U.S. Department of Agriculture

HSPD 12 Program

HSPD-12 Implementation at USDA

Personal Information Security Protections for HSPD-12 ID Card and System

July 27, 2006

Why Are We Discussing Privacy and Security?

Personal data compromises have been a recent regular news item. In addition, the latest HSPD-12 readiness survey indicated there are a number of concerns regarding the security and privacy of personal information.

- What happens if my LincPass is lost or stolen?
  - **Can my identity be stolen?**
  - **Is my credit rating at risk?**
  - **Will my Agency's data be at risk?**

- Who is managing/controlling the shared enrollment stations?
  - **How is my data protected from others?**
  - **Will other Agencies/Departments have access to my personal data?**

What Will We Cover in This Presentation?

This special topic on Personal Information Security Protections for HSPD-12 ID Card and System is intended to address:

- What elements of personal information are stored on the LincPass and within the HSPD-12 system;
- How that information is secured;
- How that information will be used; and
- Centralized management of the HSPD-12 enrollment stations.

Why does HSPD-12 require my information?

The HSPD-12 system requires specific personal information about you in order to:

- Begin the sponsorship process for the LincPass;
- Provide required information for the Federal Bureau of Investigation (FBI) background check;
- Provide LincPass issuer with confirmation that background investigations are complete;
- Notify you of LincPass card issuance; and
- Populate your LincPass with USDA-required information.

What types of personal information are required?

Here are some examples of elements of your personal information that the HSPD-12 will require in order to obtain and manage a LincPass:

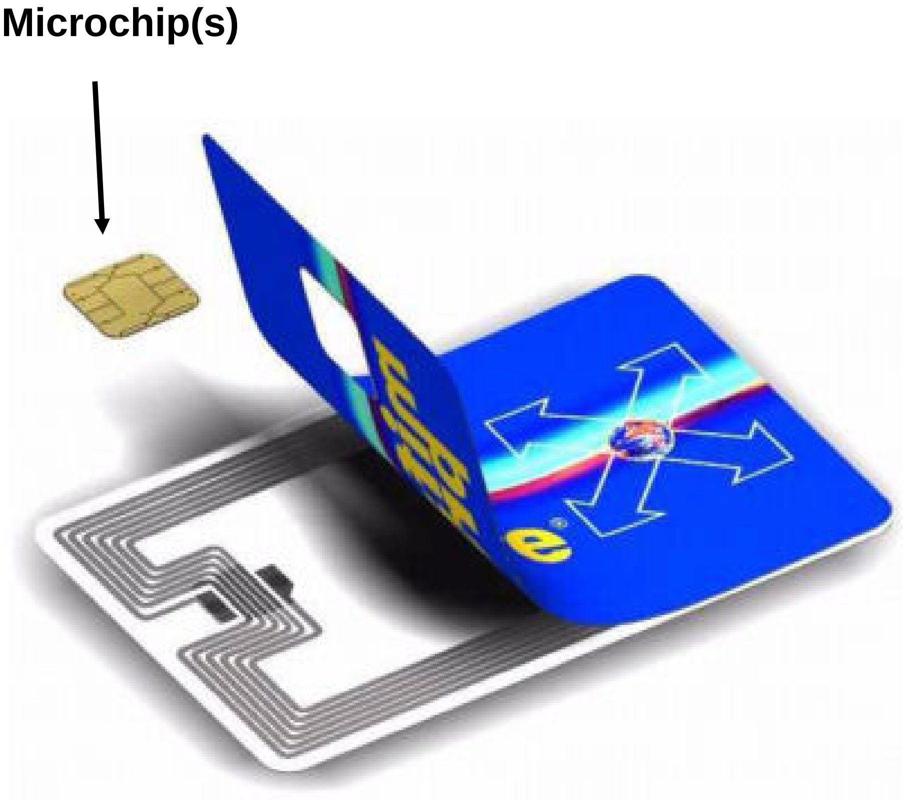
- Elements of employment status (e.g., employee ID; employee type (employee, contractor); citizenship status; Agency; occupational series; work email)
- Elements of identifying information (e.g., full name; SSN; birth date and place; gender; home address)
- Elements of information regarding the status of your Background Investigation (e.g., NACI adjudication status (successful/unsuccessful); e-QIP tracking number)

What other information is stored on the LincPass?

