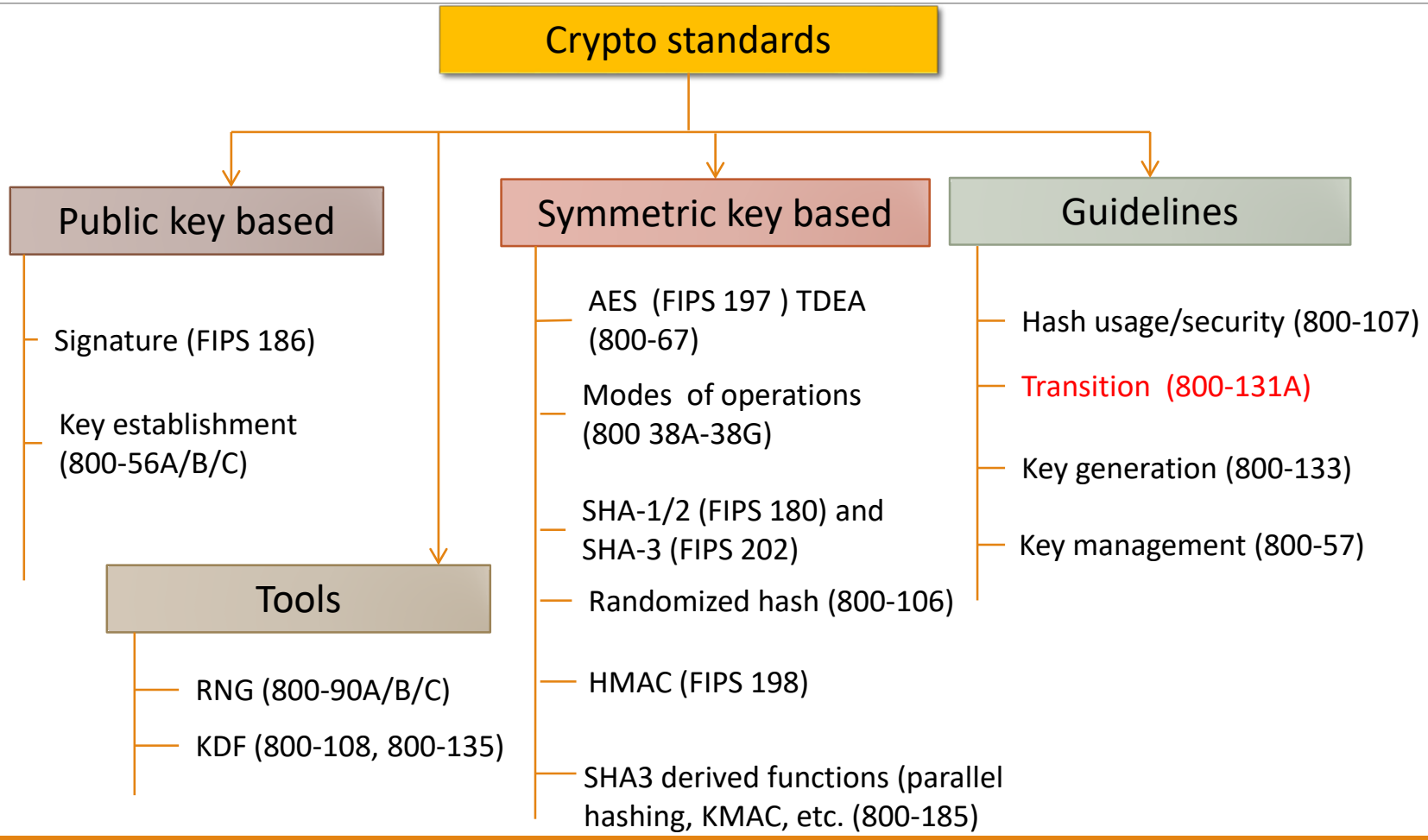
NIST Cryptography Transition Update

ANDY REGENSCHEID AND LILY CHEN
COMPUTER SECURITY DIVISION, INFORMATION TECHNOLOGY LAB
NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY (NIST)

