

Information Security and Privacy Board

Background and current status

- *Use of Hashing Algorithms in the U.S. Federal Personal Identity Verification Program*
- *Biometrics Storage Format Selection for the U.S. Federal Personal Identity Verification Program*

Curt Barker

December 2005

Topics

- ❑ General Status of U.S. Federal Personal Identity Verification Program
- ❑ Use of Hashing Algorithms in the U.S. Federal Personal Identity Verification Program
 - Processing Concept
 - Programmed Changes in Key/Hash Size Requirements
 - Other Uses of Hashes
- ❑ Biometrics Decision for Special Publication 800-76
 - Minutiae-based vs Image-based Storage
 - SP 800-76 Biometrics Storage Formats
 - Conformance Determination

Topics

- ❑ General Status of U.S. Federal Personal Identity Verification Program
- ❑ Use of Hashing Algorithms in the U.S. Federal Personal Identity Verification Program
 - Processing Concept
 - Programmed Changes in Key/Hash Size Requirements
 - Other Uses of Hashes
- ❑ Biometrics Decision for Special Publication 800-76
 - Minutiae-based vs Image-based Storage
 - SP 800-76 Biometrics Storage Formats
 - Conformance Determination

Phased-Implementation In Two Parts

- ❑ Part 1 – Common Identification and Security Requirements
 - ❑ HSPD 12 Control Objectives
 - ❑ Identity Proofing, Registration and Issuance Requirements
 - ❑ Effective October 2005
- ❑ Part 2 - Common Interoperability Requirements
 - ❑ Detailed Technical Specifications
 - ❑ Office of Management and Budget made Effective October 2006 (OMB M-05-24)
- ❑ Migration Timeframe (i.e., Phase I to II)
 - ❑ Agency implementation plans have been provided to OMB
 - ❑ OMB has issued schedule for full implementation in 2009

Implementation Status and Current Actions

- ❑ Revision to FIPS 201 (FIPS 201-1)
 - Interim Issuance Based on National Criminal History Check
 - Electronic Indication of Interim Status
- ❑ Conformance Testing of Cards Built to FIPS 201/SP 800-73 Currently Underway
 - Card Interfaces
 - Card Storage Formats
 - Middleware Interfaces
- ❑ Formal NVLAP Accreditation of NPIVP Laboratories Underway

Topics

- ❑ General Status of U.S. Federal Personal Identity Verification Program
- ❑ Use of Hashing Algorithms in the U.S. Federal Personal Identity Verification Program
 - Processing Concept
 - Programmed Changes in Key/Hash Size Requirements
 - Other Uses of Hashes
- ❑ Biometrics Decision for Special Publication 800-76
 - Minutiae-based vs Image-based Storage
 - SP 800-76 Biometrics Storage Formats
 - Conformance Determination