The LincPass is based on “smart card” technology. Next, we’ll cover two key elements of the card and explain how each is secured.

- ❑ Biometrics
- ❑ Personal Identification Number (PIN)
- ❑ Digital Certificates

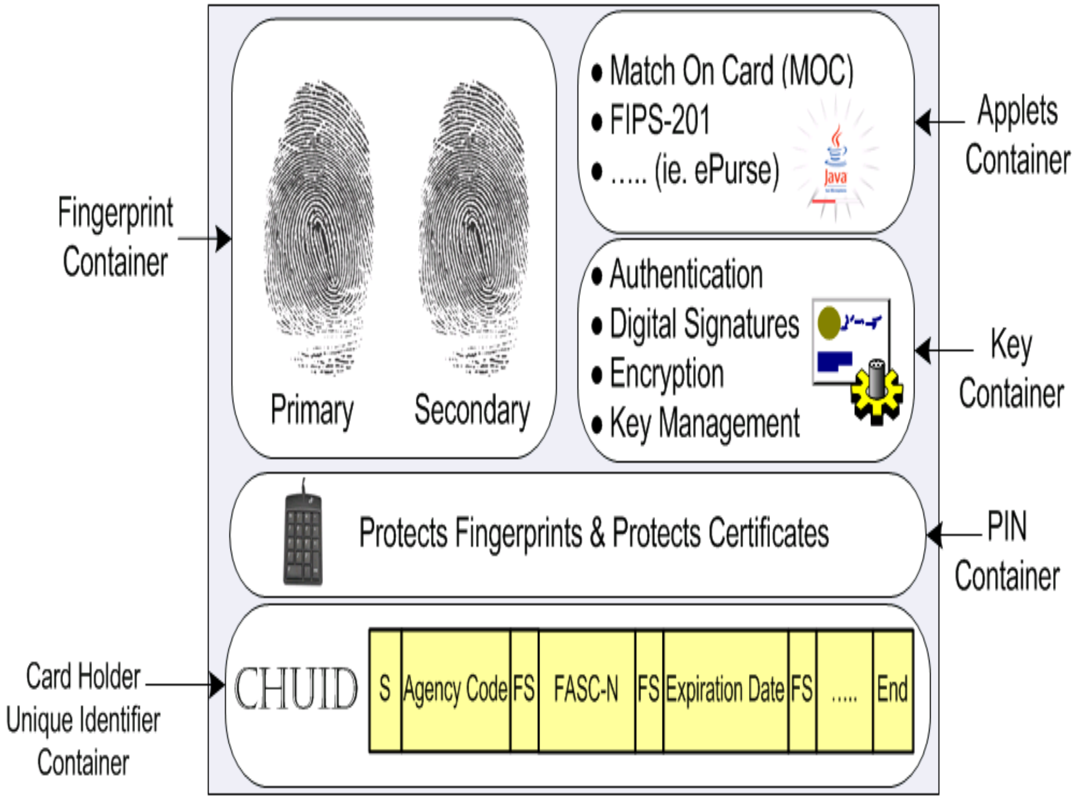
What is a smart card?



The LincPass is based on smart card technology.

- A smart card is a card containing one or more computer – readable microchips.
- These microchips contain data, such as cardholder identifying data and expiration date.
- The information on the microchips are centrally managed, so they can be deactivated immediately if lost or stolen, rendering them inoperable.
- The HSPD-12 technical standards requires technical interoperability among all Federal Departments.

What information is on the microchip?



Example of information contained on microchip

The microchips contain information about you.

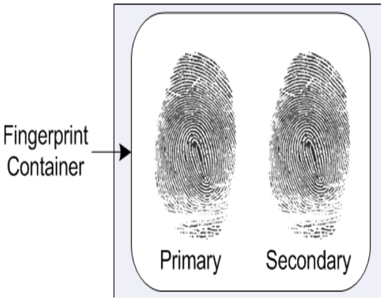
We'll review 3 types of information, how they are protected, and how they are used in HSPD-12.

