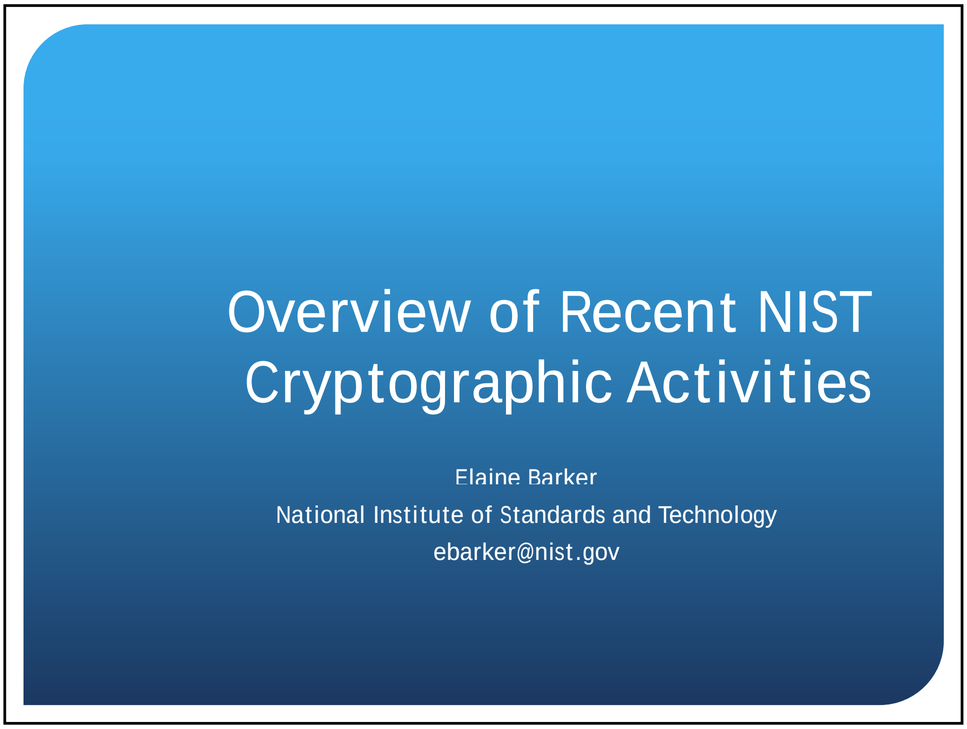
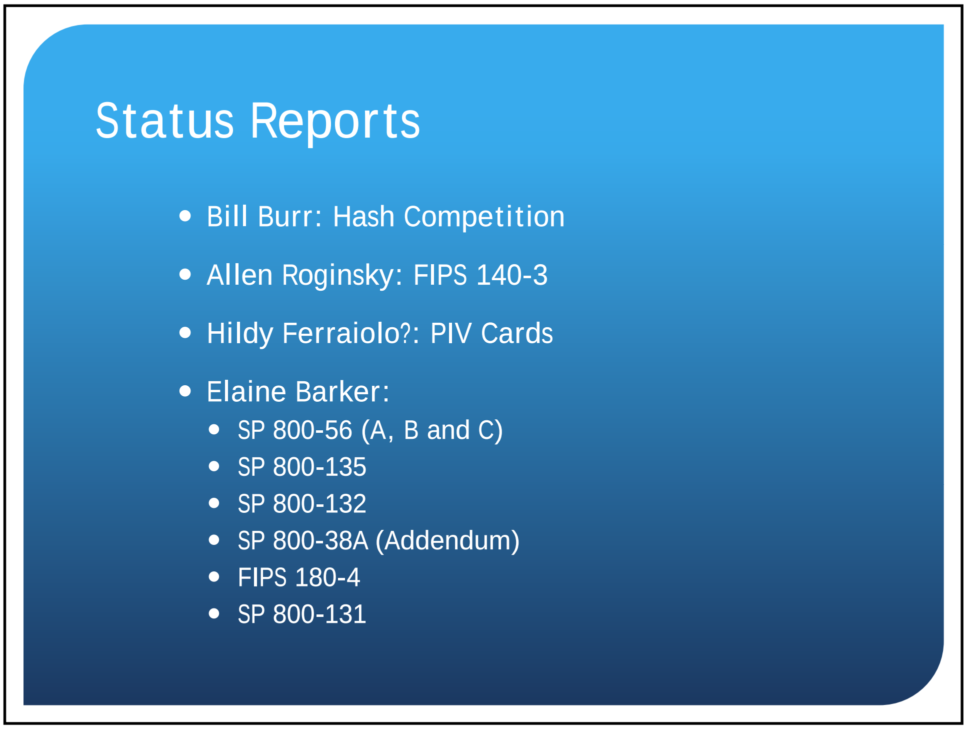


Overview of Recent NIST Cryptographic Activities

Elaine Barker
National Institute of Standards and Technology
ebarker@nist.gov



Status Reports

- Bill Burr: Hash Competition
- Allen Roginsky: FIPS 140-3
- Hildy Ferraiolo?: PIV Cards
- Elaine Barker:
  - SP 800-56 (A, B and C)
  - SP 800-135
  - SP 800-132
  - SP 800-38A (Addendum)
  - FIPS 180-4
  - SP 800-131

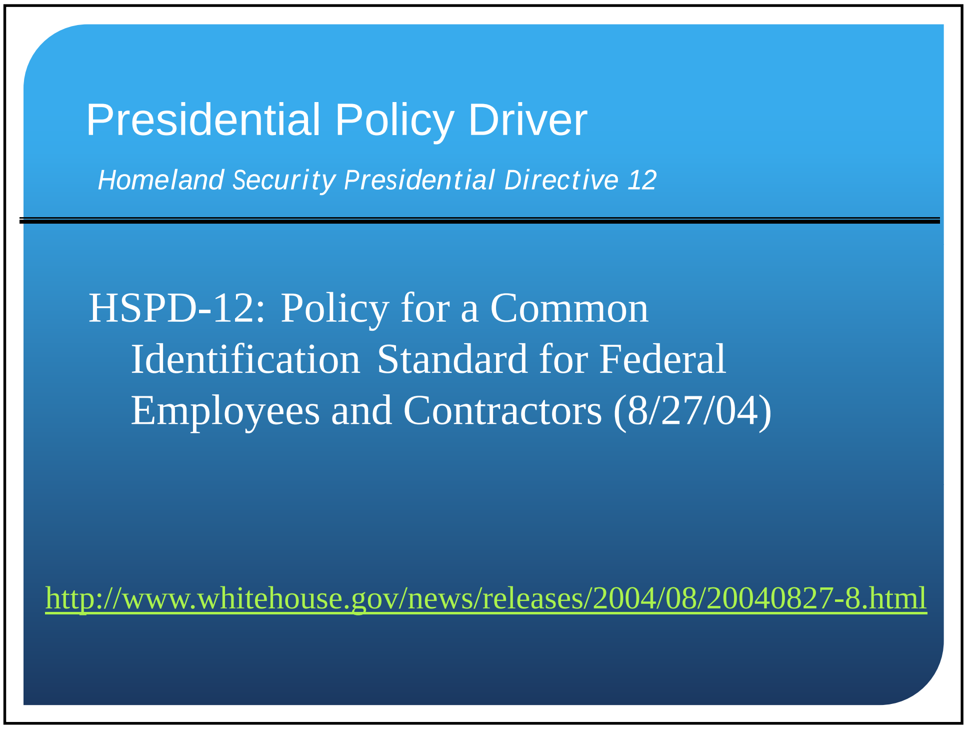
Hash Competition

FIPS 140-3

An Update on FIPS 140-3

- Went to the second public comment period
- Hundreds of comments received.
- NIST is in the process of addressing all of the received comments.
- A new draft will be available as soon as this effort has been completed.
- The standard will still have four security levels (as in FIPS 140-2) but many changes will be introduced.
- The decision will be made about the comment period for the next draft of FIPS 140-3.