NIST Cryptographic Standards



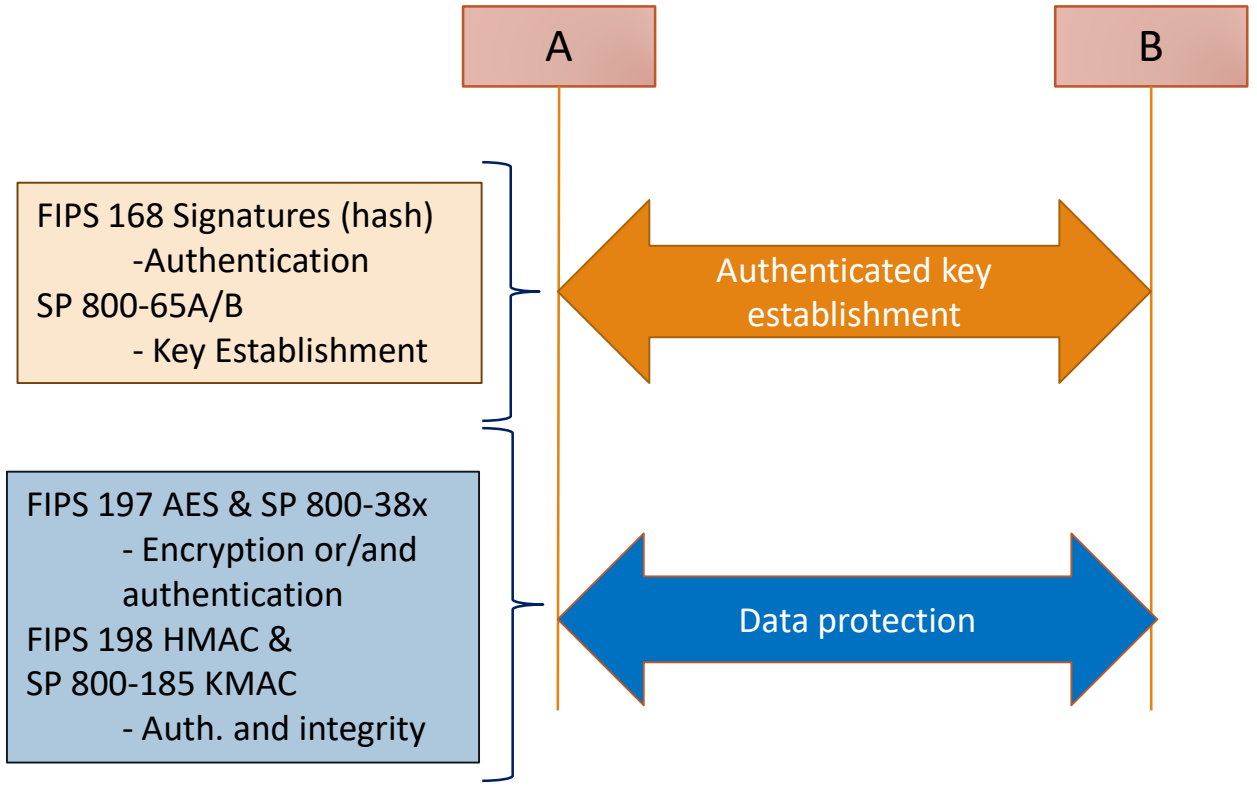
NIST Crypto Standards Usage in Practice

In communication protocols, public key and symmetric key cryptography schemes are often used together, e.g. TLS, IKE/IPsec, etc.

- Use public key cryptography to establish keys and authenticate users through signatures
- Use symmetric key cryptography to encrypt and authenticate bulk data

In trusted platform technologies,

- Use public key to establish root of trust
- Use signatures to authenticate/authorize firmware, software and applications
- Use symmetric key crypto to protect data



Cryptography Transition - General

Transition is constantly required to deal with

- Increased computing power for attacking cryptosystems
- Emergence of more sophisticated cryptanalysis techniques
- New technologies such as quantum computers

Transition is judged based on state of the art computing and cryptanalysis technologies

NIST Guidelines on transition is specified in SP 800-131A

- The latest version is Nov. 2015
- In this specification, algorithm/key length is specified in terms of “approved”, “acceptable”, “deprecated”, “disallowed”, “restricted” etc.
- In terms of 800-131A, transition means moving away from “deprecated”, abandoning “disallowed”, and adopting “approved”

Government usage of cryptography shall follow the guideline and use approved algorithms, e.g.

