



HSPD-12

Common Identification Standard for Federal Employees and Contractors

On August 27, 2004, the President signed HSPD-12 “Policy for a Common Identification Standard for Federal Employees and Contractors” (the Directive). The Directive requires the development and agency implementation of a mandatory, government-wide standard for secure and reliable forms of identification for Federal employees and contractors. As required by the Directive, the Department of Commerce issued Federal Information Processing Standard 201 (the Standard).

It further specified secure and reliable identification that —

- > Is issued based on sound criteria for verifying an individual employee’s identity
- > Is strongly resistant to identity fraud, tampering, counterfeiting, and terrorist exploitation
- > Can be rapidly authenticated electronically
- > Is issued only by providers whose reliability has been established by an official accreditation process.

Compliance with the Standard requires the activation of at least one digital certificate on the identity credential for access control. This digital certificate (and any optional digital certificates on the identity credential) must originate from:

- 1) An agency certification authority cross-certified with the Federal Bridge Certification Authority at medium assurance or higher by December 31, 2005; or
- 2) An approved Shared Service Provider.

Agencies must require the use of the identity credential for system access. Implementing Password Authority, with CAC authentication, as a front-end password management system to all other servers, devices and applications provides a rapid means of achieving compliance to the directive.

Cloakware Password Authority benefits include:

- > Auditable front-end access to all devices, systems and applications especially for those that do not support second-factor authentication mechanisms
- > Resolution of shared account usage to a unique, authorized ID
- > Broad Common Access Card vendor support via JAAS integration
- > Automated release of credentials to applications that execute on behalf of humans like automation scripts
- > Automated password management for devices, servers and applications to eliminate human knowledge of access information
- > Group-based access control to restrict which devices, servers and applications are accessible to a user
- > Role-based access control to restrict the capabilities available to a user
- > Password access policies including “change on view”, “dual approval”, “check out/in”, “help-desk ticket integration”
- > Complete audit reporting of all access and administrative activities

While many devices, servers and applications may support second-factor authentication there are many others that do not. With Cloakware Password Authority it is possible to allow all devices, servers and applications to continue to use the ID/password paradigm for access control but with Password Authority these ID/password pairs will be managed. Allowing devices, servers and applications to remain password based eliminates the retrofit effort and cost to enable smartcard authentication.

Automating the password change process for devices, servers and applications allows for frequent and regular changes according to the criticality of the specific system. Automating the process eliminates the human effort to implement the change, eliminates the potential for human error, and eliminates the knowledge of the then current password which increases the security of the system.

Password Authority delivers authenticated and authorized on-demand access to the current password required to connect to a system for both administrators and applications or scripts. Authenticating to Password Authority creates an audit record for the access activity which is then linked to the specific ID/password pair being accessed. Password access policies provide the additional granular controls over how and when a user can gain access to an account and password.

Binding the CAC supplied identity information to specific roles and groups with Password Authority limits the visibility and capability of the authenticated user to the systems under

ABOUT CLOAKWARE

Cloakware provides innovative, secure, proven software technology solutions that enable customers to protect business and digital assets in enterprise, consumer and government markets. The company has two main product lines: Cloakware Datacenter Solutions help organizations meet Governance, Risk Management and Compliance (GRC) objectives for privileged password management while ensuring business continuity and the security of mission-critical data and IT infrastructure. Cloakware Consumer Product Solutions protect software and content on PCs, set-top boxes, mobile phones and media players. Protecting more than one billion deployed applications today, Cloakware is the security cornerstone of many of the world's largest, most recognizable and technologically advanced companies. Headquartered in Vienna, VA and Ottawa, Canada, Cloakware has regional sales offices worldwide.

CONTACT INFORMATION

Corporate Headquarters

Cloakware Inc.
8219 Leesburg Pike, Suite 350
Vienna, VA, USA 22182
Tel. +1.703.752.4830

Canada

Cloakware Corporation
84 Hines Road, Suite 300
Ottawa, ON, Canada
K2K 3G3
Tel. +1.613.271.9446

www.cloakware.com



management. Roles and groups allows for adherence to the principles of lowest level of privilege and separation of duties.

Reporting of the access activity for the accounts under management provides the proof that accounts are being managed and released under the appropriate controls and policies as defined by the deploying organization.

Cloakware Password Authority can complement and accelerate your HSPD-12 compliance efforts. This paper discusses just a few of the benefits of the solution as they relate to HSPD-12. Please contact Cloakware for a more detailed explanation of our Password Authority solution.