- ❑ Fingerprints;
- ❑ Personal Identification Number (PIN);
- ❑ Digital certificates/keys;

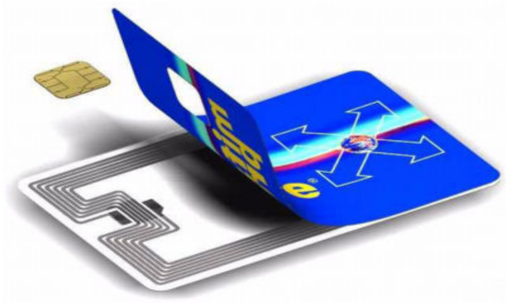
About: Fingerprints

Fingerprints Scanned

Two fingerprints captured



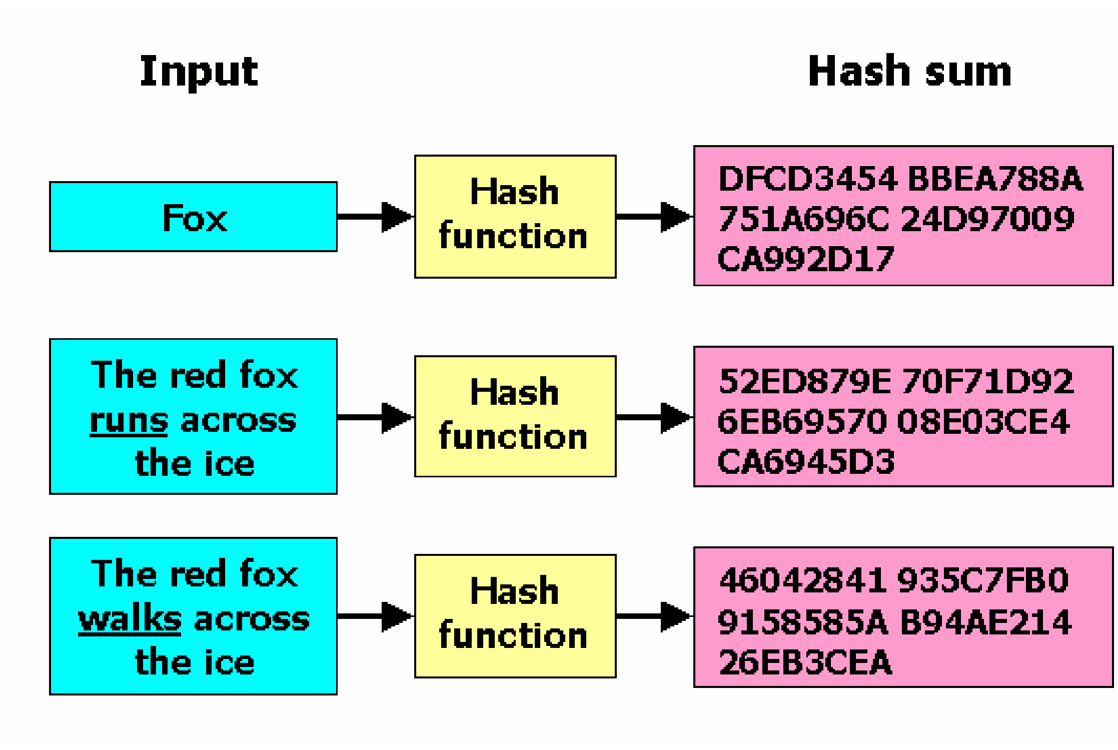
Fingerprints stored on smartcard microchip



HSPD-12 Personal Identity Verification (PIV) standards require biometric information be stored on the card:

- ❑ Biometrics refers to measurable physical characteristics that can automatically be checked by a device or application.
- ❑ PIV standards require two fingerprint captures to be stored on the LincPass.

How the Biometrics are Secured


Input
Hash sum
Fox
Hash function
DFCD3454 BBEA788A 751A696C 24D97009 CA992D17
The red fox runs across the ice
Hash function
52ED879E 70F71D92 6EB69570 08E03CE4 CA6945D3
The red fox walks across the ice
Hash function
46042841 935C7FB0 9158585A B94AE214 26EB3CEA

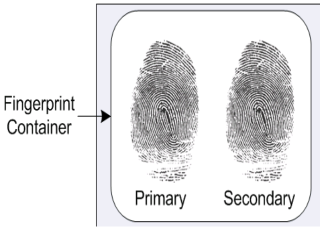
Graphic courtesy of Wikipedia

The fingerprint data is converted via a “hash” function (mathematical algorithm) into a long string of random-looking letters and numbers.

