

A large, abstract, light gray graphic on the left side of the page, consisting of several overlapping, curved shapes that create a sense of depth and movement.

MEETING THE REQUIREMENTS OF HSPD-12

The Identity Management Factor
White Paper
June 2006

Table of Contents

Executive Summary	3
Requirements of HSPD-12	4
Criteria	4
Milestones	4
The Role of Identity Management in Conformance to HSPD-12	5
Relevant Definition and Characteristics of Identity Management	5
Role of Identity Management in the HSPD-12 Concept of Operations	6
Advantages of Sun™ Identity Management for HSPD-12 Conformance	7
Comprehensive Capabilities	7
Life Cycle Management Approach	7
Extensive Integration of Technology	8
Sun Leadership and Experience	8
Sun Identity Management Products for HSPD-12 Conformance	9
Sun Java System Identity Manager	9
Sun Java System Access Manager	9
Sun Java System Directory Server Enterprise Edition	9
Sun Java System Federation Manager	9
Conclusion	10

Chapter 1

Executive Summary

The need to protect sensitive government information and resources has moved front and center in the wake of heightened security concerns over the last several years. One example of the federal government's increased emphasis on securing its facilities and systems is the issuance of the Homeland Security Presidential Directive 12 (HSPD-12) in 2004. The directive specifically addresses potential problems with employees and contractors using insecure forms of identification to access government buildings and information systems. This paper is concerned with the role that identity management products and systems can play in ensuring conformance to HSPD-12.

In addition to addressing major criteria for conformance with HSPD-12, as explained in detail in Chapter 3, identity management is particularly well suited to the task because it also addresses a second, equally urgent challenge for government. That challenge, ironically, is the need to increase openness of government operations. As the pressure to make it harder for the wrong people to access information and resources has risen, the need to make it easier for the right people to access information and resources has also grown. This need arises from the trend toward more open collaboration across government agencies, as well as beyond them, with other governments, contractors, and external entities. This openness even extends to HSPD-12. Among its requirements, as discussed in Chapter 2, is interoperability of the standard's implementation across the federal government, as well as compatibility with foreign government systems.

The right identity management solution plays a critical role in achieving the directive's goals, and in a manner that is mindful of the need for cost consciousness and control, inherent to publicly funded operations.

This paper specifically examines:

- HSPD-12 and its requirements, including the requirements of the related Federal Information Processing Standards (FIPS) 201
- Relevance of identity management to HSPD-12 and FIPS 201 conformance
- Advantages of Sun™ identity management for meeting HSPD-12 requirements
- HSPD-12-related capabilities of Sun identity management products

Chapter 2

Requirements of HSPD-12

HSPD-12 specifically mandates the promulgation of a new standard for secure, reliable identification issued to federal employees and contractors. In response to HSPD-12, the National Institute of Standards and Technology (NIST) released a new standard, FIPS 201, to provide implementation instructions for the directive. FIPS 201 consists of Personal Identity Verification (PIV) components that 1) define the minimum requirements for a system for meeting security goals that include proving identity, and 2) provide the technical specifications to meet security goals and achieve interoperability of smart cards that are to be used to meet key requirements of HSPD-12.

Criteria

The goal of HSPD-12 is to increase security, reduce identity fraud, and increase efficiency by setting guidelines and time lines for a new standard to establish secure identification for federal employees and contractors. According to the requirements of HSPD-12, secure and reliable forms of identification must meet the following criteria:

- Based on sound criteria to verify an individual's identity
- Strongly resistant to fraud, tampering, counterfeiting, and terrorist exploitations
- Allow for personal identity to be rapidly verified electronically
- Have identity tokens issued only by providers whose reliability has been established by an official accreditation process

Conformance with HSPD-12 also requires interoperability of the standard's implementation across federal badge-based facilities and information systems. This interoperability must be achieved while minimizing the risk of system penetration by terrorists or others. Furthermore, compliance requires that the implementation be compatible with foreign government systems, implying the ability to ultimately achieve international interoperability.