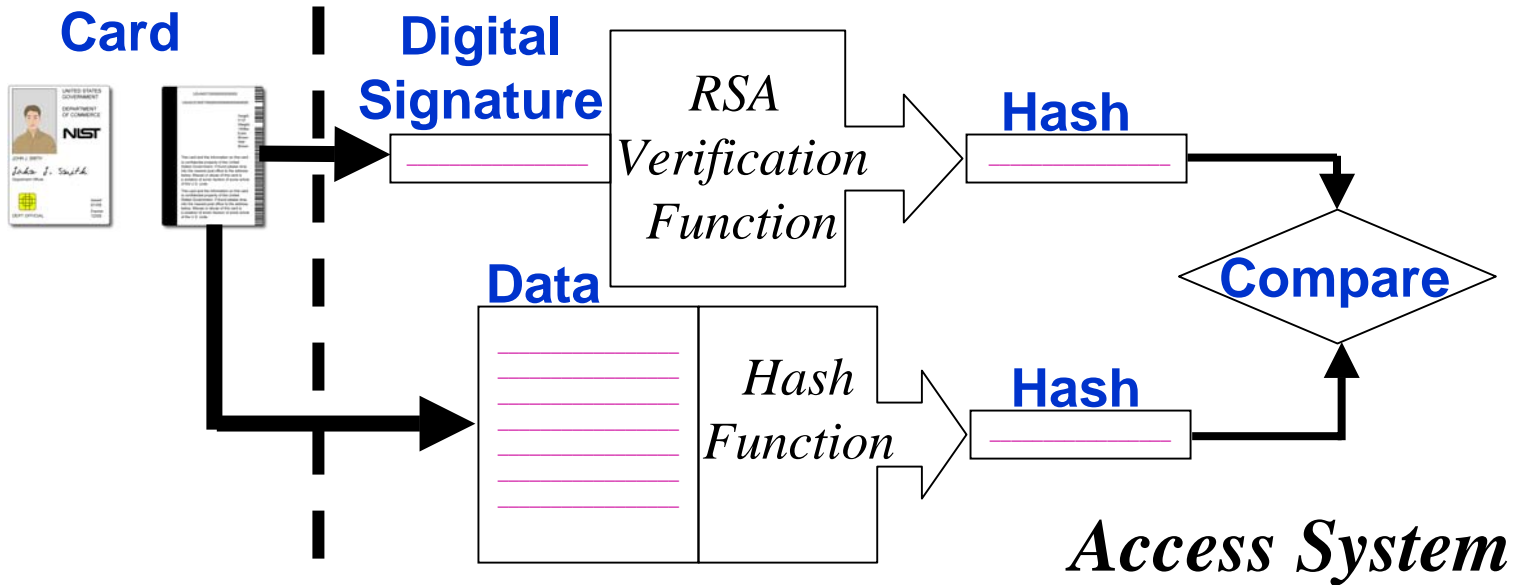
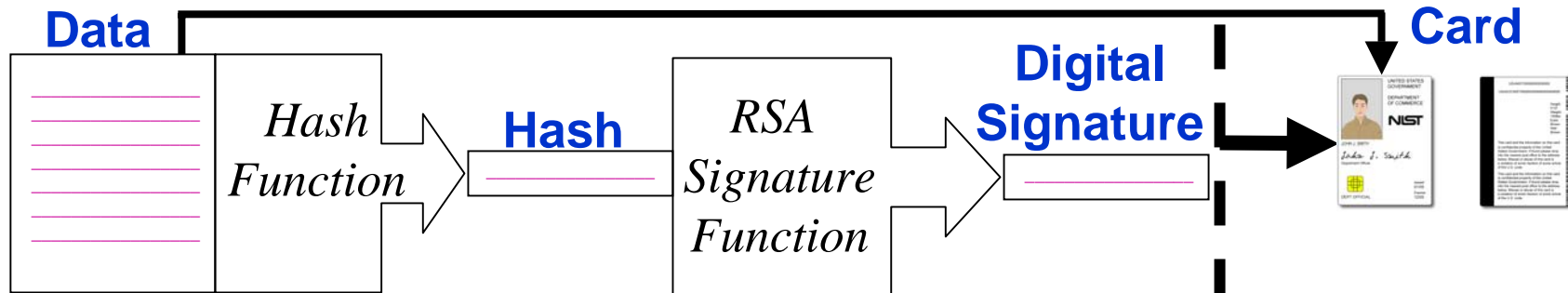
Cryptographic Algorithms and Key Sizes for Personal Identity Verification

SP 800-78 specifies:

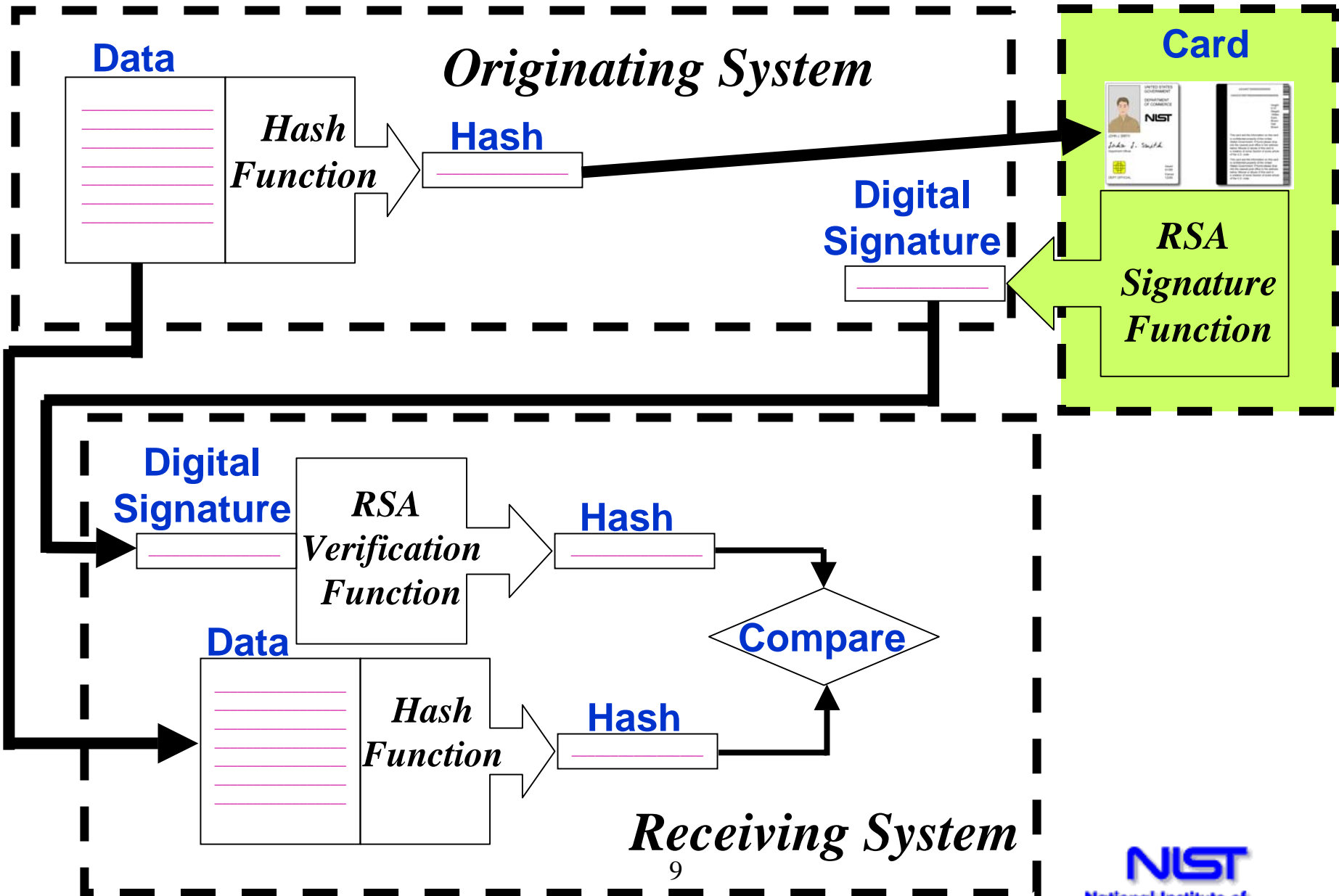
- ❑ Mandatory PIV Authentication Data (asymmetric key pair and corresponding PKI certificate)
- ❑ Optional Keys
 - Asymmetric key pair and corresponding certificate for digital signatures
 - Asymmetric key pair and corresponding certificate for key management
 - Asymmetric or symmetric card authentication keys for supporting additional physical access applications
- ❑ Cryptographic Algorithms and Key Sizes
- ❑ Authentication Information Stored on the PIV Card

Hashing Concept (Data Stored on Card)

Issuance System



Hashing Concept (Card Signs Data)



Cryptographic Algorithms and Key Sizes for Personal Identity Verification

SP 800-78 specifies:

- ❑ Digital Signatures for Card Holder-Unique ID, Stored Biometric Information, X.509 Certificates, “Security Object” that Includes these Identifying Information
- ❑ Expiration of SHA-1 Hash Algorithm and 1024 bit RSA After 12/31/2010

Other SHA-1 Uses

- ❑ Broader use of SHA-1 by the Federal PKI for the implementation of digital signatures.
- ❑ Default hash algorithm used in the creation of signatures on all certificates issued by Federal PKI CAs. SHA-1 is used (along with MD5) in the NIST National Software Reference Library.
- ❑ Hash algorithm used for certificates and other signed objects on CAC cards.
- ❑ SHA-1 is used in many other Federal applications, since it has been the recommended, FIPS-approved hash function for years.

Topics

- General Status of U.S. Federal Personal Identity Verification Program
- Use of Hashing Algorithms in the U.S. Federal Personal Identity Verification Program
 - Processing Concept
 - Programmed Changes in Key/Hash Size Requirements
 - Other Uses of Hashes
- **Biometrics Decision for Special Publication 800-76**
 - Minutiae-based vs Image-based Storage
 - SP 800-76 Biometrics Storage Formats
 - Conformance Determination

Biometric Data Specification for Personal Identity Verification

Biometrics Decision for Special Publication 800-76

- Minutiae-based Rather Than Image-based Storage
- SP 800-76 Biometrics Storage Formats
 - ANSI/INCITS 378
 - EER Compatible With TSA Requirement
- Conformance Determination
 - MINEX?
 - NPIVP?

Thank you.

Questions....

Contact Information:

Curt Barker

wbarker@nist.gov

301-975-8443