- ❑ Note that the hash sums are the same size, no matter how long or short the input.
- ❑ Also, the hash sums look very different even when there is only slight differences in the input.
- ❑ Hash algorithms cannot be reversed.

How Biometrics Are Used

Fingerprints stored on card



↓

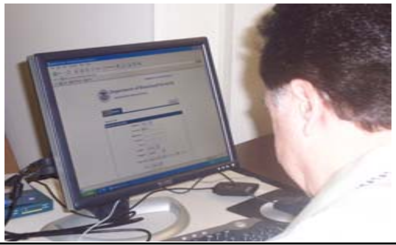
Finger scanned via fingerprint scanner

↓

Computer matches fingerprints when accessing computers/buildings

↓

Access granted if fingerprint images match



How your fingerprints will be used:

- Your hashed fingerprint images stored on the card can be compared to a fingerprint image captured real-time via a fingerprint scanner that is attached to a door or to a computer.
- If the real-time image matches one of the fingerprint images stored on the card, your identity is authenticated. This capability is known as “match-on-card.”

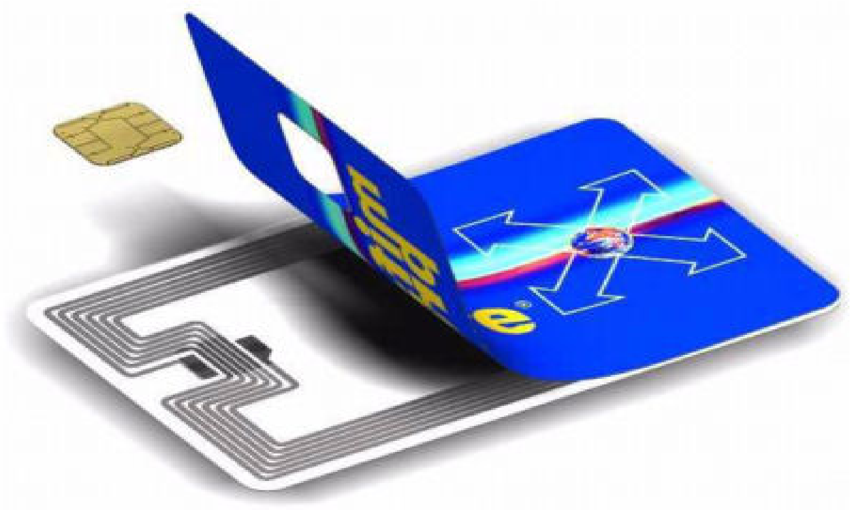
About: Personal Identification Number (PIN)

PIV standards require use of a Personal Identification Number (PIN):

- ❑ Creation and use of PIN activates your LincPass.
- ❑ Your PIN provides an additional factor of authentication (“something you know”) to control access to information on the card.

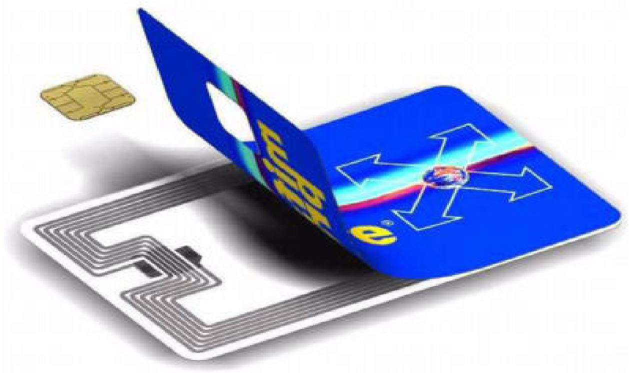
How the PIN Is Secured

Security of your PIN is the same as for your fingerprints:



- The PIN you generate will be stored on the smart card microchip in a hashed format.
- PIN entries are limited; the card is “locked” if user exceeds preset limit of attempts.
- User must go through procedure to reset card.

