



Achieving Compliance

Over the years, the methods by which employees and contractors of government agencies have identified themselves have been as diverse as the agencies they represent. Such inconsistencies can threaten the security of an agency's people, facilities and assets.

That's why HSPD-12 calls for a common identification and verification standard for federal employees and contractors. FIPS 201 outlines a specific approach for compliance with the directive, requiring the creation and issuance of a common identification credential that is interoperable and can also be used for applications such as physical and logical access control.

Diebold CredentialOne can help you build the infrastructure to enable FIPS 201 compliance. Whether you need assistance with start-up or management support for implementation, CredentialOne is fully customizable to your agency's unique needs. Diebold can partner with you on any element of your FIPS 201 program or we can help manage your program for you from start to finish.

Evaluating Your Current System

Evaluation is the first step of any security strategy. As you build your identity management strategy, it is vital to evaluate your current system and identify its role in your HSPD-12-compliant program. Diebold can help you incorporate legacy equipment into your new program, and our experts can ensure the effective convergence of your physical and logical systems.

Understanding Factors of Identity Authentication

A variety of factors can be used to verify and authenticate a person's identity. The more factors you use, the more assurance you have that a person is who he or she claims to be. As you increase the number of factors required to prove identity, you simultaneously increase the level of assurance or confidence in that identity. Identity authentication assurance level is often referred to in terms of how many factors are required to prove identity – most commonly, single-factor, two-factor or three-factor authentication.



Four categories of unique information can be used to establish an identity and then authenticate it: something you are, something you know, something you have and something you are assigned. Diebold recommends capturing as many details or versions of these factors as possible when enrolling an individual in an identity and access management program. Even if your organization isn't planning to use every factor during the initial phase of the program, capturing multiple factors and multiple versions of each factor during the enrollment process can save time and can ensure a variety of information is available for future program expansion. For example, when capturing biometrics, consider capturing multiple modes of distinguishable personal characteristics, even if your agency will only use one biometric mode for identity verification and authentication.

SOMETHING YOU ARE

Any personal characteristic that can be distinguished – your fingerprint, iris, retina, face, voice, DNA, handwriting, etc. – can be used as a factor of identification. These personal traits are commonly referred to as biometric factors.

SOMETHING YOU HAVE

At their very core, HSPD-12 and FIPS 201 are about marrying something you have (the credential) to one or more of the other factors of identification for the purpose of verifying and authenticating the claimed identity. Any object in your possession that can be used as an identifier can be considered something you have. Often referred to as a token, the identifying object is most commonly a card, but can also be a number of other items.

SOMETHING YOU KNOW

The possession of distinct knowledge also can be used as a factor of identification. Examples of such knowledge include Personal Identification Numbers (PINs), passwords or a mother's maiden name.

SOMETHING YOU ARE ASSIGNED

Information or characteristics that are assigned are often the most basic of identity details. Examples include your name, title, Social Security Number, address or other basic biographic information. The other three factors are typically used to validate or authenticate this assigned identity claim.





Navigating the Process

Diebold CredentialOne can include a basic provisioning service, such as PIV or CAC enabling a PACS for physical access control based on the smart card identity data elements, or a complete, turnkey FIPS-201 compliant solution with an extensible and scalable system infrastructure platform. The platform includes processes and components for establishing personal identity and managing credential issuance and systems – provisioning for multiple usage. The FIPS 201 process steps include:

STEP 1: SPONSORSHIP

A qualified individual (an employee or contractor of your agency) in need of a credential is provided a means of entering his or her application into the system by a vetted and approved sponsor.

STEP 2: PRE-ENROLLMENT

A Web-based pre-enrollment process is provided to capture biographic data (name, address, Social Security number, etc.) via online enrollment forms. The applicant enters his or her information and submits the application for the sponsor's approval.

STEP 3: SPONSOR APPROVAL

A vetted and approved sponsor or trusted agent reviews and either approves or rejects the applicant's pre-enrollment application.

STEP 4: REGISTRATION

Once an application is approved, the applicant is directed to an enrollment station where a trusted agent authenticates documents, captures unique biometric data and transmits the captured data to an Identification Management System (IDMS) for secure storage.

STEP 5: PROOFING AND VETTING

Various specialized databases, systems and services are used to perform background checks. Using up-to-date information, an applicant's request is validated and he or she is either granted or denied a credential. Adjudication officers process any indeterminate findings.

STEP 6: AUTHORIZATION OF ISSUANCE

The IDMS then issues a card production request to the Card Management System (CMS). IDMS forwards a card production package, also referred to as the "payload," containing all biographic and biometric data to the CMS.

STEP 7: CHUID GENERATION

The CMS receives the card production package from the IDMS, which generates the Card Holder Unique Identifier (CHUID) and sends the data field contents to the Card Production System (CPS) for either outsourced centralized card production and/or on-site distributed card printing.



STEP 8: CARD PERSONALIZATION

The unique and electronically bonded personal identity credential is produced by combining the biographical, biometric and digital keys to create a unique token that uniquely links the individual and the “personalized” credential data. Card personalization is now performed either through a centralized or distributed process.

STEP 9: CARD ISSUANCE

The applicant appears at a card issuance station where his or her identity and associated details are validated and the card is activated with the public key infrastructure (PKI) certificate from the certificate authority, and a unique private key and a Personal Identification Number (PIN) are now assigned. The electronic personalization process typically occurs at the time of issuance.

STEP 10: CARD USAGE

The unique smart card credential can now be associated with physical access control privileges, logical access control privileges or a variety of other configurations determined by the security manager.