SNIA DEVELOPER CONFERENCE
SDC 24
BY Developers FOR Developers

September 16-18, 2024
Santa Clara, CA

Changes in Encryption and Other Security Algorithms

Paul Suhler

Principal Engineer, SSD Standards, KIOXIA

Chair, IEEE Security in Storage Working Group

Overview

- Changes Coming in the IEEE 1619 XTS-AES Algorithm
- Post Quantum Cryptographic Algorithms
- Trends in Sanitization Techniques
- New Standards and Standards Setting Organization Interactions
- Call to Action

Changes Coming in IEEE 1619 (Standard for Cryptographic Protection of Data on Block-Oriented Storage Devices)

IEEE 1619 – Changing Requirements

- IEEE 1619-2018 defines the XTS-AES encryption mode, which is approved for use in FIPS 140-3 certifications.
- SP 800-140C Rev. 2 (Approved Security Functions) section 6.2.2 lists:
- SP 800-38E (*Recommendation for Block Cipher Modes of Operation: The XTS-AES Mode for Confidentiality on Storage Devices)*, which refers to the old IEEE 1619-2007.
- NIST has pointed out a problem (see next slide) that will weaken security as drives become larger.
- When IEEE publishes the new 1619, NIST will update 800-38E to point to the new 1619.

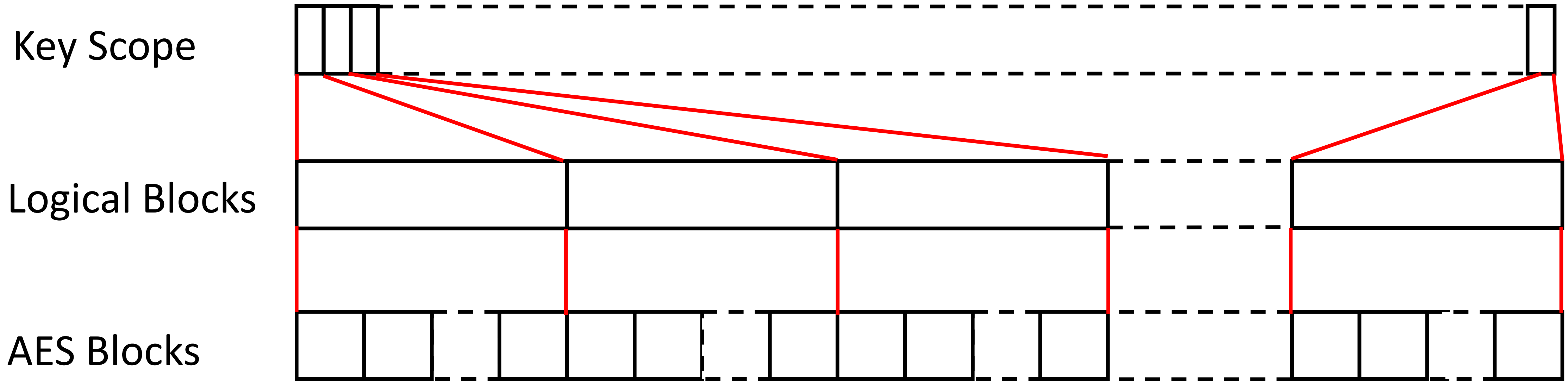
IEEE 1619 – Previous Requirements

- “Key Scope” is the amount of data that can be encrypted with a particular key, expressed in 128-bit AES blocks.
- IEEE 1619-2018 allowed up to 2^{64} AES blocks in a key scope (and earlier versions, e.g., 2007, were even more lenient).
- That is 2^{68} bytes, about 256 exabytes.
- But that large size is a problem …

IEEE 1619 – Problem!

- The more data that is encrypted with a single key, the better the chance an attacker can derive the encryption key and read the data.
  - 1 petabyte would give a success rate of 2^{-37} (eight in a trillion).
  - 1 exabyte (1000 petabytes) would give a success rate of 2^{-17} (eight in a million).
- NIST suggested that SISWG reduce the size of the Key Scope.
- 1619 -2024 will require:
  - The Key Scope ***shall not*** exceed 2^{44} blocks (256 TiB).
  - The Key Scope ***should not*** exceed 2^{36} blocks (1 TiB).
  - The Data Unit shall not exceed 2^{20} blocks (16 MiB).