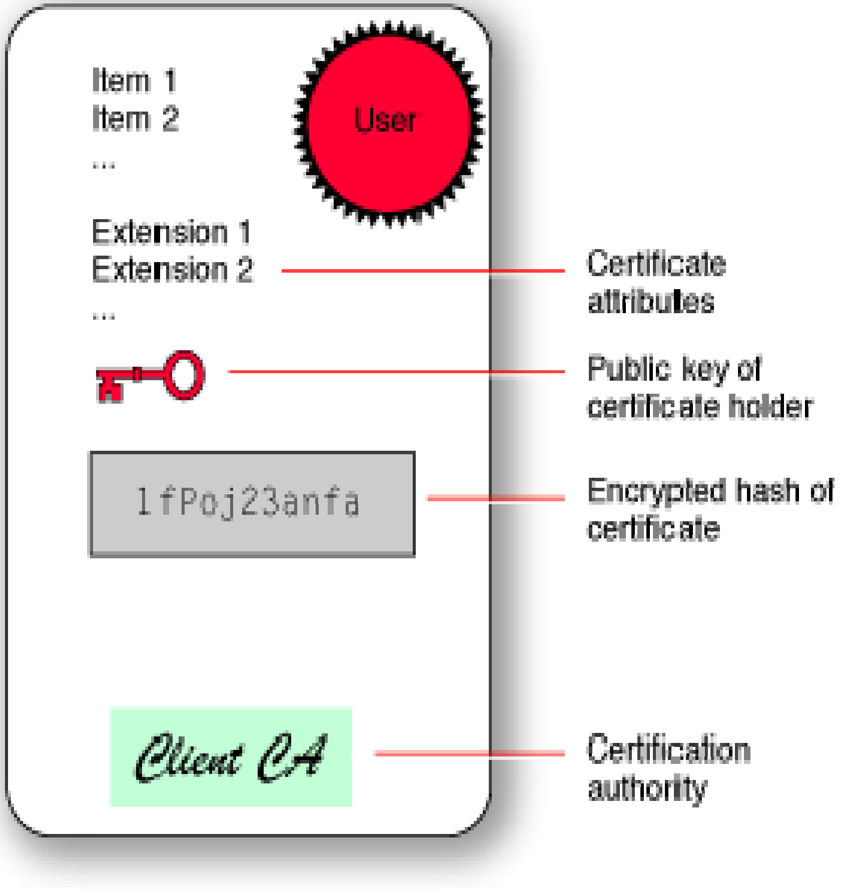
How the PIN is used



The PIN is used to control the ability to unlock the information on the card

- In essence, you are proving your identity to the card.
- The HSPD-12 system compares the PIN you enter into the keypad with the PIN you have stored on your card's microchip. If the two PIN's match, your identity is authenticated.
- Your biometric info is only accessible with the PIN.

About: Digital Certificates



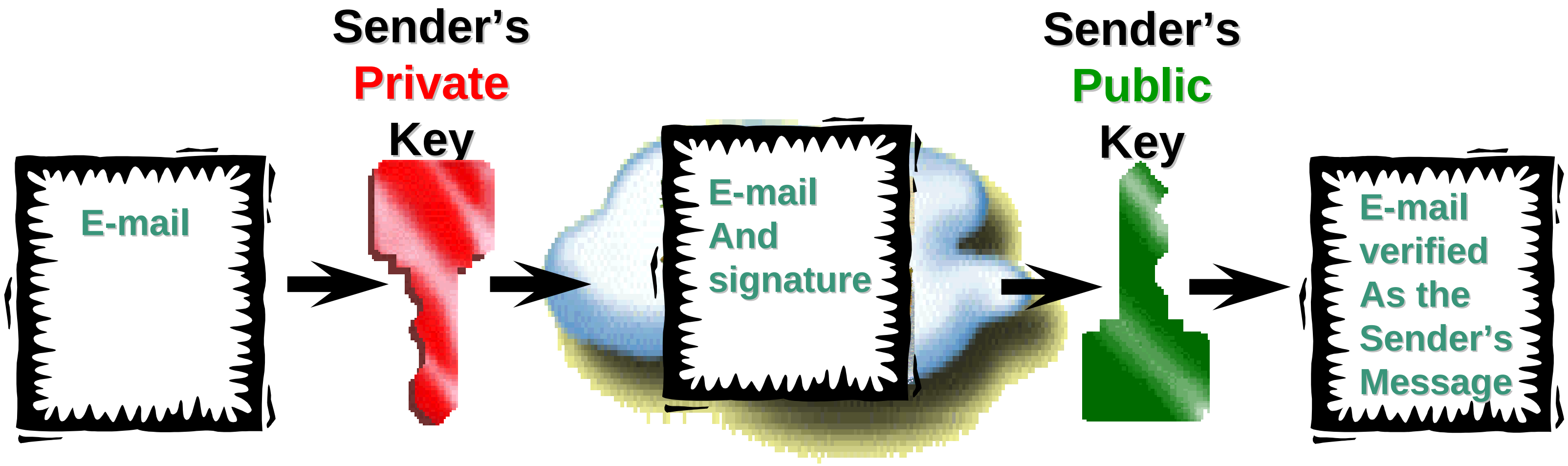
A digital certificate is a digital form of identification, much like a passport or driver's license.