PIV Cards

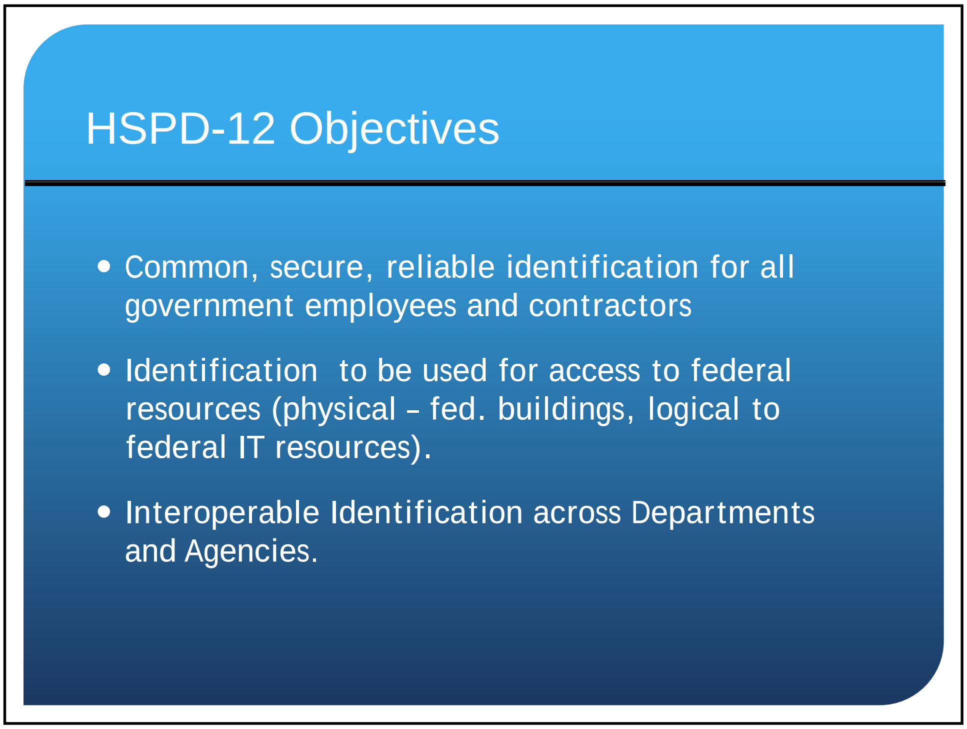


Presidential Policy Driver

Homeland Security Presidential Directive 12

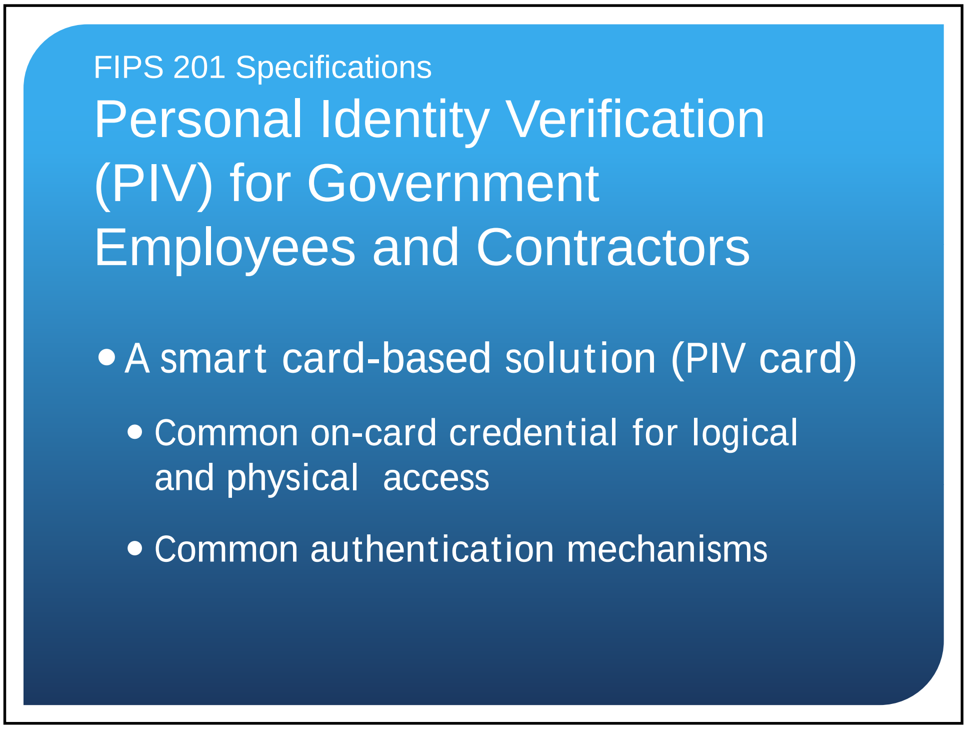
HSPD-12: Policy for a Common Identification Standard for Federal Employees and Contractors (8/27/04)

http://www.whitehouse.gov/news/releases/2004/08/20040827-8.html



HSPD-12 Objectives

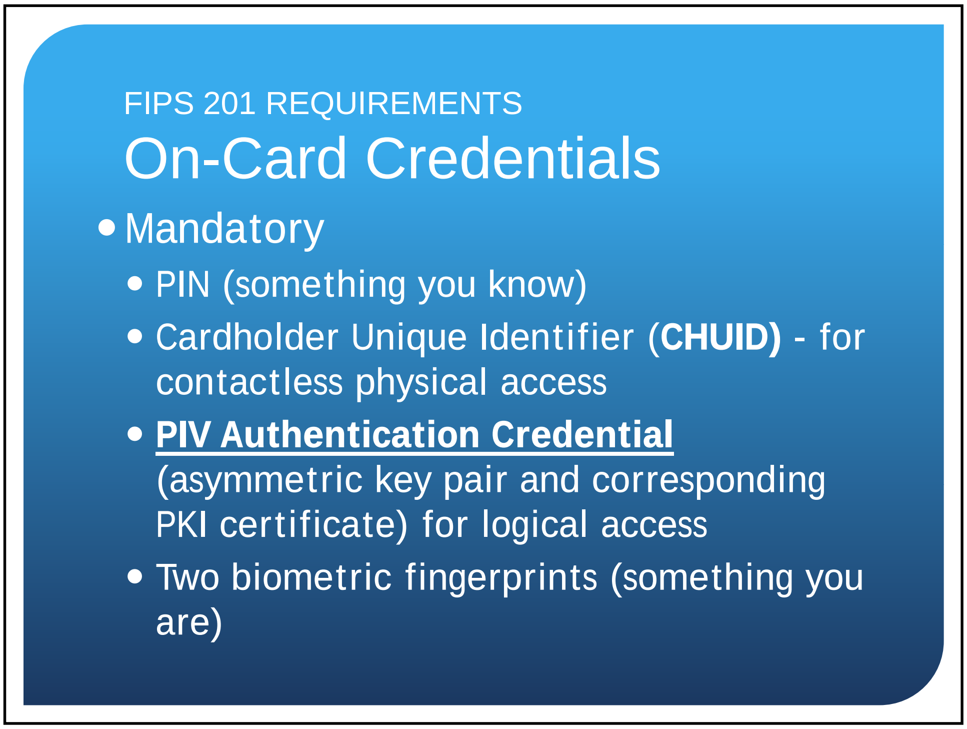
- Common, secure, reliable identification for all government employees and contractors
- Identification to be used for access to federal resources (physical – fed. buildings, logical to federal IT resources).
- Interoperable Identification across Departments and Agencies.



FIPS 201 Specifications

Personal Identity Verification (PIV) for Government Employees and Contractors

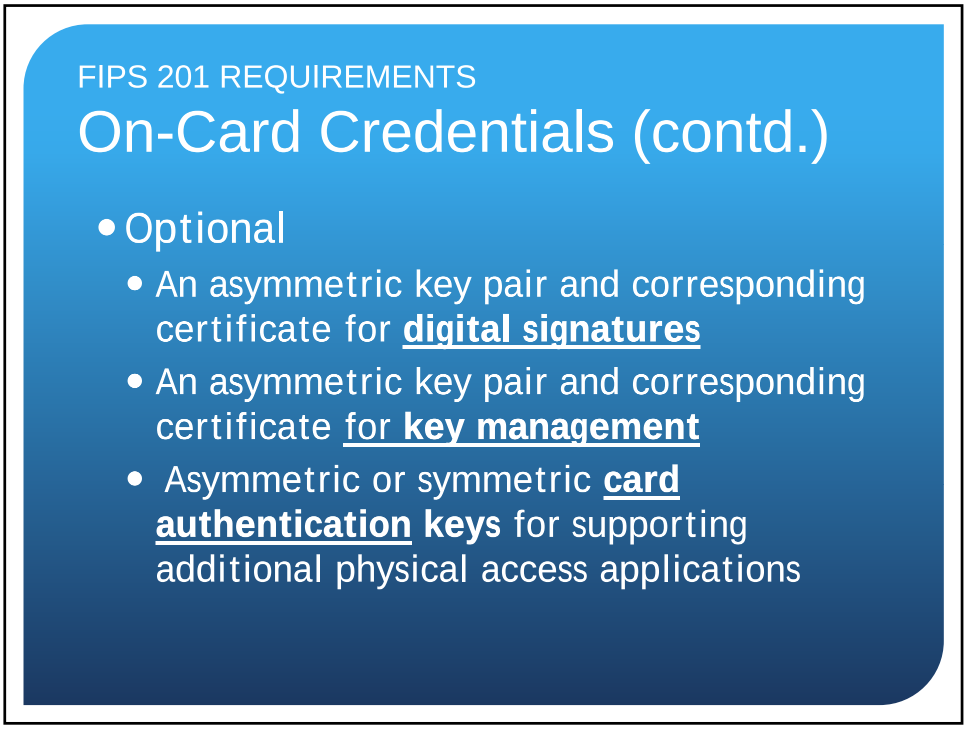
- A smart card-based solution (PIV card)
  - Common on-card credential for logical and physical access
  - Common authentication mechanisms



FIPS 201 REQUIREMENTS

On-Card Credentials

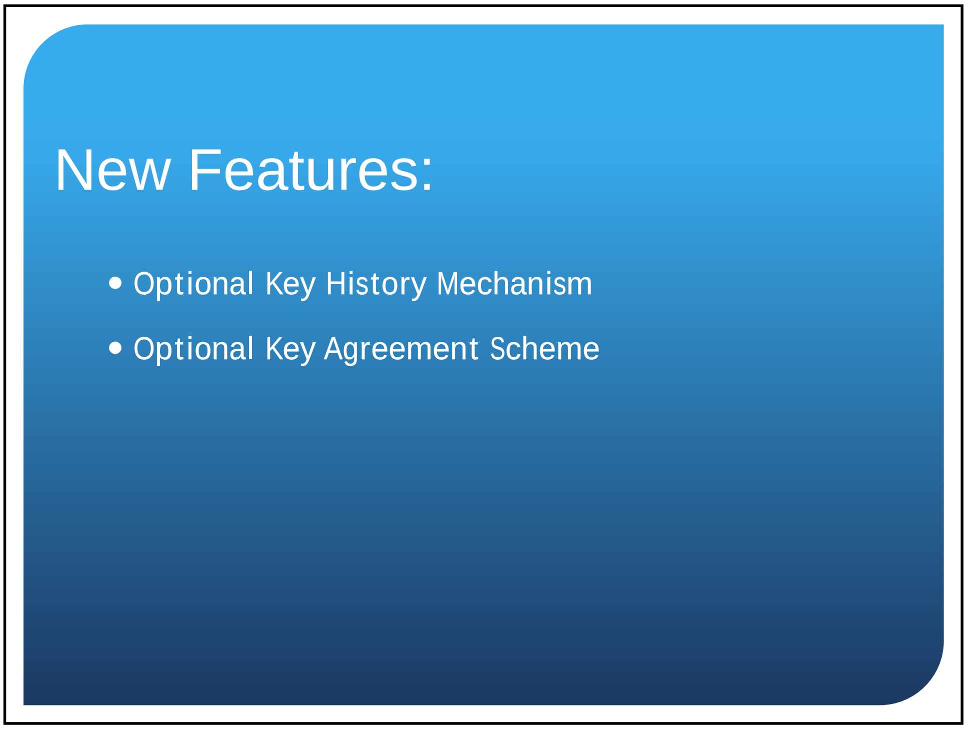
- Mandatory
  - PIN (something you know)
  - Cardholder Unique Identifier (**CHUID)** - for contactless physical access
  - **PIV Authentication Credential** (asymmetric key pair and corresponding PKI certificate) for logical access
  - Two biometric fingerprints (something you are)



