



INSIDE:
**Department
of Defense
Solution
Spotlight**

Certificate-Based Authentication:

A Homeland Security Imperative

Novell.

Advertising Supplement to Federal Computer Week

Use of Novell® Certificate Login Addresses Security Challenges, Alleviates Risks

To strengthen security measures used by all federal agencies, President Bush issued Homeland Security Presidential Directive 12 (HSPD-12), which requires a common form of identification be issued to all federal employees and contractors.

Under the HSPD-12 mandate, identification methods using smart card technology will be utilized to grant only authorized individuals access to buildings and computer resources. The regulation is widely viewed as a logical step forward. In today's complex political, cultural and economic climate, both public and private sector institutions are reinforcing the security of their physical facilities and logical IT systems.

To comply with the new regulation, simple passwords — easily hacked, often forgotten and a chronic IT headache — are being replaced by multi-factor authentication processes using various combinations of identification technologies.

This explains why the Department of Defense, for example, is using smart cards and Public Key Infrastructure (PKI) to address the need for

stronger authentication. Smart cards can safely store a wide range of personal data such as fingerprints, facial images and employee identification codes, as well as PKI-based digital certificates and encryption keys.

Embedded processors enable card users to digitally sign documents and encrypt messages for secure transmission over non-classified networks. Smart card access solutions for physical facilities, security and personal computer login are commercially available from a variety of suppliers. Until recently, however, PKI-based smart card authentication faced significant limitations, especially for controlling access to heterogeneous IT environments with many shared services and applications.

Complex login procedures requiring digital signatures and encrypted message exchanges could be daunting for inexperienced users to learn, and redundant login processes for each location, system and service would waste time and sap productivity. One of the most serious obstacles was related to recent releases of the Windows server operating system, which introduced difficulties with its own proprietary form of smart

Certificate-based Authentication at the U.S. Department

Washington Headquarters Services (WHS), an agency of the U.S. Department of Defense (DOD), is a services provider for many DOD agencies and organizations, including the Office of the Secretary of Defense (OSD). As such, it provides a range of administrative and operational services, including accounting, building maintenance, communications, human resource management, information technology, records management and software development.

Under the direction of Carl Vercio, the WHS Identity Protection and Management Program provides comprehensive Public Key Infrastructure (PKI), Public Key Enabling, Common Access Card (CAC) and Biometrics support for 15,000 users in the D.C. metropolitan area.

All OSD and WHS employees possess a CAC — the official identification card for DOD military, civilian and eligible contractor personnel. The CAC is a visual ID card that also uses smart card technology to provide a digital ID for both physical and logical access to DOD facilities and networks. With more than 3.1 million users, the CAC is unquestionably among the world's most

ambitious smart card implementations. Like all DOD agencies, WHS is working to implement solutions that realize the security benefits and improved business processes of the Department's billion-dollar investment.

Regulatory requirements for improved security, including mandates such as Homeland Security Presidential Directive 12 (HSPD-12) and the Federal Information Processing Standard (FIPS) 201, have fostered a government-wide desire for stronger authentication processes.

According to Vercio, HSPD-12 is long overdue and sets the stage for the DOD and other federal agencies to develop interoperable identity cards and credentials that can be recognized and trusted by all organizations. "Our customers are demanding that our physical and logical access control business practices be reviewed and changed to allow the DOD to trust the credentials issued by another agency for use at DOD locations," he said.

The CAC, containing digital certificates stored on an embedded micro-controller and secured by a PIN (Personal Identification Number), is used to authenticate