- The digital certificate includes:
  - **Your name;**
  - **A unique identification number;**
  - **An expiration date;**
  - **A copy of the certificate holder's public key; and**
  - **The digital signature of the certification authority.**

How Digital Certificates secure documents

Digital Certificates allow you to electronically ‘sign’ documents, and encrypt files. This is done through the use of a KEYPAIR, one public key and one private key.

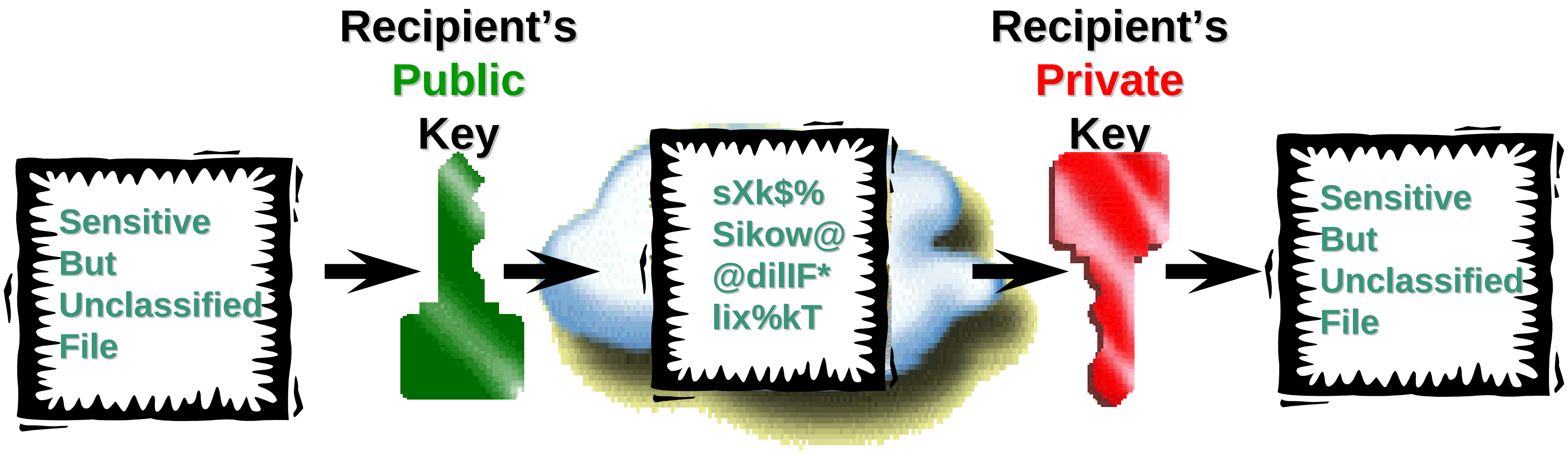
Signing a document:



What is signed with one key,
can only be *verified* with the other key.

How Digital Certificates secure documents, cont.