Milestones

The federal government has imposed strict deadlines for meeting the HSPD-12 requirements, and executive departments and agencies have no time to lose. Currently, they must already be in compliance with the first part of the FIPS 201 guidelines, which necessitates the establishment of common identity and security requirements, as well as the definition of specifications to support minimum requirements for technical interoperability. No later than October 27, 2006, departments and agencies must deploy products and systems that conform to HSPD-12. By that date, they must:

- Issue appropriate credentials for new employees and contractors (or, for current employees, phase in new credentials by October 27, 2007)
- Implement the standard's technical requirements in the areas of personal authentication and access controls, as well as card management
- Use an appropriate card authentication mechanism as determined by specific levels of risk
- Use at least one digital certificate on the identity credential for access control

More detailed information is available in the *Federal Identity Management Handbook* published by the Federal Identity Credentialing Committee of the U.S. Government Services Agency (GSA). Additional documents are available from the Federal CIO Council on the e-Authentication Web site at <http://cio.gov/eauthentication>.

Chapter 3

The Role of Identity Management in Conformance to HSPD-12

How can identity management address the requirements of HSPD-12 to 1) create secure and reliable forms of identification that meet the criteria outlined in Chapter 2, and 2) deploy appropriate products and systems that meet the looming deadline of October 27, 2006? The right identity management solution can help meet both these challenges.

Relevant Definition and Characteristics of Identity Management

Identity management is, at the most basic level, automation of processes that deliver access to an organization's networked information assets to the right people at the right time — and deny access to others. When integrated with systems for physical access, such as card-based systems, these broad identity management capabilities can be made to extend beyond information assets to include physical facilities. Ultimately, identity management can provide the foundation for aggregation of physical and logical access control, resulting in a consolidated system where the same credentials could be used for both types of access control.

An effective identity management solution will:

- Manage, enforce, and standardize broad organizational access-control policies across diverse applications and systems, whether within one agency or department, throughout the broader world of agencies, and, increasingly, the even larger universe that includes outside contractors, foreign governments, and other external entities
- Synchronize and standardize identity information about individuals across applications and environments — again, both within discrete departments and agencies, across them, and beyond
- Manage identity information over the life cycle of an identity, and synchronize it across all repositories of identity data as it changes over time
- Use strong authentication to control access to resources when users attempt to use them
- Extend access control and single sign-on (SSO) mechanisms across departmental boundaries, while centralizing administration of authorization and authentication in order to make it easier for departments to meet stringent guidelines and time-sensitive rollouts
- Provide accurate reporting and auditing of who accessed what information and other resources, and who authorized their access, to limit potential risks to the security of sensitive assets
- Take full advantage of automation and technology integration in order to increase the solution's deployment speed and lower costs, as well as reduce ongoing costs and other administrative burdens of maintaining a solution over time

These characteristics make identity management well suited to playing a key role in meeting HSPD-12 requirements for creating forms of identification that are based on sound identity verification criteria, resistant to security breaches, and allow for rapid electronic verification of personal identification. They are also specifically relevant to fulfilling the need for personal authentication and access controls. And they meet the ever-present requirement for solutions that reflect cost consciousness and make the most of taxpayer investment in government systems.

Role of Identity Management in the HSPD-12 Concept of Operations

The preceding information describes generally how identity management relates to conformance with HSPD-12. The following information demonstrates the nearly ubiquitous and practical role identity management can play in the process of identity verification and issuance, as defined by FIPS 102 and its specific PIV components.

First, let's look at the operational process proposed by PIV.

1. An individual applies for credentials.
2. The request goes through appropriate channels.
3. The request is processed.
4. Credentials are issued and recorded.
5. The individual attempts access.
6. Identify and credentials are verified by the system.
7. Access is granted.

Now, let's consider how identity management fits into a practical implementation of the concept. The U.S. GSA positions the identity management system as the central component of the PIV-based identify verification and issuance process. The identity management system is where an applicant's identity information goes when it is initially submitted, and where that information is processed. It is also where the capabilities reside to verify the applicant's identity, including the applicant's role or roles within the organization and corresponding levels of access, and to provision resources for the applicant accordingly. In the PIV-defined, card-based access environment, the identity management system automatically provides verified identity information to the system that produces and personalizes card credentials, and then to the issuing department or agency for card activation.

After this verification-and-issuance scenario, identity management continues to play a critical role as the system responsible for managing identity information throughout its life cycle. In this role, each time an individual seeks access, the identity management system's authentication and authorization capabilities must act to grant or deny access, based on whether the individual is who he or she claims to be, and whether the individual is authorized for access to the particular resources for which access is being requested. This activity is dynamic, constantly changing as the individual's role changes within the department or agency — and abruptly ceasing when the relationship to the organization ends. Through it all, access activity is constantly audited and reported so that the department or agency always knows who has access to what, who authorized it, and when there has been an unauthorized attempt at access.