- TLS cipher-suite negotiation - The server **shall** be configured to only use cipher suites that are composed entirely of Approved algorithms (see SP 800-52 Rev.1)

Cryptography Transition - Challenges

The transition costs money

- Replacing systems with insecure crypto algorithms maybe costly or beyond the budget allowed

The transition may not work well with interoperability

- For backward compatibility reasons, some protocols accept insecure crypto in the cipher-suite negotiation, e.g. in TLS
- Making hard rules on transition may make it not interoperable

The transition is much more complicated than selecting algorithms and key lengths

- The transition must consider details, e.g. padding, PKCS #1 used in encryption
- The transition must check the use scenarios, e.g. how many blocks of data to be encrypted with one key

The transition must coordinate with current industry practice which can be diversified

- Some industry well accepted practice may not be consistent with NIST standards
- Sometimes, it is hard to find “common” accepted practice

Cryptography Transition – Rule of Thumb

NIST has required minimum security strength of 112 bits since 2010

Implications

- RSA for key establishment and signature (SP 800-56B and FIPS 186) – for $n = p \cdot q$, $|n|$ **shall** be at least 2048 bits
- DSA signatures over GF(p) (FIPS 186) – $|p|$ shall be at least 2048 bits, the subgroup size q **shall** be at least 224 bits
- For ECDSA (FIPS 186), the size of elliptic curve group **shall** be at least 224 bits
- Hash function in SHA-2 and SHA-3 families **shall** be used for digital signatures (FIPS 180 and FIPS 202)
- Block ciphers
  - Three-key triple DES (SP 800-67)
  - AES 128, 192, and 256 (FIPS 197)

Cryptography Transition – FIPS 140 Validation

FIPS 140 validation is the vehicle to enforce the requirements for government usage

- Look for FIPS 140 validated cryptographic modules

FIPS 140: requirements in 11 areas to the design and implementation of a cryptographic module

Cryptographic Module Validation Program (CMVP): NIST/CSEC program to test modules

- Vendors submit modules
- Testing conducted by accredited test laboratories

References:

CMVP: http://csrc.nist.gov/groups/STM/cmvp/

FIPS 140 Validated Modules: http://csrc.nist.gov/groups/STM/cmvp/validation.html

Transition Update – Triple DES

Triple DES is based on Data Encryption Standard (DES)

- DES is a block cipher with 64 bits block size and 56 bits key size
- DES was specified in FIPS 46, published in 1977, and withdrawn in 2005

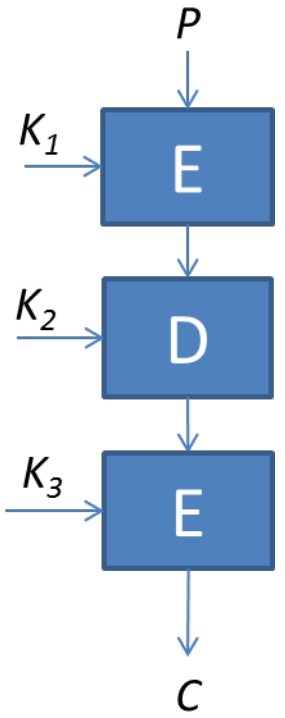
Triple DES called DES three times and can support two key version and three key version

- Triple DES is specified in SP 800-67
- Two-key triple DES is disallowed after 2015
- Three-key triple DES is acceptable

The attack: ***Sweet32: Birthday attacks on 64-bit block ciphers in TLS and OpenVPN*** (ACM CCS 2016) imposes that when more than 2^{20} blocks of data is encrypted with a given key, triple DES is not secure

SP 800-67 Rev2 (Nov. 2017) sets a new data limit of 2^{20} for a given key

- In case that the data rate is high and enforcing such a limit is infeasible, such as TLS, triple DES is no longer approved



Transition Update – Random Number Generator

Security of cryptography relies on random number generator

Usually, a true random number generator is used as an entropy source (or multiple entropy sources) for a pseudorandom number generator to obtain the desired distribution

NIST specifies random number generator in SP 800-90 series: 90A- deterministic random bit generator (DRBG); 90B- entropy source; 90C – construction

Two important factors

- True random source (entropy)
- Inversible DRBG

Historically, some other random number generators have been specified and adopted, e.g. RNG specified in X9.31

