

NOAA HSPD-12 Logical Access Control Policy

Purpose and Scope

The purpose of this policy is to define the roles and responsibilities on implementing the Homeland Security Presidential Directive 12 (HSPD-12) Logical Access Control (LAC) throughout NOAA. The HSPD-12 provides a secure and reliable form of identification for NOAA employees and contractors; it also establishes an official credential and accreditation process to enable rapid authentication electronically. Guidance from OMB further mandates all new logical and physical access control systems must be enabled to accept HSPD-12 credentials for authenticating Federal employees and contractors beginning in FY 2010. In FY 2011, agencies must use existing funding to upgrade existing physical and logical access control systems to use HSPD-12 credentials.

NOAA has been issuing DoD Common Access Cards (CAC), comparable with Personal Identify Verification (PIV) cards, since 2007. All eligible NOAA employees or the majority of contractors have received the new CACs as of today. Multiple attributes, including a digital certificate, about your Identity have been tied with your CAC. This certificate, nearly impossible to manipulate, is used to authenticate while you are accessing a NOAA computing resource. The goal of this HSPD-12 implementation efforts is to utilize a two-factor authentication method using your CAC and Pin for the network and internal web applications.

The implementation will include four main areas: Client configuration upgrade, Server/Domain Controller configuration upgrade, validation infrastructure establishment, and applications and Single Sign on (SSO).

1. Each client computer needs, at a minimum, to install a card reader (hardware), middleware (ActivClient), desktop certificate validator (software), and DoD and OCSP Root Certificates.
2. Each server or domain controller requires its own server certificate, DoD Root Certificates and enterprise validator installed.
3. A robust infrastructure including Online Certificate Status Protocol (OCSP) responders for providing signed validations from all clients, and an identity attribute authentication directory for authenticating NOAA identities or synchronizing with local domain controllers or directories has to be established.
4. Applications enabled with CAC certificate and SSO can be then addressed after prior three areas have been completed successfully.

This policy will impact all NOAA employees, contractors, vendors and agents with a NOAA-owned or personally-owned computer or workstation connected to the NOAA network. Further this policy applies to all end user initiated communications between NOAA's network and the Intranet web servers, or any services required an authentication process internally.

Authority

This policy is pursuant to and consistent with HSPD-12, OMB Passback 2010 and Memorandum M-06-16. Supporting documents include:

NOAA HSPD-12 Logical Access Control Policy

- (1) New Badge Requirements for Employees and Contractors, Office of Security at NOAA, 17 March 2009
- (2) Investigative Standards for Foreign Nationals Receiving HSPD-12 Compliant Smartcards and Related Processing Issues for Foreign Nationals and Contractors, 11 February 2009
- (3) NOAA HSPD-12 PIV-II Implementation Plan, 23 October 2007
- (4) Security Requirements for Getting a New NOAA ID Card, Office of Security at NOAA, 26 September 2007
- (5) Homeland Security Presidential Directive HSPD-12 PIV-1 Implementation And Suitability Processing POLICIES & PROCEDURE, 21 September 2007
- (6) Security Requirements for getting a NOAA ID Card, Office of Security at NOAA, 20 July 2006
- (7) NAO 212-13, NOAA Information Technology Security Policy
- (8) NOAA IT Security Manual 212-1300

Intended Audience

All NOAA Line Offices, Registration Authority (RA), Line Office or Local Registration Authority (LRA), System Administrators (SA), employees, temporary employees, contractors and agents are included.

Description

One of major computing deficiencies today is in the authentication method. When you enter your set of user ID and password to authenticate yourself, you believe nobody in the world would be able to guess the combination you had just entered. But think again. Since the information entered is in a digital form and transmitted over the network or internet, such information may be intercepted, copied, manipulated and replayed silently.

Authentication methodologies involve three basic factors:

- something you know (e.g., user ID, password, Pin);
- something you have (e.g., ATM card, smart card); and
- something you are (e.g., biometric characteristic, such as a fingerprint).

When you enter your user ID and password, password is the only protection for your account or identity. Authentication methods that depend on more than one factor are very difficult to compromise than single-factor methods. That is the obvious reason the banking industry adapted two-factor authentication method in 1967.

When you received your CAC, you had gone through the rigorous and accredited HSPD-12 credentialing process. The Pin, you were asked to enter, is equivalent to the ATM PIN, which can unlock your identity for authentication purposes. This secure identity in the same analogy can be used to access network, network drives, printers, email, web applications and other NOAA applications. If you forget about your Pin, you can get it reset at any Real-time Automated Personnel Identification System (RAPID) or Pin Reset stations using your fingerprints.