Encrypting a document:



Sensitive But Unclassified File

Recipient's **Public** Key

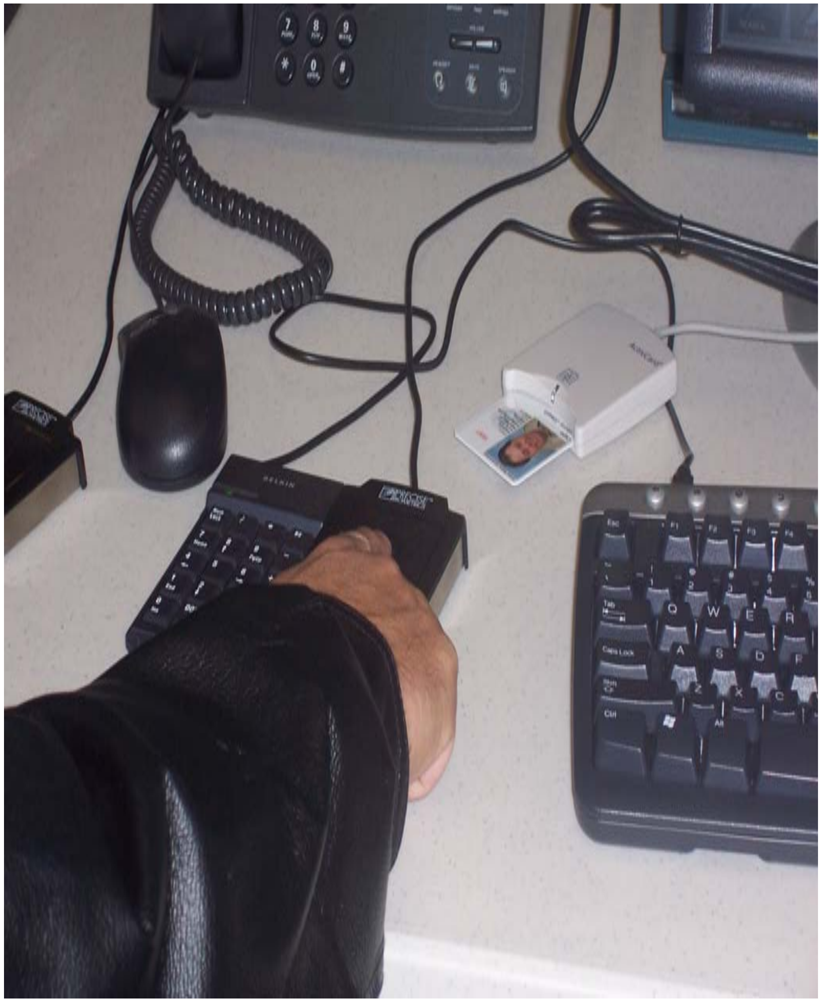
sXk$%
Sikow@
@dillF*
lix%kT

Recipient's **Private** Key

Sensitive But Unclassified File

What is encrypted with one key,
can only be decrypted with the other key.

How the Digital Certificates are Used



There are several potential uses for digital certificates on a smart card:

- ❑ Authentication for physical or logical system access;
- ❑ E-mail encrypting; and
- ❑ Digital signing.

FIPS 201-1 specifies that the LincPass is required to have a PIV authentication key for use of physical and logical access systems.

Additional uses of digital certificates are left for Departments and agencies to determine.

Why is all this information needed?

HSPD-12 was mandated in order to strengthen the government’s ability to authenticate the identity of who it employs and who is allowed access to Federal buildings and computer systems.

- We now have a common standard for identity authentication across the Federal government.
- The LincPass will support a variety of identity authentication mechanisms across Departments and Agencies.
- Once a person’s identity is authenticated, authorizations can be assigned for physical (i.e., building) and logical (i.e., computer) access systems.

What is Authentication?

Authentication using PIN, biometrics or certificate on card.

Authentication is the process of determining whether someone actually is who he or she declares to be:

- ❑ It assigns a degree of confidence one can have on another’s identity;
- ❑ It is needed to make secure and reliable access control decisions; and
- ❑ It can be strengthened by providing two or more factors (i.e. PIN + biometrics).

How Authentication Strengthens Identity Assurance

Biometrics along with PKI will allow USDA employees Physical and Logical access. This access will provide stronger identity and security assurance levels.

Physical Access: Allows access into USDA and other departmental buildings.

Logical Access: Allows access to computer systems.

Factors of Authentication	**Physical**	**Logical**
Something you have	PIV Card	PKI Certificate
Something you know	PIN (unlocks fingerprint)	PIN (unlocks fingerprint/certificate)
Something you are	Fingerprint	Fingerprint

What is Authorization?