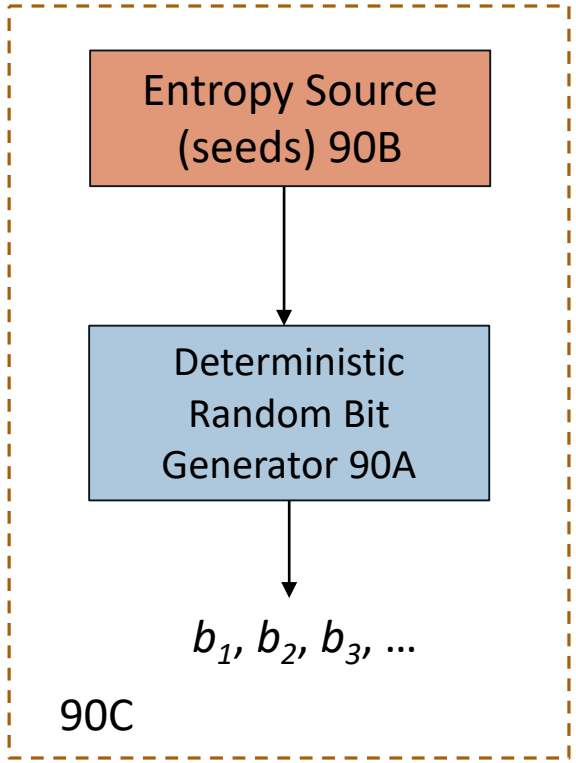
- These RNG algorithms are disallowed after 2015

A recent discovered attack “Don't Use Hard-coded Keys (DUHK)” explores a weak RNG specified in X9.31 which is broken in 1997

- It does not have true random input and DRBG is reversible
- The non random “seeds”, generated from a single DRBG, are hard coded to devices
- By discovering status, the traffic from any VPN using FortiOS 4.3.0 to FortiOS 4.3.18 can be decrypted

The lesson is learnt in a hard way

- We (NIST) should have deprecated it way sooner and told people to stop using it!
- Never use hard coded seeds generated by a single RNG for different devices



Transition Update – Key Establishment

NIST Specified Key Establishment Schemes are mainly in two categories

- Discrete log based (in 800-56A): various DH, MQV and the respective elliptic curve versions
- Factorization based (in 800-56B): RSA encryption for key transport and key agreement

Major Internet Protocols adopted some of these schemes

- TLS 1.2 and earlier versions support three options for key establishment: RSA, ephemeral- static DH, ephemeral- ephemeral DH
- TLS 1.3 supports only ephemeral - ephemeral DH for its perfect forward secrecy feature
- IKEv1 and IKEv2 use ephemeral-ephemeral DH

NIST team is working on a revision of 56A (draft released for public comments Aug. 2017)

- The next revision of 56A uses safe primes *p* for DH and MQV over GF(*p*)
- Using safe primes is consistent with TLS and IKE and the gap is filled
- After the publication of the revision of 56A, compliance is required

NIST is also working on a revision on 56B and will include larger module size |n| > = 3072

Transition to Post-Quantum Cryptography

Quantum computing changed what we have believed about the hardness of discrete log and factorization problems

- Using quantum computers, an integer *n* can be factored in polynomial time using Shor's algorithm
- The discrete logarithm problem can also be solved by Shor's algorithm in polynomial time

As a result, the public key cryptosystems deployed since the 1980s will need to be replaced

