them access to network resources without the need for user name and password." The PIN, which only the CAC holder knows, provides access to the digital certificates on the card to authenticate the user to the network. "Without a

CAC and knowledge of the PIN, you are not going to be authenticated as one of the authorized users on our network," said Glen Lee, a contractor from Reality Based IT Services, Ltd., who leads the WHS Identity Protection and Management Team.

Continuity of Operations, Improved Business Processes Top List of Requirements

One of the most pressing user requirements was the ability to support multiple operating system environments and ensure that the new authentication process did not affect continuity of operations.

"We needed a flexible solution to allow us to maintain continuity of operations," Lee said. According to Lee, it is not uncommon for people to forget their CAC, and the system must have the ability to still provide them access



to the network with high assurance. The use of standard X.509 PKI certificates for authentication by the CBNL solution permits temporary guest or access cards containing DOD PKI certificates to be signed out to users, allowing them to perform many of their day-to-day business functions that do not require their personal CAC.

"Users will not be able to send signed E-mail, read encrypted E-mail, or access systems or Web sites that require their personal CAC," said Vercio. "They will at least be able to access their files or data on the computer or network, send and read regular E-mail, and perform other functions that would permit them to get through a workday without requiring them to endure the one-to-two-hour D.C. commute home to get their CAC."

Lee explained that the solution had to empower the local network administrators to ensure that network access is not denied to the entire community because of environmental or operational issues outside their control. The concern was that the lack of the most current certificate revocation information (certificate revocation lists, or CRLs) from the Defense Department PKI could prevent an entire user community from accessing its local network. "It is crucial that users be able to continue to authenticate with their CAC even if the latest CRLs are not immediately available," he said. "Otherwise, we have a denial of service to the network until either everyone is provided a password or new certificate revocation information becomes available. Either way, we encounter significant downtime at a significant cost." CBNL addresses these issues.

Also high on the list of requirements was single user access to multiple accounts. The WHS environment is typical of many federal agencies in which employees have multiple roles, each requiring a separate account for network access. WHS needed a way to allow the use of the same CAC to authenticate users into those multiple accounts but still maintain a specific audit trail.

It is also common for more than one individual to require access to the same account. For instance, an administrative assistant to the agency director is likely to be authorized to

read and send E-mail at the director's request. Instead of sharing a password, which violates good security practices, an account can be configured in CBNL for access by multiple individuals using their own CAC. Once again, this process is audited so that it is clear who accessed the account at a particular date and time.

Simplified Solution Allows Agency to Leverage Investment

Another major objective was improving the business process. Currently, the organization relies on passwords that according to DOD policy must be changed periodically.

"Any solution that we brought to the table had to prevent users from needing to know their password or manage it on their own," said Lee, who acknowledged that password management by users has inherent shortcomings, such as users forgetting, writing down, or not creating very secure passwords.

Furthermore, CBNL will prove to be a smart way to do business because the number of calls to the help desk will be dramatically reduced. Users will have the same PIN for the life of their card.

"Having one common way of accessing the network, whether through remote access, the Web, or desktop reduces the complexity of what users have to do," said Lee. "User frustration should be significantly reduced because users will follow the same process every time, anyplace."

IT Team Experiences Novell Solution Firsthand

The WHS Identity Protection and Management Team will be deploying the Novell authentication solution initially throughout WHS and selected OSD components and will eventually become the enterprise solution.

For deployment, IT staffs are targeted as the early adopters of the solution. "This process allows us to vet the solution with those who are more tolerant of change so they can understand what the user experience is going to be," said Lee, adding that his team is committed to making sure the user experience is a positive one, because "success breeds acceptance."

Novell Authentication Lays Groundwork for Multilevel Authentication

In the existing environment, a PIN is used along with the CAC to gain entry to the network. However, in the future, the Defense Department may augment authentication procedures with additional requirements such as a biometric component. The added levels of security will be accomplished through Novell's authentication chaining.

CBNL pre-positions DOD to use not only the CAC but also the smart cards of its federal partners that result from the implementation of HSPD-12. Said Vercio: "We sincerely hope that one day soon, our federal partners can enter the Pentagon using their agency HSPD-12 ID card and be able to login to a workstation on their temporary work site network using the same smart card with CBNL." ●

Novell®

To learn more about HSPD-12 and Novell's Certificate-Based Network Login solution, contact your Novell representative or call 1-800-321-4272. You can also visit www.novell.com/hspd12

Novell, the Novell logo and NetWare are registered trademarks of Novell, Inc. in the United States and other countries.

*Linux is a registered trademark of Linus Torvalds. UNIX is a registered trademark of X/Open Company Ltd. Microsoft and Windows are registered trademarks and Active Directory is a trademark of Microsoft Corporation. All other third party marks are the property of their respective owners.