NOAA HSPD-12 Logical Access Control Policy

1. On the client side, each client device needs to have a smart card reader, which communicates with the CAC and unlocked your identity credential. ActivClient is the middleware, a crypto service provider, managing all encryption between the card and authentication requests. If the certificate on a CAC is unexpired and generated from the same root certificate, the revocation status of the certificate is next to be examined. A certificate validator is required to check the revocation status of a certificate. As a result, DoD and OCSP root certificates need to be loaded into the device certificate trust store so all authentication processes in the background are signed and trusted.
2. Servers and domain controllers need server certificates. These certificates have to be requested by system administrators with approvals from the Line Office/Local Registration Authority (LRA). These certificates also call device certificates, which identify themselves as trusted identities in the process. When a client requests access to a server or domain, the responding server will authenticate the client credential by validating its certificate. Likewise, the client also authenticates the server's identity at the same time. It is a two-way process. An enterprise validator or repeater is required for checking the status of the client certificate on a server or domain controller. Servers and domain controllers also need the same DoD and OCSP root certificates as those installed on the clients.
3. The authentication infrastructure mainly includes an Identity authentication directory and a redundant OCSP responder cluster. OCSP responders actually validate and respond to the revocation status requests from desktop validators. When a validator forwards its request to OCSP responders, responders have to respond quickly back to the validator. If the forwarding responder is not answering, the request will be forwarded the next responder. If none of the responders were available, the authentication process would fail between the server and client. And no access is allowed. The identity authentication directory designed to authenticate each NOAA user maintains several common attributes on a CAC including:
 - a. Last Name
 - b. Phone number
 - c. Street address
 - d. Email Address
 - e. EDIPI
 - f. Pubic Key Certificate

Based on these attributes, a CAC holder can be specifically authenticated as a NOAA CAC holder, not CAC belongs to other DoD franchises. These attributes can be synchronized with a NOAA CAC open directory for domain authorization proposes.

4. Internal web applications including IIS, Apache, and others may be easily transitioned to the certification authentication method with installation of an Access Manager extension. In addition, a web server needs DoD and OCSP root certificates, and OCSP web server extension loaded in the system for authentication purposes. Client and server based or legacy applications would need a SSO agent on each client to leverage the credential on the CAC. The majority of legacy servers or services are not CAC enabled.

NOAA HSPD-12 Logical Access Control Policy

Roles and Responsibility

NOAA CIO/CFO council aids the project manager in lining up, getting commitment from, and managing cross-functional support resource needs; manages project funding shortfalls and validation and efforts to secure external funding; and ensure project is tracking to budget, performance and schedule; and review and approve project progress reports.

Line Office is responsible for client and server implementation requirements, contributes to the project funding, helps the project manager navigate the organization's political environment and prioritizes applications for CAC enablement, affirms project manager officially, provides official backing of the project, communicates project closure and results to organization, acts as an escalation route for the project manager, arbitrates and resolves conflict and interface problems that the project manager escalates.

Line office/Local Registration Authority (LRA) determines LAC requirements for each Line Office, schedule field implementation requirements and priorities, coordinates the Line Office fielding schedule, completes DISA LRA certification training (held monthly), certifies Line Office system administrators for requesting and revoking server certificates and others, assists Registration Authority (RA) in identifying and revoking server certificates no longer in use and provides an HSPD-12 implementation monthly progress report.

Office of IT Security Office (ITSEC), the Project Manager, is responsible for standing up the authentication infrastructure, assists each Line Office and field offices enabling CAC authentication, provides guidance and facilitates any piloting efforts, develops a NOAA HSPD-12 implementation plan, performs RA functions and issues device certificates for servers and signing certificates for OCSP responders, leads the application conversion and SSO efforts, and reports HSPD-12 progress to the CIO/CFO council.

Exceptions

Any domain controllers or internal web servers will implement CAC two-factor authentication by FY11. Any exceptions to this policy will be reported to OMB.

Enforcement

The IT Security Office will report the progress to the CIO or CFO council monthly.

Compliance

Compliance will be gauged through automated audits as directed by the NOAA CIO.

Definitions

Authentication - the process of determining whether someone or something is, in fact, who or what it is declared to be. In computer networks (including the Internet), authentication is commonly done

NOAA HSPD-12 Logical Access Control Policy

through the use of logon passwords. Knowledge of the password is assumed to guarantee that the user is authentic.

Certificate - A digital certificate is an electronic "credit card" that establishes your credentials when doing business or other transactions on the Web. It is issued by a certification authority (CA). It contains your name, a serial number, expiration dates, a copy of the certificate holder's public key (used for encrypting messages and digital signatures), and the digital signature of the certificate-issuing authority so that a recipient can verify that the certificate is real.

Certificate Authority (CA) – A system authority in a network issues and manages security credentials and public key for message encryption. As the major part of a public key infrastructure (PKI), a CA checks with a registration authority (RA) to verify information provided by the requestor of a digital certificate. If the RA verifies the requestor's information, the CA can then issue a certificate.

Registration Authority (RA) – An individual approves certificate requests on CA by system administrators. Certificates are then installed on servers as their electronic credential.

Line Office/Local Registration Authority (LRA) – An individual verifies and ensures that system administrators requesting server certificates within his or her Line Office are trust worthy and gone through the rigorous HSPD-12 process.

Root Certificate – A self-signed certificate that identifies the Root CA. A root certificate is top of the chain of trust. It is used to affiliate or verify digital certificates within the same chain of trust.

Validator – It is short of Validation Authority (VA) validator, which sends a validation request or inquiry to a VA responder to confirm the revocation status of a certificate.