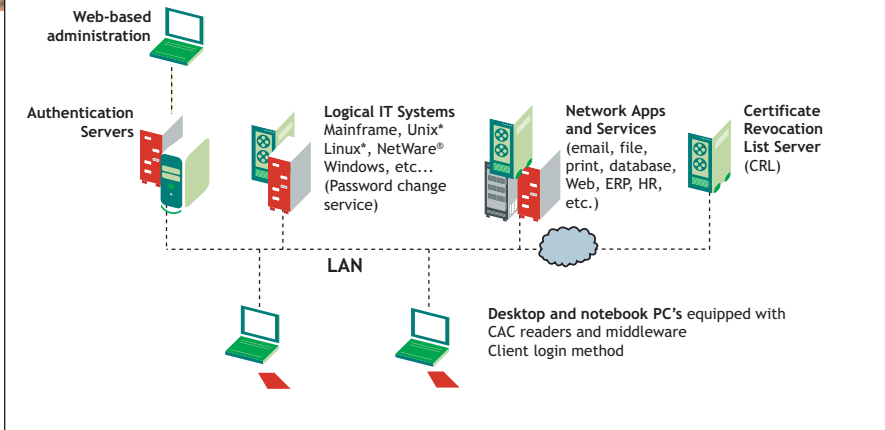
the CAC owner, sign documents and encrypt messages. The CAC architecture conforms to open industry standards and is designed to support current and future authentication methods, including biometrics.

Before 2003, DOD users typically authenticated to networks with a user ID and password. WHS decided to take the lead in closing what has been considered a widespread vulnerability by developing a stronger authentication process leveraging the DOD's existing smart card and PKI investment.

After a formal acquisition process, WHS selected BearingPoint, Inc., and Novell to develop and deploy a new authentication solution, called Certificate-Based Network Logon (CBNL), which will eventually become an enterprise-wide CAC authentication solution. In January 2005, WHS began deploying CBNL to its 1,800 users and to selected OSD components.

"Novell offered a vendor-agnostic alternative that formed the basis of the agency's new authentication solution," said Glen Lee, E-security Technical Director, Reality Based IT Services, Ltd. (RBIS, Ltd.), Laurel, Md.,

The Novell Certificate-Based Network Login Solution Architecture



card/PKI authentication. As a result, even organizations with extensive PKI-based smart card programs are still relying on easily compromised passwords to secure many Windows-based services.

For government organizations seeking open, standards-based secure authentication using smart cards, digital certificates and public key cryptography, Novell® Certificate Login (NCL) provides a comprehensive and customizable solution. NCL replaces the risks, costs and management overhead of password maintenance with a highly secure, multi-factor process that simplifies resource access for authorized users and reduces the management



This schematic shows the solution deployed in a typical smart card-enabled environment featuring: An existing smart card and PKI; Desktop and notebook PCs equipped with card readers and middleware; Linux, NetWare, Unix, Windows or mainframe-based services and applications.

workload on administrative personnel. In particular, government agencies currently using smart cards are likely to find this solution ideally suited to both their security needs and existing IT infrastructure.

That's because Novell has more than 20 years of experience as a strategic solutions provider to national,

regional and local governments around the world. Novell government solutions combine industry-leading technology and service expertise to help governments address the need for flexible, efficient, interactive and secure systems that leverage existing technology investments and accommodate new applications.

The company supports all products and solutions with a robust and global ecosystem that includes design and deployment expertise, strong partner relationships and an unparalleled commitment to service and support.

of Defense

the contractor leading the WHS Identity Protection and Management Team.

Novell's identity management tools provided the foundation for CBNL, which in turn influenced the development of Novell Certificate Login. CBNL utilizes the CAC with DOD PKI certificates to authenticate users to the network. A significant benefit to WHS was that there was no need to replace or modify current operating systems, hardware or software; CBNL hardware and software components simply augment the existing IT environment.

WHS decided to use the CAC and PIN to improve network security and certain business processes. Users need both the CAC and a PIN (something each person has, plus something they know) to gain access to network services. "This significantly reduces the security threat of unauthorized access by individuals who should not be on our network," said Lee.

CBNL greatly increases the DOD's network security and provides other benefits as well. The use of the CAC and PIN eliminates the need for users to manage long, complex passwords. "The process of changing pass-

words has been automated, rotating as required, at administratively configurable time periods such as every 24 hours," said Lee.

The cost of resetting passwords and getting that information to users was a help desk challenge that has essentially been eliminated. Lee expects the WHS to see a rapid return on investment once users have been trained to use their CAC and PINs to gain access to network services and applications.

The biggest challenge ahead is one of change management, as the agency strives to ensure what's delivered to customers is as seamless and easy to use as possible. "We expect a bit of a spike in help desk calls because this is new; however, continual usage will significantly reduce administrative burdens and improve the overall user experience," said Lee.