FIPS 201 REQUIREMENTS

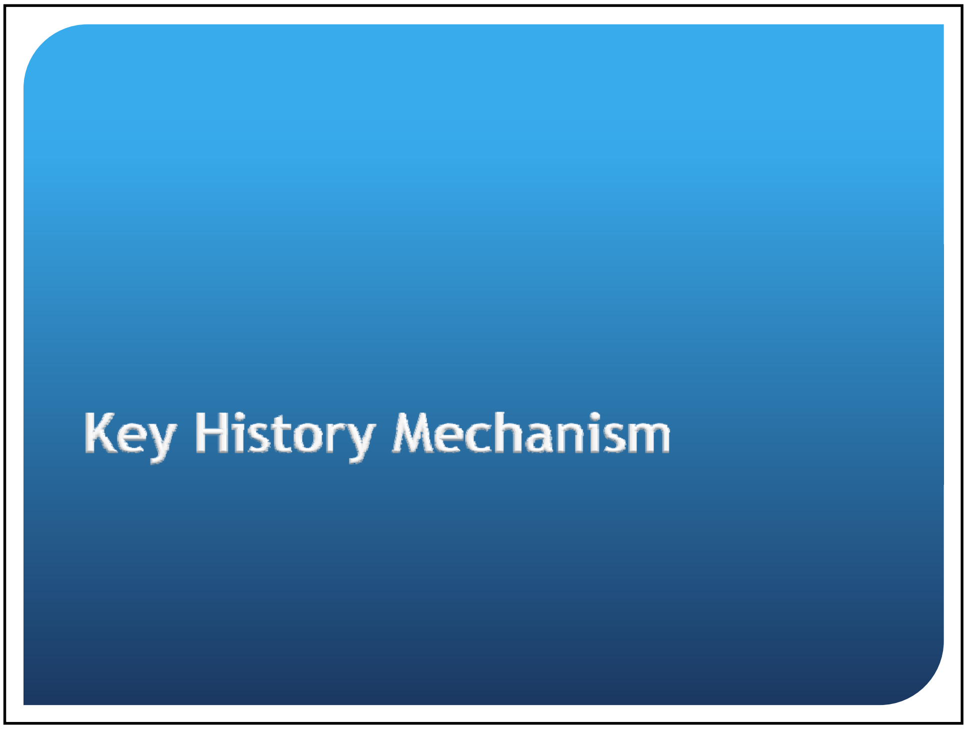
On-Card Credentials (contd.)

- Optional
  - An asymmetric key pair and corresponding certificate for **digital signatures**
  - An asymmetric key pair and corresponding certificate for **key management**
  - Asymmetric or symmetric **card authentication keys** for supporting additional physical access applications

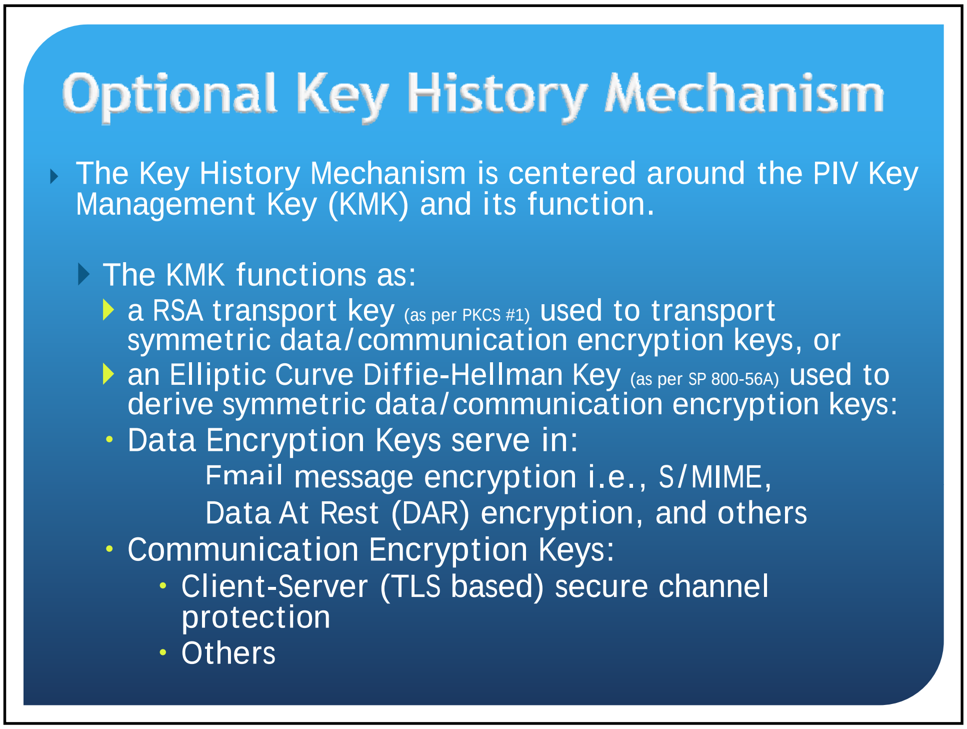


New Features:

- Optional Key History Mechanism
- Optional Key Agreement Scheme



Key History Mechanism

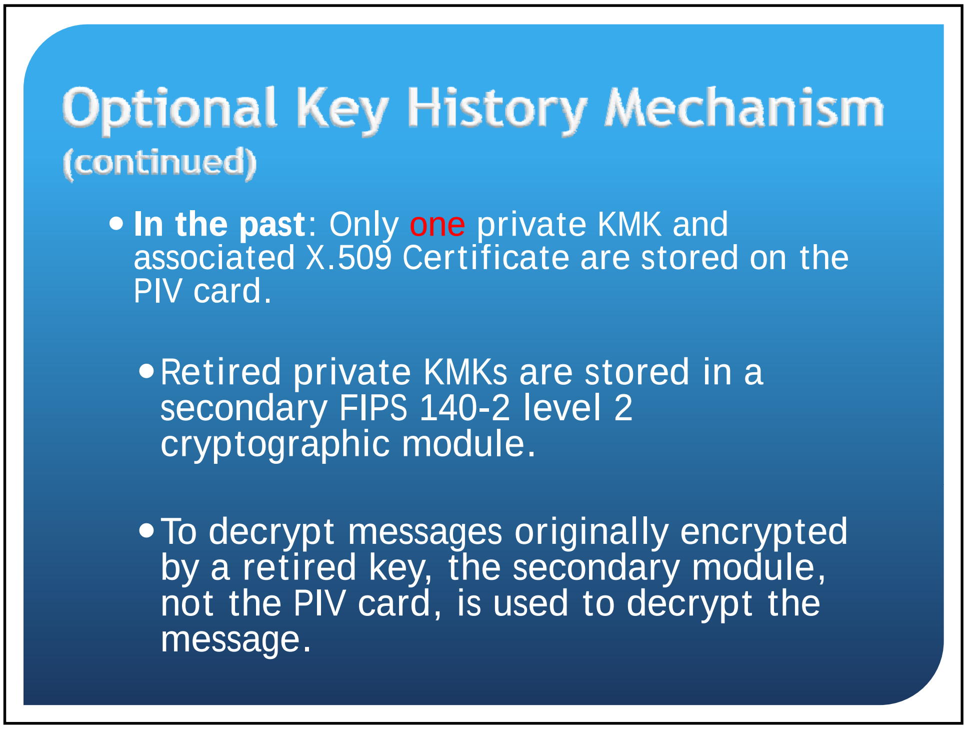


Optional Key History Mechanism

- The Key History Mechanism is centered around the PIV Key Management Key (KMK) and its function.
  - The KMK functions as:
    - a RSA transport key (as per PKCS #1) used to transport symmetric data/communication encryption keys, or
    - an Elliptic Curve Diffie-Hellman Key (as per SP 800-56A) used to derive symmetric data/communication encryption keys:
    - Data Encryption Keys serve in:

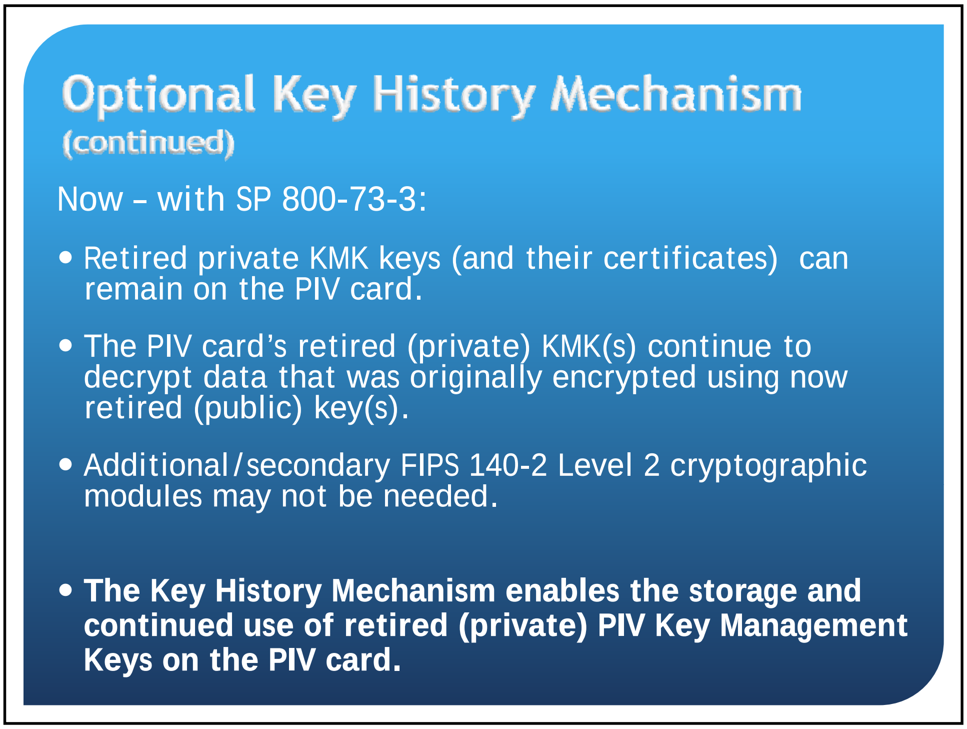
      Email message encryption i.e., S/MIME,

      Data At Rest (DAR) encryption, and others
    - Communication Encryption Keys:
      - Client-Server (TLS based) secure channel protection
      - Others



Optional Key History Mechanism (continued)

- **In the past**: Only one private KMK and associated X.509 Certificate are stored on the PIV card.
  - Retired private KMKs are stored in a secondary FIPS 140-2 level 2 cryptographic module.
  - To decrypt messages originally encrypted by a retired key, the secondary module, not the PIV card, is used to decrypt the message.



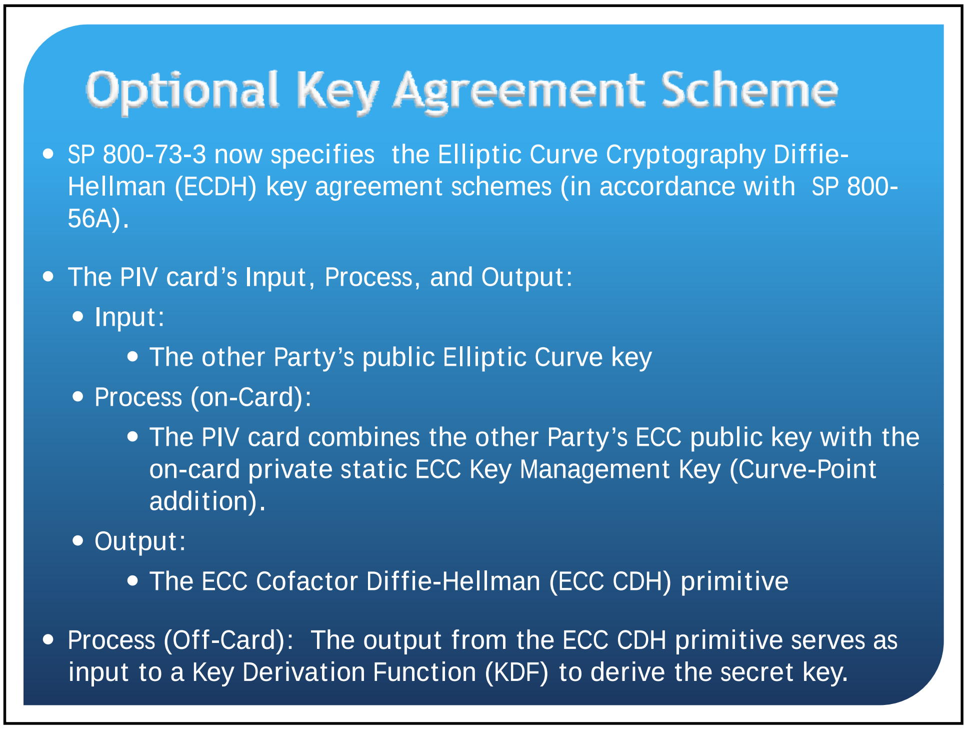
Optional Key History Mechanism (continued)

Now – with SP 800-73-3:

- Retired private KMK keys (and their certificates) can remain on the PIV card.
- The PIV card’s retired (private) KMK(s) continue to decrypt data that was originally encrypted using now retired (public) key(s).
- Additional/secondary FIPS 140-2 Level 2 cryptographic modules may not be needed.

- **The Key History Mechanism enables the storage and continued use of retired (private) PIV Key Management Keys on the PIV card.**

Optional Key Agreement Scheme



Optional Key Agreement Scheme

- SP 800-73-3 now specifies the Elliptic Curve Cryptography Diffie-Hellman (ECDH) key agreement schemes (in accordance with SP 800-56A).
- The PIV card's Input, Process, and Output:
  - Input:
    - The other Party's public Elliptic Curve key
  - Process (on-Card):
    - The PIV card combines the other Party's ECC public key with the on-card private static ECC Key Management Key (Curve-Point addition).
  - Output:
    - The ECC Cofactor Diffie-Hellman (ECC CDH) primitive
- Process (Off-Card): The output from the ECC CDH primitive serves as input to a Key Derivation Function (KDF) to derive the secret key.

Thank you for listening!

Hildegard Ferraiolo (SP 800-73 editor)

(301) 975 6972

hildegard.ferraiolo@nist.gov

http://csrc.nist.gov

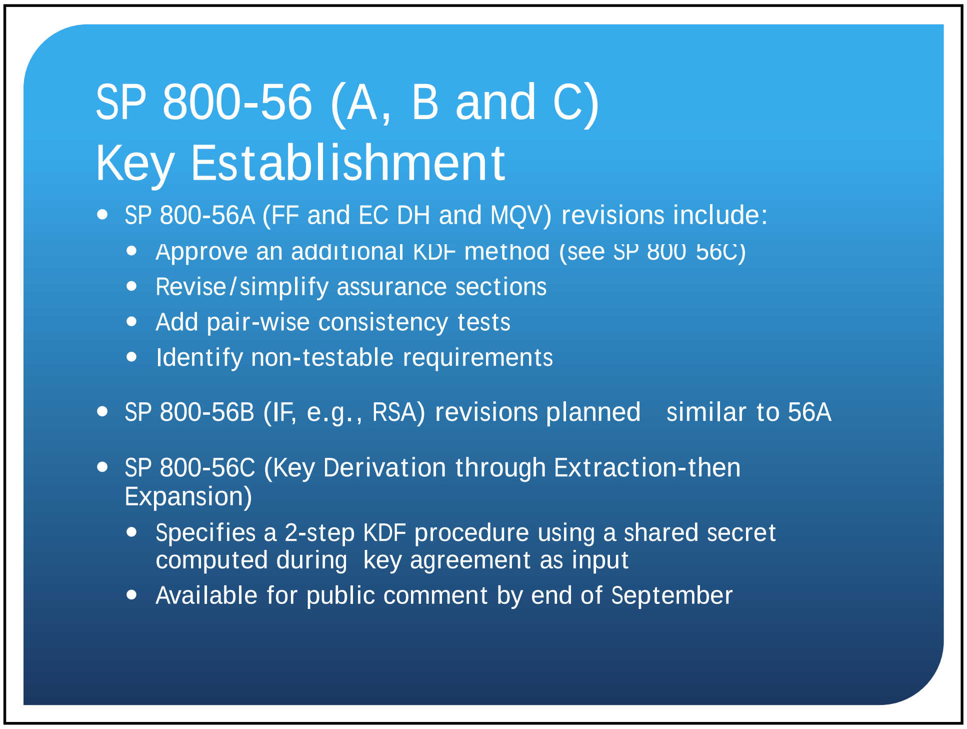
David Cooper (Technical Lead - PKI)