Authorization is the process of giving someone permission to do or to have something:

- ❑ It is a means to determine if one can access certain facilities after they have been authenticated and approved;
- ❑ It determines what buildings you have access to and what is permissible to view on a computer system; and
- ❑ It is determined by individual agencies through policies and system administration definitions.

A LincPass Scenario

Now let's bring the Personal Identity Verification concepts of Authentication and Authorization together by reviewing a scenario using the LincPass:

Sally is a USDA employee. Her Agency's Physical Access Control System defines her as having authorized access to:

and

Building A

The Operations Center in Building A

Let's see how Sally uses her LincPass to gain access to the building and the secured room…

A LincPass Scenario, cont.

In order to gain access to Building A…

Sally uses her LincPass in a card reader

The Physical Access Control System authenticates Sally's identity information stored on the LincPass and confirms her authorization to access Building A

Sally is able to enter Building A

A LincPass Scenario, cont.

In order to gain access to the Operations Center in Building A, which requires a higher level of identity authentication…

Sally uses her LincPass in a card reader

Sally enters her PIN number on the keypad

The Physical Access Control System authenticates her identity information on the LincPass, compares her stored PIN to the PIN she just supplied, and confirms her authorization to access the Operations Center.

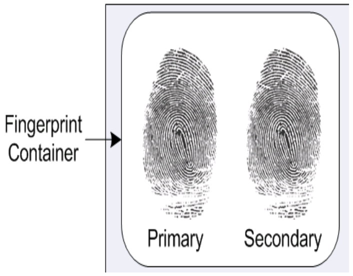
Sally is able to enter the Operations Center

Card Security Summary

UNITED STATES
GOVERNMENT
DEPARTMENT
OF COMMERCE
NIST
JOHN J. SMITH
John J. Smith
Department Official
DEPT OFFICIAL
Issued
01/05
Expires
12/05
USANIST0000000000000
USADOCNIST000000000000000000000
Height
5'10"
Weight
150lbs
Eyes
Brown
Hair
Brown

This card and the information on this card is confidential property of the United States Government. If found please drop into the nearest post office to the address below. Misuse or abuse of this card is a violation of some Section of some article of the U.S. code.

This card and the information on this card is confidential property of the United States Government. If found please drop into the nearest post office to the address below. Misuse or abuse of this card is a violation of some Section of some article of the U.S. code.



- ❑ Smart Card technology
  - Stores information in the form of one-way hash values
  - Compares authentication methods ‘on the card’
- ❑ Digital Certificates
  - Allows you to verify and trust the sender
  - Allows for encryption of Sensitive files
- ❑ PIN and Fingerprints
  - Allows for multiple-factor authentication in both physical and logical access methods.
- ❑ Centrally managed
  - Allows for cards to be deactivated immediately

HSPD-12 System Security

There are a number of security requirements for processes that are part of the Card Issuance and Management Subsystem of HSPD-12. These requirements are guided by:

- Office of Management and Budget (OMB) Circular No. A-130 (Management of Federal Information Resources) computer security controls;
- Federal Information Security Management Act (FISMA);
- National Institute of Standards and Technology (NIST) publications;
- Certification and accreditation (C & A) requirements; and
- NIST plans to conduct reviews of the enrollment stations to ensure adequate controls are in place.

Additional Reading

- **HSPD-12**, Policy for a Common Identification Standard for Federal Employees and Contractors
- **OMB M-05-24**, Implementation of HSPD 12 - Policy for a Common Identification Standard for Federal Employees and Contractors
- **FIPS 201-1**, Personal Identity Verification for Federal Employees and Contractors
- **SP 800-37**, Guide for the Security Certification and Accreditation
- **SP 800-53**, Recommended Security Controls for Federal Information Systems
- **SP 800-73**, Interfaces for Personal Identity Verification
- **SP 800-76**, Biometric Data Specification for Personal Identity Verification
- **SP 800-78**, Cryptographic Algorithms and Key Sizes for Personal Identity Verification
- **SP 800-79**, Guidelines for the Certification and Accreditation of PIV Card Issuing Organizations
- **SP 800-85**, PIV Middleware and PIV Card Application Conformance Test Guidelines (Revision to permit transitional and end-point issuance system conformance certification)