With CBNL, WHS will provide to its users a common network logon experience. Whether through remote access solutions, the Web, or the desktop, users will simply be required to insert their CAC and enter their PIN to gain access to the network.



*Carl Vercio, director,
WHS Identity Protection and Management Program*



Identity Management Using Novell® Certificate Login

Novell® Certificate Login (NCL) is a strong, multi-factor authentication solution that leverages existing smart card and public key infrastructure (PKI) technologies. Combining NCL with additional Novell technology, federal agencies can provide secure, but easily managed access control for Linux*, NetWare®, Unix*, Windows* and mainframe environments.

An authentication layer of proven Novell identity management software components provides the centralized login services for a wide range of IT environments including support for Novell eDirectory and Microsoft Active Directory* and other network domains using digital certificates stored on a user's smart card.

NCL can scale to support any number of users, applications and locations, and is extensible to accommodate additional authentication factors. NCL is also interoperable with any internal or external certificate authority.

Novell Certificate Login acts as an authentication mechanism that allows users to login to all network resources using digital certificates stored on their smart card, such as the Department of Defense Common Access Card (CAC). (See related case study on page 2). This open, standards-based solution replaces multiple passwords with an easy-to-use, multi-factor authentication process.

NCL automates the authentication process, making it transparent for users and easily manageable for an IT staff. Key features of NCL include:

- A meta-directory service that synchronizes user and resource information across network directories, domain controllers and any PKI infrastructure, providing centralized real-time access management and control capabilities;
- Certificate lifecycle management capabilities including issuance, secure storage, encrypted transmission, validation and revocation list maintenance;
- Comprehensive encryption, decryption and key management services;
- An authentication factor interface capable of integrating additional identification technologies, including biometrics, in varying combinations;
- An auditing and reporting service that automatically logs authentication events and the identity of participants.

Novell Certificate Login will scale from small office applications to the largest global enterprise environments, and will interoperate with any internal or external certificate authority.

Key Benefits

NCL provides a range of benefits for government audiences, including:

- **Increased security** of networks, applications and data using strong, multi-factor authentication — eliminating risks associated with poorly managed passwords. Rigorous security measures for credential storage, handling and transport minimize the potential for theft or tampering.

- **Enhanced user productivity** because the simple authentication process masks the complexities of certificate-based directory authentication and makes authorized domain resources conveniently available in a single login process.

- **Economy and extensibility** because NCL leverages existing smart card and PKI investments, and provides built-in support for biometrics and other current and emerging authentication technologies.

- **Reduced administrative workload** because NCL eliminates password-related user account administration, and provides an easy-to-use web-based management console for login system administration.

- **Convenience and ease of use** from a flexible authentication process that works even for mobile users logging on to their workstations in disconnected mode, or if authentication servers are temporarily unavailable.

In addition to the Novell software integrated into NCL, the solution includes modules to automate administrative processes, including:

- **Disconnected Mode** – A module that encrypts the user's Windows credentials in the workstation registry, allowing the user to authenticate to the workstation using a smart card when the workstation is disconnected from the network, or if the NCL server is unavailable.

- **Temporary Certificate** – A feature that allows a temporary smart card and certificate to be issued to users who have lost or forgotten their cards.

- **Password Change** – Because many security policies require periodic password changes, user passwords are changed to random values based on rules created by the system administrator.

- **Hardware Certificate** – During the login process, certificate attributes are verified and submitted for authentication.

- **Certificate Expiration Notification** – A module that checks the user's certificate expiration date and issues a notice when it detects approaching expiration.

- **CRL Grace Period** – To extend the use of a certificate revocation list (CRL) that has reached its next update, when a fresh CRL is not yet available.

- **Workstation Lockdown** – A post-login feature that locks down a workstation when the user's smart card is removed, which prevents unauthorized users from accessing network resources.

To learn more about HSPD-12 and Novell Certificate Login, contact your Novell Solutions Provider, your Novell representative or call 1-888-321-4272. You can also visit www.novell.com/hspd12

Novell, Inc.
404 Wyman
Suite 500
Waltham, MA 02451
www.novell.com