(301) 975 3194

david.cooper@nist.gov

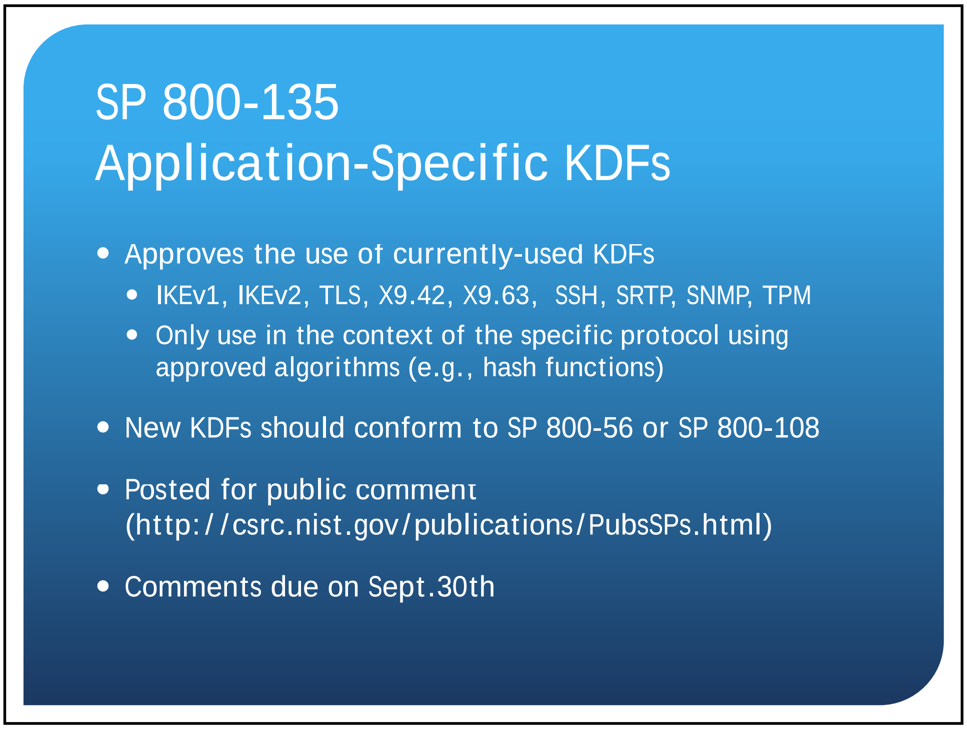
http://csrc.nist.gov

Miscellaneous Activities



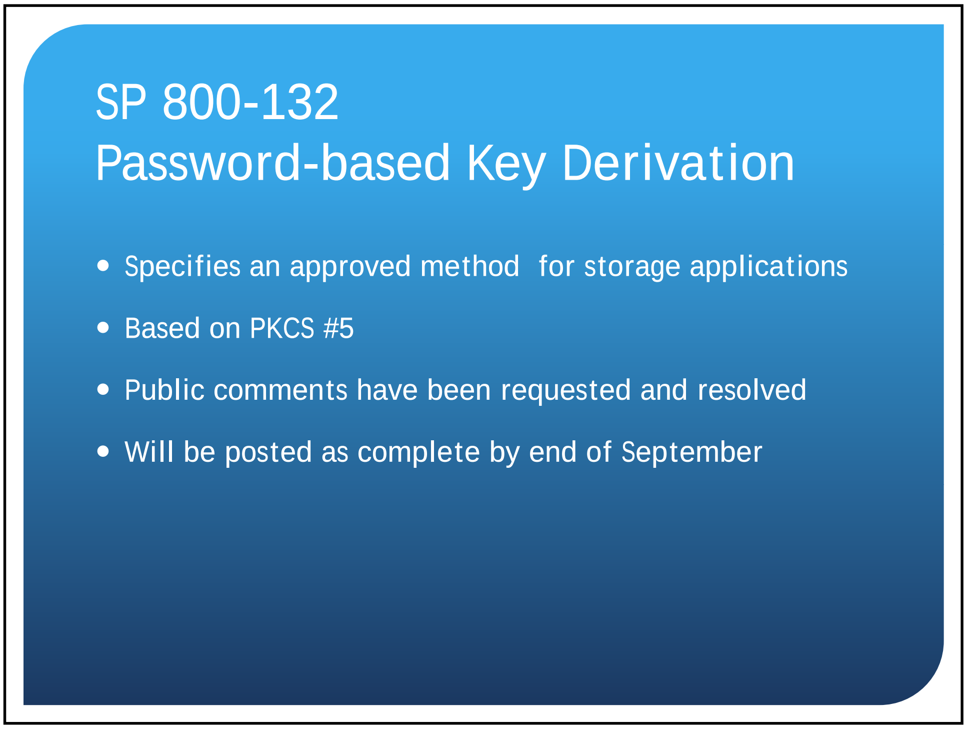
SP 800-56 (A, B and C) Key Establishment

- SP 800-56A (FF and EC DH and MQV) revisions include:
  - Approve an additional KDF method (see SP 800 56C)
  - Revise/simplify assurance sections
  - Add pair-wise consistency tests
  - Identify non-testable requirements
- SP 800-56B (IF, e.g., RSA) revisions planned   similar to 56A
- SP 800-56C (Key Derivation through Extraction-then Expansion)
  - Specifies a 2-step KDF procedure using a shared secret computed during key agreement as input
  - Available for public comment by end of September



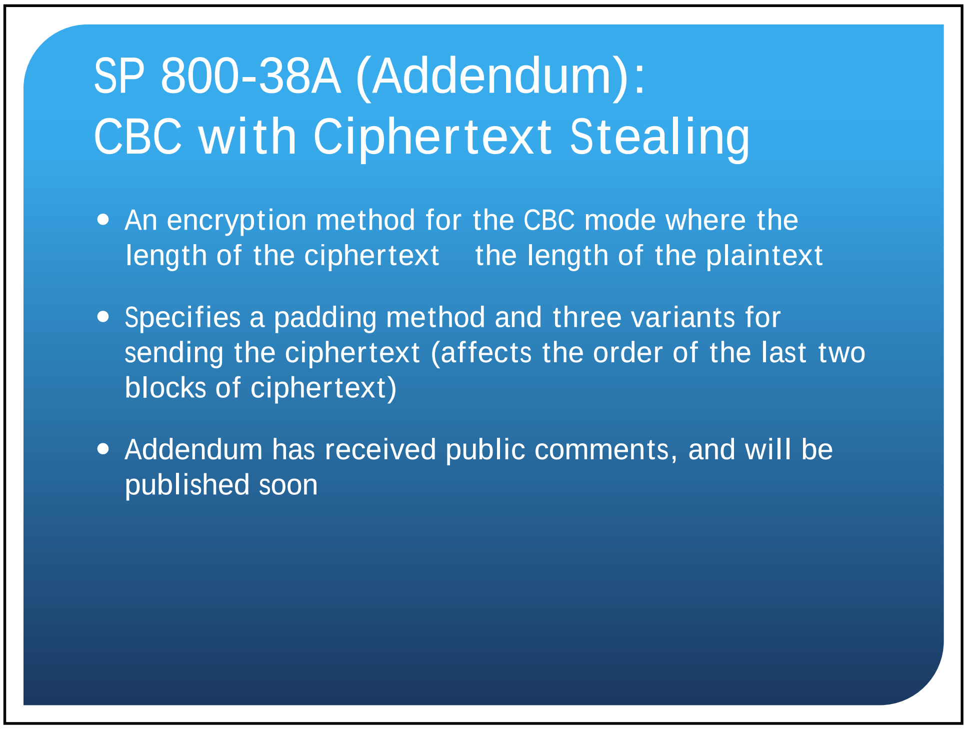
SP 800-135 Application-Specific KDFs

- Approves the use of currently-used KDFs
  - IKEv1, IKEv2, TLS, X9.42, X9.63, SSH, SRTP, SNMP, TPM
  - Only use in the context of the specific protocol using approved algorithms (e.g., hash functions)
- New KDFs should conform to SP 800-56 or SP 800-108
- Posted for public comment (http://csrc.nist.gov/publications/PubsSPs.html)
- Comments due on Sept.30th



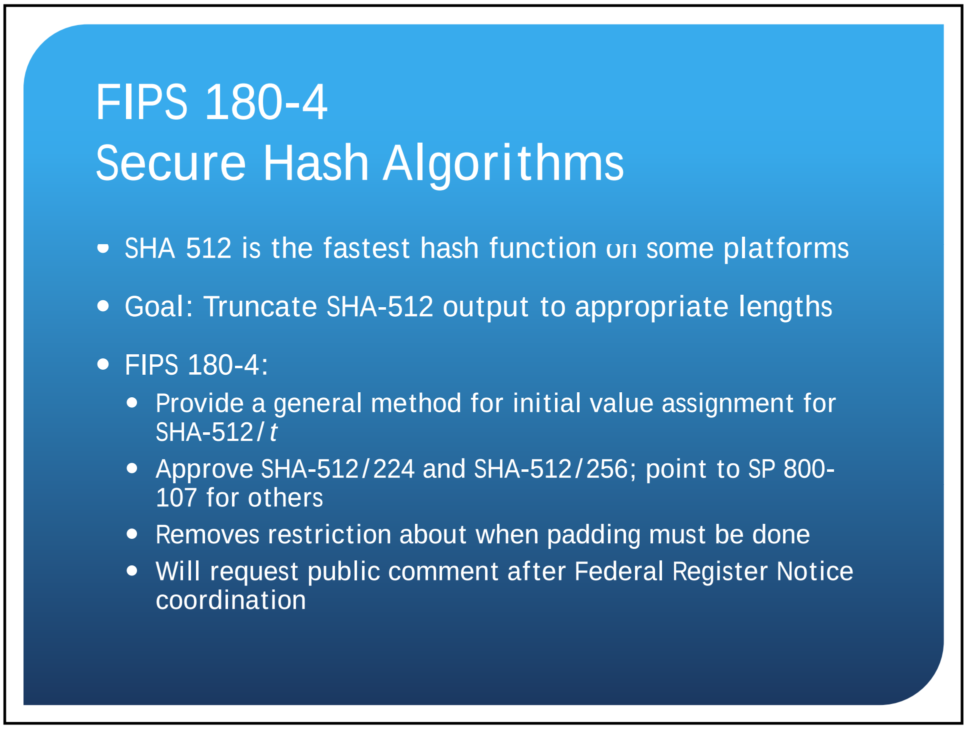
SP 800-132
Password-based Key Derivation

- Specifies an approved method for storage applications
- Based on PKCS #5
- Public comments have been requested and resolved
- Will be posted as complete by end of September