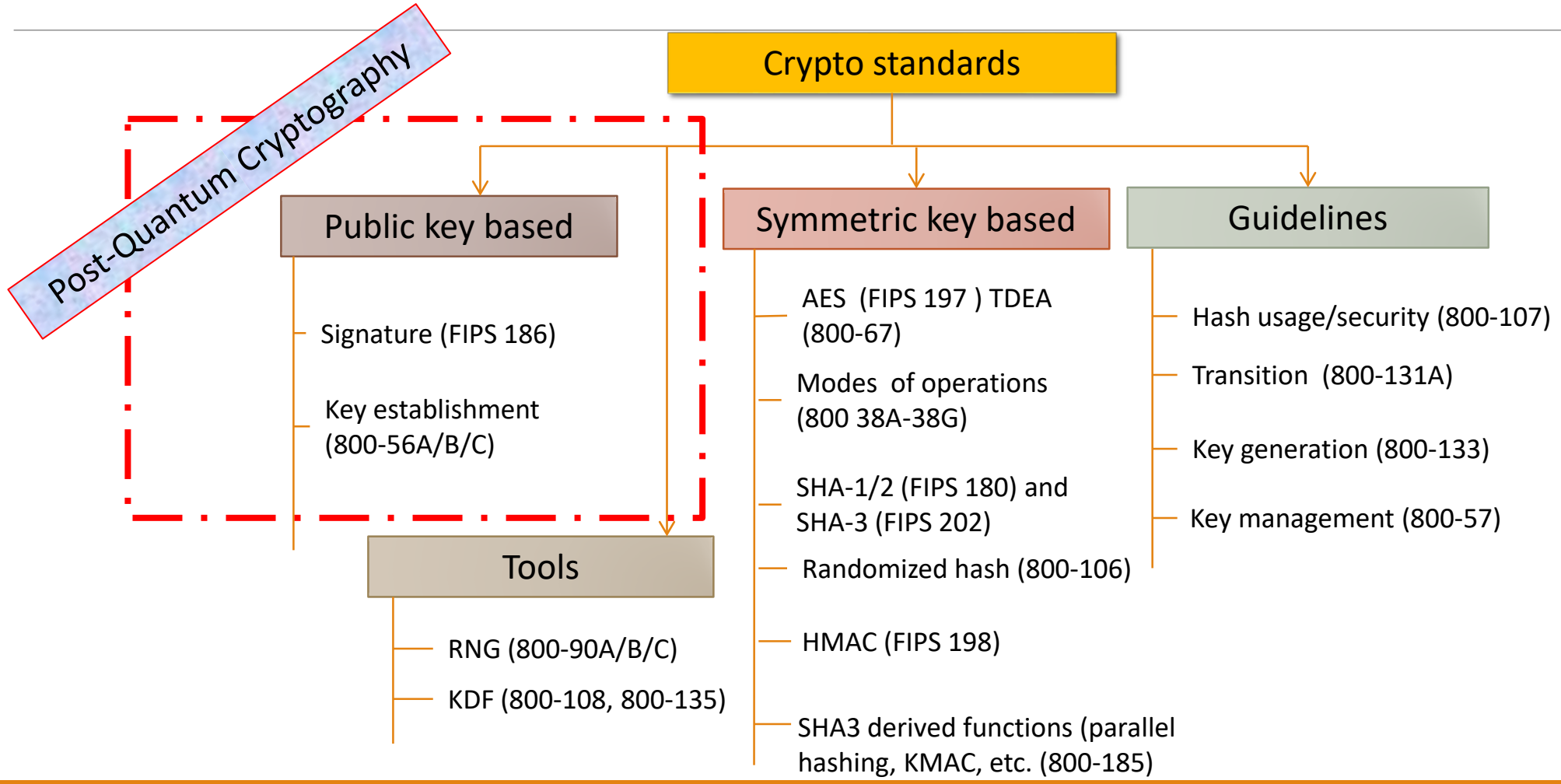
- RSA signatures, DSA and ECDSA (FIPS 186-4)
- Diffie-Hellman Key Agreement over finite fields and elliptic curves(NIST SP 800-56A)
- RSA encryption (NIST SP 800-56B)

We have to look for quantum-resistant counterparts for these cryptosystems

Quantum computing also impacted security strength of symmetric key based cryptography algorithms

- Grover's algorithm can find n bits AES key with approximately $\sqrt{2^n}$ operations
- Intuitively, we should double the key length, if 2^{64} quantum operations cost about the same as 2^{64} classical operations

Quantum Impact to NIST Standards



NIST Team has been in action

2012 – NIST begin PQC project
- Research and build NIST team

April 2015 – 1st NIST PQC workshop

Feb 2016 – NIST Report on PQC (NISTIR 8105)

Feb 2016 – NIST preliminary announcement of standardization plan

Aug 2016 – Draft submission requirements and evaluation criteria released for public comments

Sep 2016 – Comment period ends

Dec 2016 – Announcement of finalized requirements and criteria(Federal Register Notice)

Nov. 30, 2017 – Submission deadline, received 82 submissions

Dec. 24, 2017 – Announced the first round 69 algorithms, as “complete and proper”

NIST Timeline

NIST will hold the first PQC Standardization Conference in April 11-13, 2018

Initial analysis phase 12-18 months

Narrow the pool and hold the second workshop in late 2019

Second analysis phase 12-18 month

May take third analysis phase if needed

Expect draft standards in 2022-2023

Transition Guidelines will be provided after standards are published

Summary

Cryptography transition is critical to securely use cryptographic algorithms and methods

The transition is not restricted to algorithms and key lengths but many details for security implementations

NIST team relies on input from research and application community to justify transition and provide practical guidance

Specific messages for

- Designers: consider crypto agility to accommodate potential transitions
- Government users: look for FIPS 140 validated cryptography modules
- System administrators: follow NIST guidelines for configuring specific application servers and clients