Chapter 4

Advantages of Sun™ Identity Management for HSPD-12 Conformance

Sun identity management securely delivers the comprehensive capabilities, life cycle management, and extensive integration to help enable departments and agencies to conform to the HSPD-12 directive quickly and cost-efficiently. In addition, Sun is widely recognized for its leadership in identity management and is an experienced vendor to governments.

Comprehensive Capabilities

Sun identity management includes the following products, which are described in detail in the next chapter.

- Sun Java™ System Identity Manager, a provisioning component that automates processes associated with granting and revoking access to resources, and enables accurate auditing and reporting of access activities
- Sun Java System Access Manager, a single, integrated solution for authenticating and authorizing all user requests for identity-based access to resources
- Sun Java System Federation Manager, which enables open, secure collaboration among multiple agencies and other governments on a large scale
- Sun Java System Directory Server Enterprise Edition, which provides a scalable and highly available central repository for storing and managing identity profiles

Life Cycle Management Approach

These Sun products provide the life cycle identity management required for conformance with HSPD-12. From the moment an employee or contractor becomes associated with a government department or agency, to the second the individual ceases to be connected to the organization, Sun products manage the user's entire identity life cycle. To make this possible:

- Workflows are automated and designed to integrate with PIV-driven smart card applications
- All provisioned elements are tracked and all access actions are auditable
- Complex workflows and interdependencies are automated
- Timely deprovisioning or partial deprovisioning occurs when there are changes in employee role or status during the identity life cycle
- Access control over resources exists at any time in the life cycle that users attempt to access them
- Access control and SSO mechanisms extend across departmental boundaries, and administration of authentication and authorization is centralized
- Authoritative source of identity information is established

Extensive Integration of Technology

Sun identity management products are designed for rapid, easy integration with other access-related products and systems, as well as with existing IT infrastructures. This speeds and simplifies product rollout, reduces deployment costs, and delivers more options to departments and agencies seeking to conform to HSPD-12. Examples of Sun identity management integration include:

- Out-of-the-box resource adapters that can be easily configured to enable provisioning of users into card-based access systems
- Standards-based integration with other business systems, as well as with a variety of third-party security and identity solutions
- Single, unified framework for authentication and policy-based authorization across systems and environments
- Web SSO capabilities, as well as compatibility with third-party enterprise single sign-on (ESSO) solutions
- Ability to leverage and reuse services across departments, agencies, and external entities such as outside contractors or other governments
- Compatibility with smart card platforms for departments and agencies that choose to implement digital identity card technology for secure physical access

Sun Leadership and Experience

Sun is widely recognized as a leading force in identity management. For example, in its Q1 2006 *Forrester Wave* report on provisioning, Forrester Research noted Sun's position as a market leader. Gartner positioned Sun in the "Leaders" quadrant of its H106 *User Provisioning Magic Quadrant*. Gartner places companies in the "Leaders" quadrant based on their completeness of vision and ability to execute. Sun is also a veteran vendor to the federal government, providing identity management infrastructure for federal agencies, as well as state and local governments.

Sun identity management meets government needs well for several reasons.

- Strong support for open standards facilitates interoperability within current agency environments, limiting the need for additional significant IT investment.
- Scalability in highly secure environments is proven in large-scale implementations. Among the most prominent is the Common Access Card program of the U.S. Department of Defense (DoD). Built on Sun identity management and Java Card™ technology, the program consolidates multiple access cards used by employees into a single card with secure extensibility to accommodate changing roles throughout the user life cycle.
- Only Sun identity management brings together centralized control over access to secure information, automated processes, and complete auditing and reporting — a unique combination that enables government to deliver the highest levels of information security while controlling costs.
- Sun's experience with secure, card-based solutions extends to its own operations with the company's Java Badge program to enable consolidated, secure access to physical and networked company resources.

Chapter 5

Sun Identity Management Products for HSPD-12 Conformance

Sun identity management products deliver the following specific capabilities in support of HSPD-12 conformance.