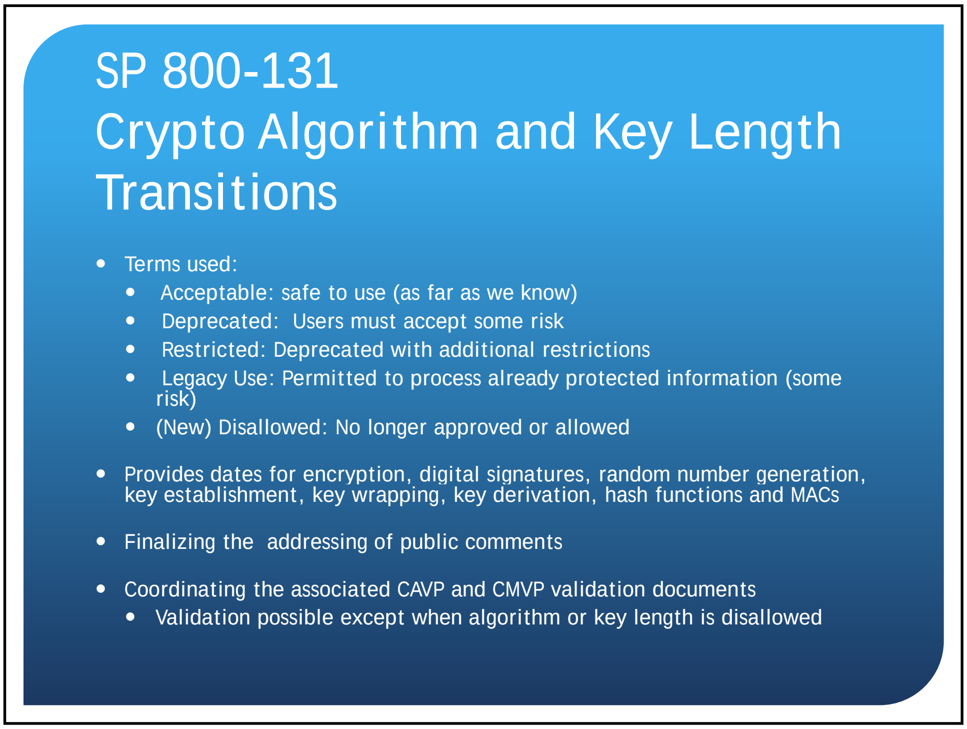
SP 800-38A (Addendum):
CBC with Ciphertext Stealing

- An encryption method for the CBC mode where the length of the ciphertext   the length of the plaintext
- Specifies a padding method and three variants for sending the ciphertext (affects the order of the last two blocks of ciphertext)
- Addendum has received public comments, and will be published soon



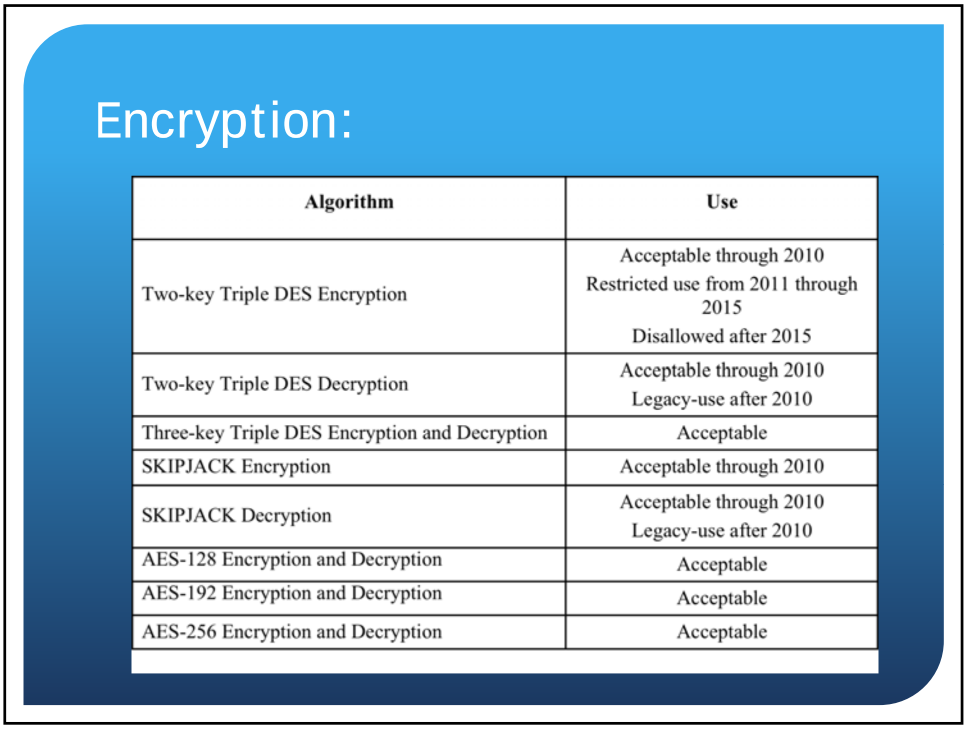
FIPS 180-4
Secure Hash Algorithms

- SHA 512 is the fastest hash function on some platforms
- Goal: Truncate SHA-512 output to appropriate lengths
- FIPS 180-4:
  - Provide a general method for initial value assignment for SHA-512/*t*
  - Approve SHA-512/224 and SHA-512/256; point to SP 800-107 for others
  - Removes restriction about when padding must be done
  - Will request public comment after Federal Register Notice coordination



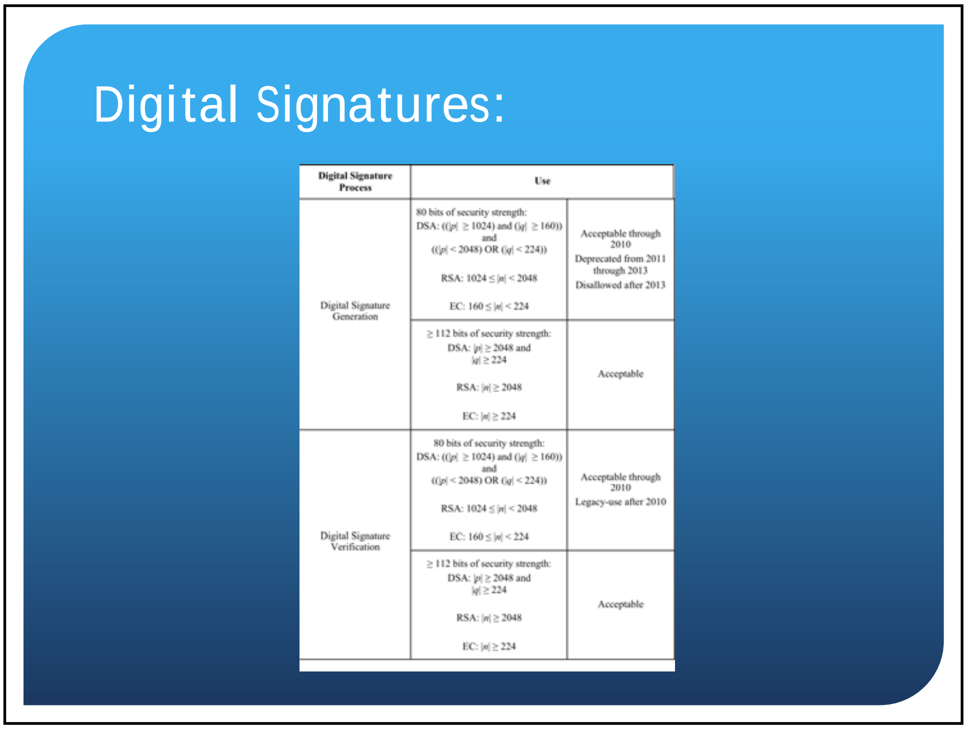
SP 800-131
Crypto Algorithm and Key Length Transitions

- Terms used:
  - Acceptable: safe to use (as far as we know)
  - Deprecated: Users must accept some risk
  - Restricted: Deprecated with additional restrictions
  - Legacy Use: Permitted to process already protected information (some risk)
  - (New) Disallowed: No longer approved or allowed
- Provides dates for encryption, digital signatures, random number generation, key establishment, key wrapping, key derivation, hash functions and MACs
- Finalizing the addressing of public comments
- Coordinating the associated CAVP and CMVP validation documents
  - Validation possible except when algorithm or key length is disallowed



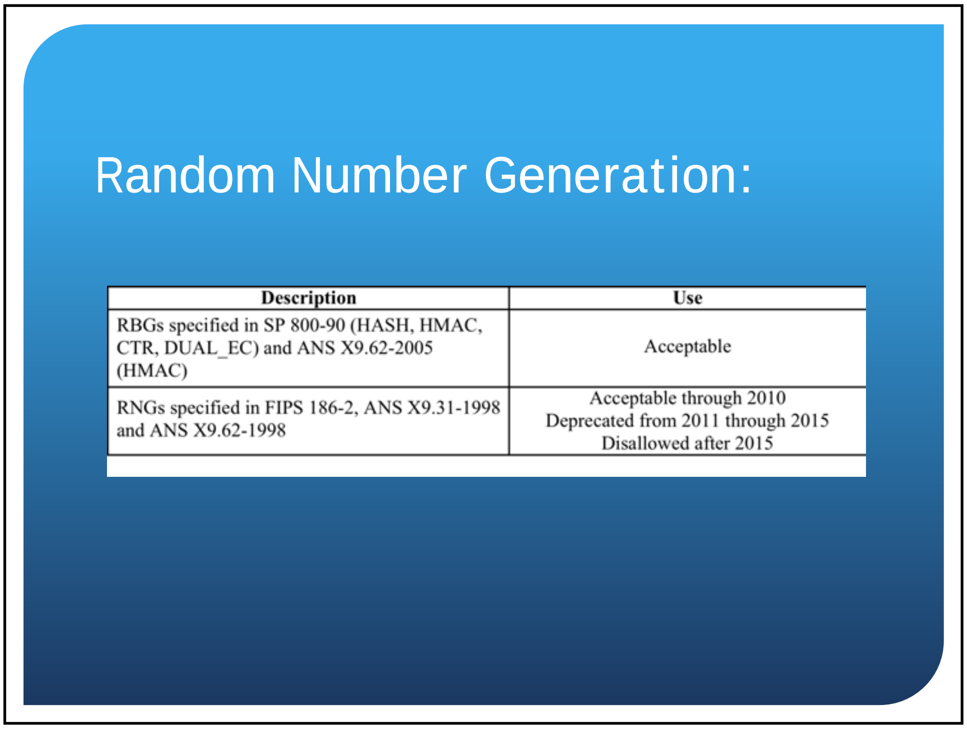
Encryption:

Algorithm	Use
Two-key Triple DES Encryption	Acceptable through 2010 Restricted use from 2011 through 2015 Disallowed after 2015
Two-key Triple DES Decryption	Acceptable through 2010 Legacy-use after 2010
Three-key Triple DES Encryption and Decryption	Acceptable
SKIPJACK Encryption	Acceptable through 2010
SKIPJACK Decryption	Acceptable through 2010 Legacy-use after 2010
AES-128 Encryption and Decryption	Acceptable
AES-192 Encryption and Decryption	Acceptable
AES-256 Encryption and Decryption	Acceptable



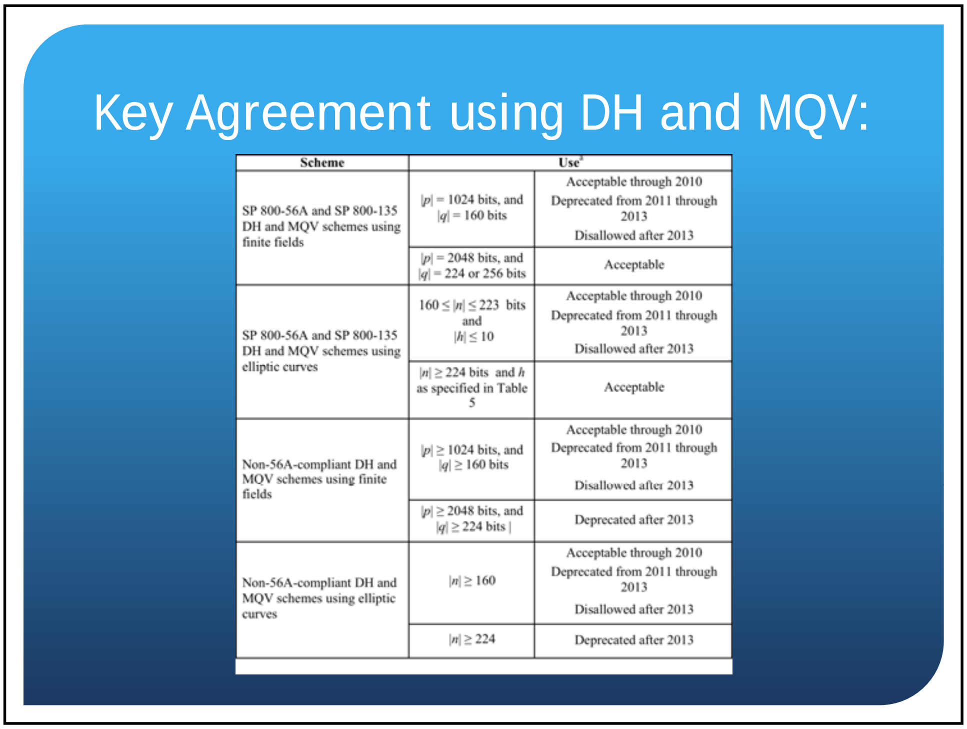
Digital Signatures:

Digital Signature Process	Use	
Digital Signature Generation	80 bits of security strength: DSA: (($\|p\| \geq 1024$) and ($\|q\| \geq 160$)) and (($\|p\| < 2048$) OR ($\|q\| < 224$)) RSA: $1024 \leq \|n\| < 2048$ EC: $160 \leq \|n\| < 224$	Acceptable through 2010 Deprecated from 2011 through 2013 Disallowed after 2013
	$\geq$ 112 bits of security strength: DSA: $\|p\| \geq 2048$ and $\|q\| \geq 224$ RSA: $\|n\| \geq 2048$ EC: $\|n\| \geq 224$	Acceptable
Digital Signature Verification	80 bits of security strength: DSA: (($\|p\| \geq 1024$) and ($\|q\| \geq 160$)) and (($\|p\| < 2048$) OR ($\|q\| < 224$)) RSA: $1024 \leq \|n\| < 2048$ EC: $160 \leq \|n\| < 224$	Acceptable through 2010 Legacy-use after 2010
	$\geq$ 112 bits of security strength: DSA: $\|p\| \geq 2048$ and $\|q\| \geq 224$ RSA: $\|n\| \geq 2048$ EC: $\|n\| \geq 224$	Acceptable



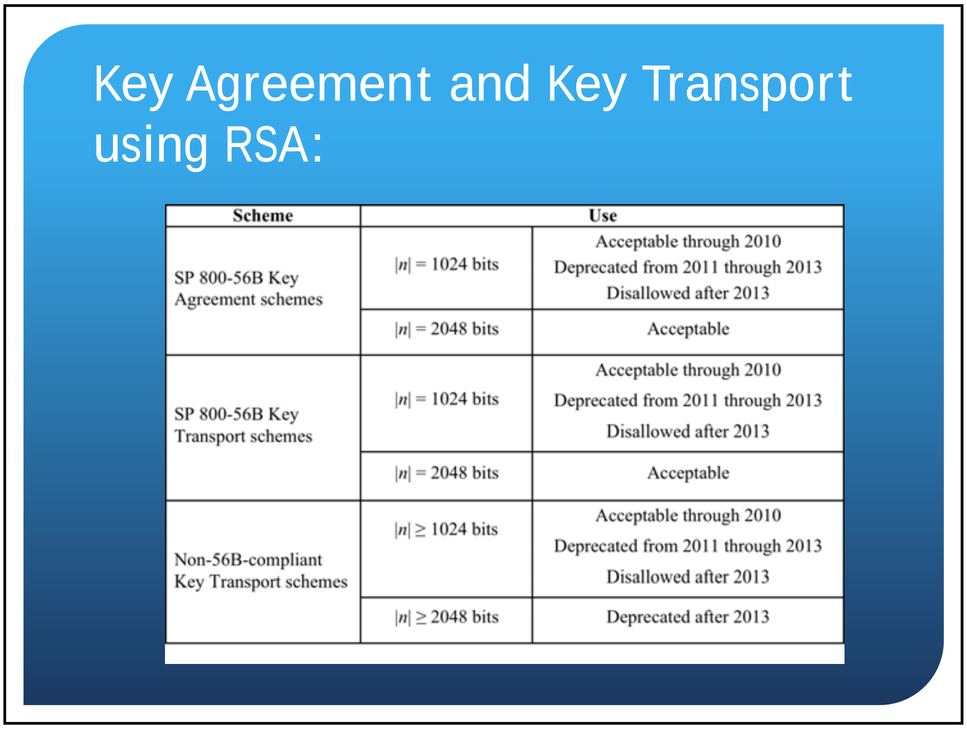
Random Number Generation:

Description	Use
RBGs specified in SP 800-90 (HASH, HMAC, CTR, DUAL_EC) and ANS X9.62-2005 (HMAC)	Acceptable
RNGs specified in FIPS 186-2, ANS X9.31-1998 and ANS X9.62-1998	Acceptable through 2010 Deprecated from 2011 through 2015 Disallowed after 2015



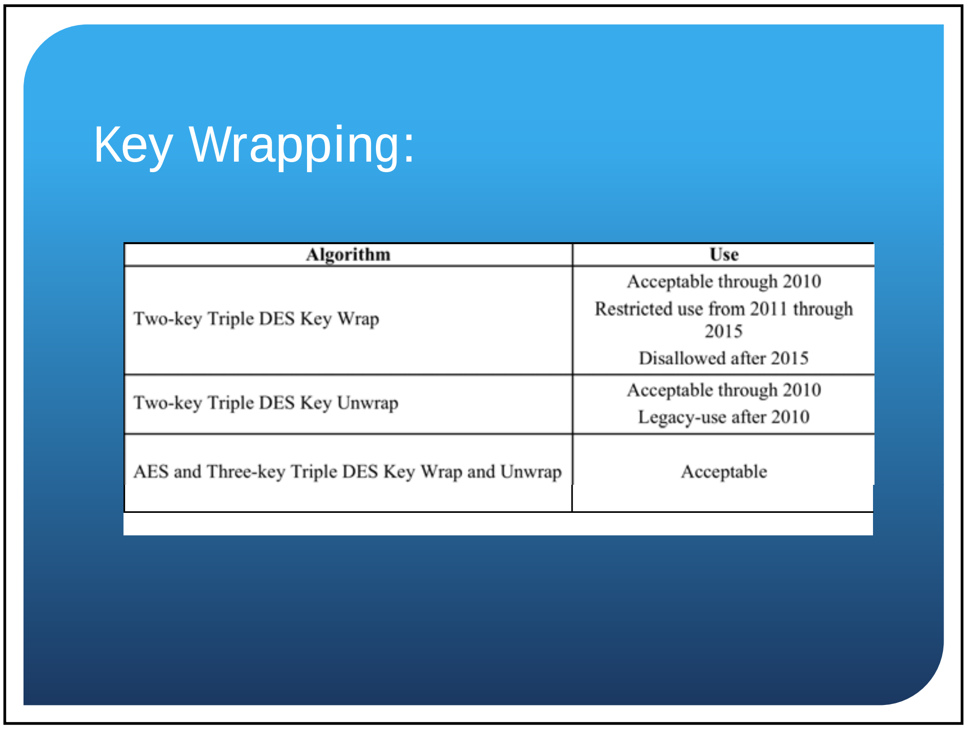
Key Agreement using DH and MQV:

Scheme	Use[3]	
SP 800-56A and SP 800-135 DH and MQV schemes using finite fields	$\lvert p\rvert = 1024$ bits, and $\lvert q\rvert = 160$ bits	Acceptable through 2010 Deprecated from 2011 through 2013 Disallowed after 2013
	$\lvert p\rvert = 2048$ bits, and $\lvert q\rvert = 224$ or 256 bits	Acceptable
SP 800-56A and SP 800-135 DH and MQV schemes using elliptic curves	$160 \le \lvert n\rvert \le 223$ bits and $\lvert h\rvert \le 10$	Acceptable through 2010 Deprecated from 2011 through 2013 Disallowed after 2013
	$\lvert n\rvert \ge 224$ bits and h as specified in Table 5	Acceptable
Non-56A-compliant DH and MQV schemes using finite fields	$\lvert p\rvert \ge 1024$ bits, and $\lvert q\rvert \ge 160$ bits	Acceptable through 2010 Deprecated from 2011 through 2013 Disallowed after 2013
	$\lvert p\rvert \ge 2048$ bits, and $\lvert q\rvert \ge 224$ bits |	Deprecated after 2013
Non-56A-compliant DH and MQV schemes using elliptic curves	$\lvert n\rvert \ge 160$	Acceptable through 2010 Deprecated from 2011 through 2013 Disallowed after 2013
	$\lvert n\rvert \ge 224$	Deprecated after 2013



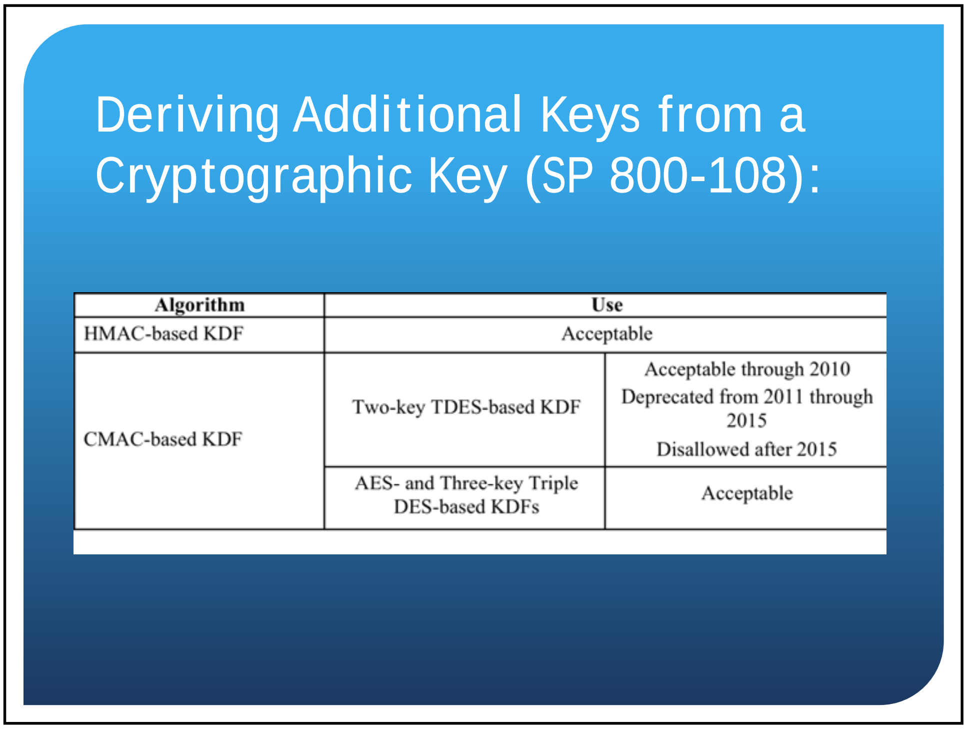
Key Agreement and Key Transport using RSA:

Scheme	Use	
SP 800-56B Key Agreement schemes	$\lvert n \rvert$ = 1024 bits	Acceptable through 2010 Deprecated from 2011 through 2013 Disallowed after 2013
	$\lvert n \rvert$ = 2048 bits	Acceptable
SP 800-56B Key Transport schemes	$\lvert n \rvert$ = 1024 bits	Acceptable through 2010 Deprecated from 2011 through 2013 Disallowed after 2013
	$\lvert n \rvert$ = 2048 bits	Acceptable
Non-56B-compliant Key Transport schemes	$\lvert n \rvert \geq$ 1024 bits	Acceptable through 2010 Deprecated from 2011 through 2013 Disallowed after 2013
	$\lvert n \rvert \geq$ 2048 bits	Deprecated after 2013



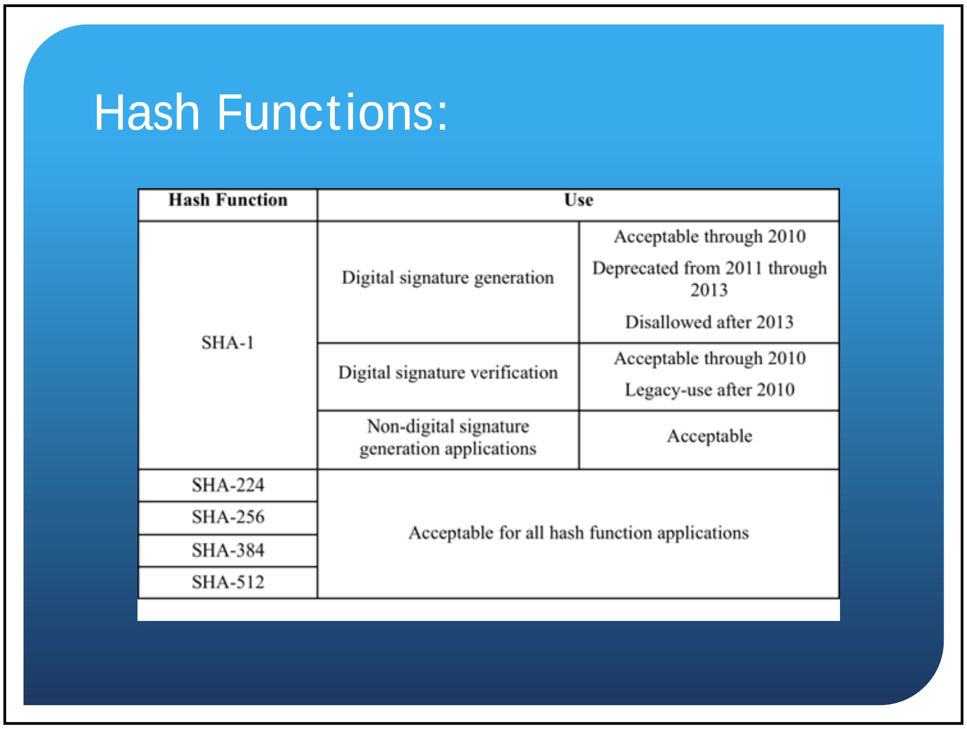
Key Wrapping:

Algorithm	Use
Two-key Triple DES Key Wrap	Acceptable through 2010 Restricted use from 2011 through 2015 Disallowed after 2015
Two-key Triple DES Key Unwrap	Acceptable through 2010 Legacy-use after 2010
AES and Three-key Triple DES Key Wrap and Unwrap	Acceptable



Deriving Additional Keys from a Cryptographic Key (SP 800-108):

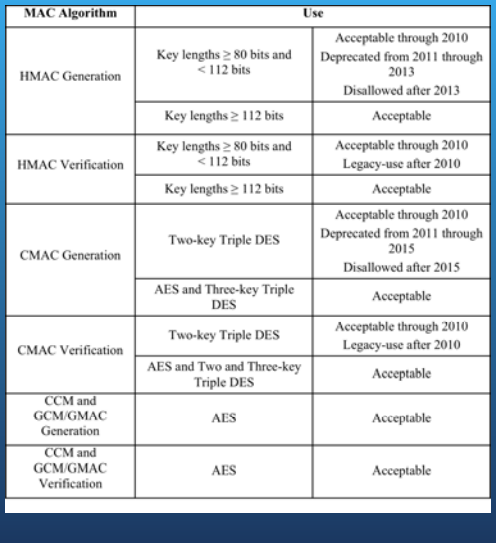
Algorithm	Use	
HMAC-based KDF	Acceptable	
CMAC-based KDF	Two-key TDES-based KDF	Acceptable through 2010 Deprecated from 2011 through 2015 Disallowed after 2015
	AES- and Three-key Triple DES-based KDFs	Acceptable



Hash Functions:

Hash Function	Use	
SHA-1	Digital signature generation	Acceptable through 2010 Deprecated from 2011 through 2013 Disallowed after 2013
	Digital signature verification	Acceptable through 2010 Legacy-use after 2010
	Non-digital signature generation applications	Acceptable
SHA-224	Acceptable for all hash function applications	
SHA-256		
SHA-384		
SHA-512		

Message Authentication Codes:



MAC Algorithm	Use	
HMAC Generation	Key lengths ≥ 80 bits and < 112 bits	Acceptable through 2010 Deprecated from 2011 through 2013 Disallowed after 2013
	Key lengths ≥ 112 bits	Acceptable
HMAC Verification	Key lengths ≥ 80 bits and < 112 bits	Acceptable through 2010 Legacy-use after 2010
	Key lengths ≥ 112 bits	Acceptable
CMAC Generation	Two-key Triple DES	Acceptable through 2010 Deprecated from 2011 through 2015 Disallowed after 2015
	AES and Three-key Triple DES	Acceptable
CMAC Verification	Two-key Triple DES	Acceptable through 2010 Legacy-use after 2010
	AES and Two and Three-key Triple DES	Acceptable
CCM and GCM/GMAC Generation	AES	Acceptable
CCM and GCM/GMAC Verification	AES	Acceptable

Questions?