Sun Java System Identity Manager

This comprehensive product for managing identity profiles and permissions throughout the identity life cycle:

- Automates user provisioning and password management to improve efficiency, lower costs, and enhance security when implementing the HSPD-12 standard
- Proven in customer deployments to support millions of user identities
- Provides integrated workflow capabilities to manage all processes in accordance with HSPD-12
- Enables separation of duties and roles to provide complete life cycle management under HSPD-12
- Includes fully integrated, identity-based auditing capabilities to provide comprehensive auditing and reporting to ensure HSPD-12 compliance

Sun Java System Access Manager

This integrated solution for authenticating and authorizing user requests for access to resources:

- Meets HSPD-12 requirements for identity verification and authentication by providing robust, centralized authentication capabilities
- Uses role- and rule-based authorization that enables effective life cycle management of identities under HSPD-12
- Supports HSPD-12 interoperability requirements through seamless integration with existing infrastructures and systems via multiplatform software development kit (SDK) support
- Enables SSO for heterogeneous environments, including Microsoft Windows desktops
- Deploys with a single Web Archive (WAR) file for easy, cost-effective rollout

Sun Java System Directory Server Enterprise Edition

A market-leading directory solution that:

- Supports efficient identity life cycle management under HSPD-12 by providing a central repository for identity information from multiple sources
- Most widely deployed, Lightweight Directory Access Protocol (LDAP)-based directory server, with more than 1.5 million licenses sold
- Provides highly secure and easy-to-manage directory services
- Features password synchronization with Microsoft Active Directory to enhance security and improve service to users

Sun Java System Federation Manager

Designed to enable large-scale external collaboration, it:

- Supports a standards-based framework for trusted partnerships across organizational boundaries, enabling a level of extensibility critical to meeting HSPD-12 requirements for interoperability and openness
- Enables repeatable integration with external systems to lower interoperability costs

Chapter 6

Conclusion

Conformance with the federal government's HSPD-12 directive presents departments and agencies with a formidable challenge. By October 27, 2006, they must implement a new standard for secure, reliable identification of employees and contractors. Identity management in general, and Sun identity management in particular, plays an important role in enabling departments and agencies to meet this challenge. Sun identity management products:

- Lay a solid foundation for the aggregation of physical and logical access control
- Enable standardization and automation of processes associated with securely establishing and managing identities
- Deliver workflow-driven technology to ensure standardization of access control rules and roles
- Provide life cycle management of identity information for timely, accurate changes to individual access rights — including immediate deprovisioning of resources
- Include accurate reporting and auditing of all individual access rights, what each individual has accessed, and who authorized access
- Offer integration and compatibility characteristics required to support interagency and intergovernment interoperability
- Standards-based and interoperable with existing applications, data stores, and other resources
- Excel in heterogeneous IT environments often characteristic of government agencies

To learn more about identity management and its contributions to the security of federal government information and resources, visit www.sun.com/identity.

© 2006 Sun Microsystems, Inc., 4150 Network Circle, Santa Clara, CA 95054 USA

All rights reserved.

This product or document is protected by copyright and distributed under licenses restricting its use, copying, distribution, and decompilation. No part of this product or document may be reproduced in any form by any means without prior written authorization of Sun and its licensors, if any. Third-party software, including font technology, is copyrighted and licensed from Sun Suppliers.

Parts of the product may be derived from Berkeley BSD systems, licensed from the University of California.

Sun, Sun Microsystems, the Sun logo, Java, Java Card, and the Network is the Computer are trademarks, registered trademarks, or service marks of Sun Microsystems, Inc. in the U.S. and other countries.

UNIX is a registered trademark in the United States and other countries, exclusively licensed through X/Open Company, Ltd.

All SPARC trademarks are used under license and are trademarks or registered trademarks of SPARC International, Inc. in the U.S. and other countries. Products bearing SPARC trademarks are based upon an architecture developed by Sun Microsystems, Inc.

The OPEN LOOK and Sun Graphical User Interface was developed by Sun Microsystems, Inc. for its users and licensees. Sun acknowledges the pioneering efforts of Xerox in researching and developing the concept of visual or graphical user interfaces for the computer industry. Sun holds a non-exclusive license from Xerox to the Xerox Graphical User Interface, which license also covers Sun's licensees who implement OPEN LOOK GUIs and otherwise comply with Sun written license agreements.

RESTRICTED RIGHTS: Use, duplication, or disclosure by the U.S. Government is subject to restrictions of FAR 52.227-14(g)(2)(6/87) and FAR 52.227-19(6/87), or DFAR 252.277-7015(b)(6/95) and DFAR 227.7202-3(a). DOCUMENTATION IS PROVIDED "AS IS" AND ALL EXPRESS OR IMPLIED CONDITIONS, REPRESENTATIONS AND WARRANTIES, INCLUDING ANY IMPLIED WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE OR NON-INFRINGEMENT ARE DISCLAIMED, EXCEPT TO THE EXTENT THAT SUCH DISCLAIMERS ARE HELD TO BE LEGALLY INVALID.