IEEE 1619 – Data Elements

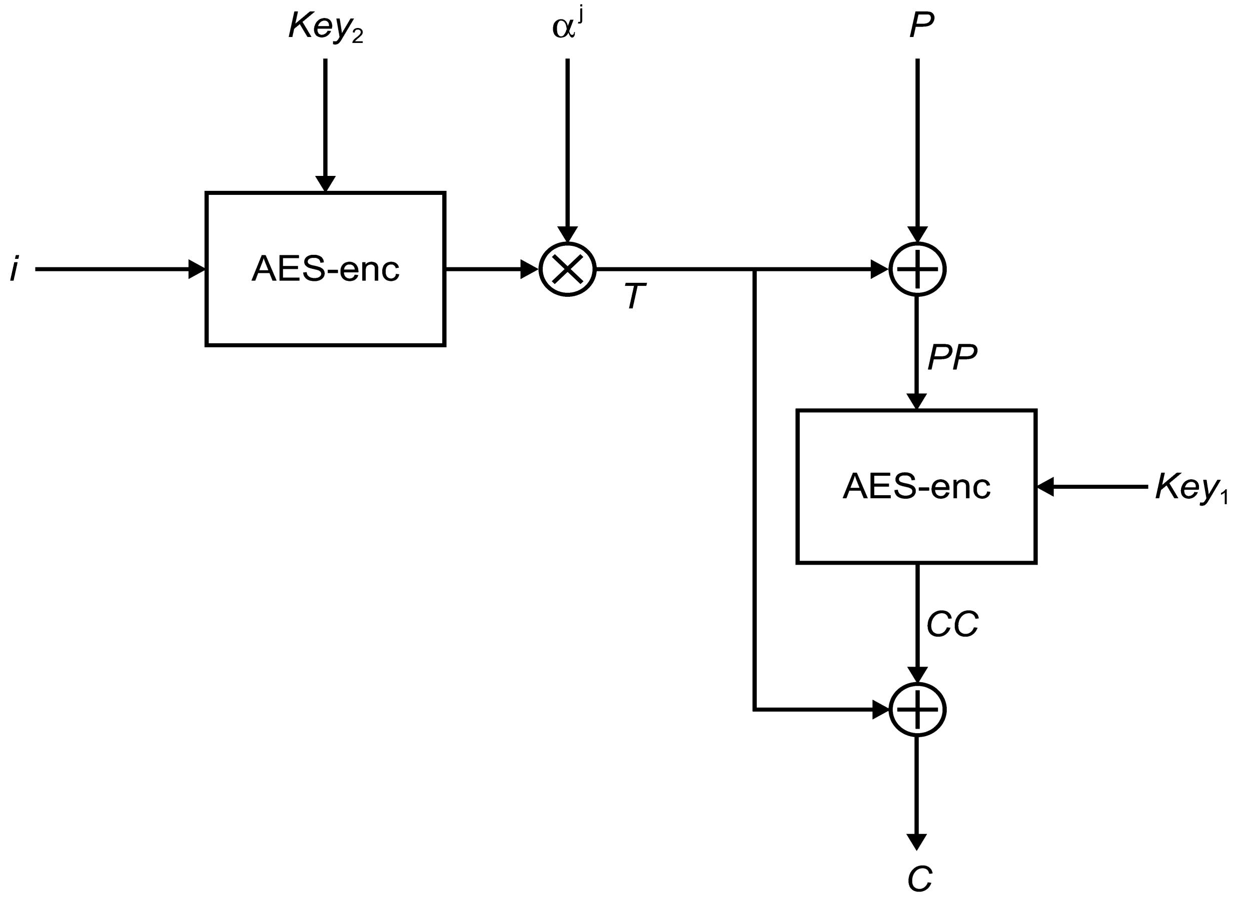


Example sizes:

Logical Block:	4 KiB
AES Blocks per LB:	256

XTS-AES Encryption

- The XTS-AES secret key is composed of Key1 and Key2. (Key = Key1 | Key2)
  - P is the user data (plaintext) being encrypted – a logical block.
  - C is the encrypted user data (ciphertext).
  - ⊗ is modular multiplication over the binary field GF(2).
  - "i" is often implemented as the logical block address (LBA).
  - "j" is the index of the AES block within that logical block.
- The LBA is encrypted to produce T, which is XOR-ed with the incoming plaintext and outgoing ciphertext.
- Decryption operates similarly.



IEEE 1619 – What Does This Mean to Me?

- These changes will affect upcoming implementations…
- Previously, a drive was effectively not required to have more than one key.
- Now, following the mandatory, more lenient requirement, the drive must maintain a separate key for approximately each 256 TB of data.
- Following the optional, more stringent requirement (1 TiB per key) a 32 TB drive will need to keep 32 keys.
- Drive must track how many AES blocks have been have been encrypted with each key.
- Drive must track which key is used to encrypt each logical block. This can be implemented in multiple way.
- We do not know what NIST will require.

IEEE 1619 – Changing a Logical Block Inefficiently

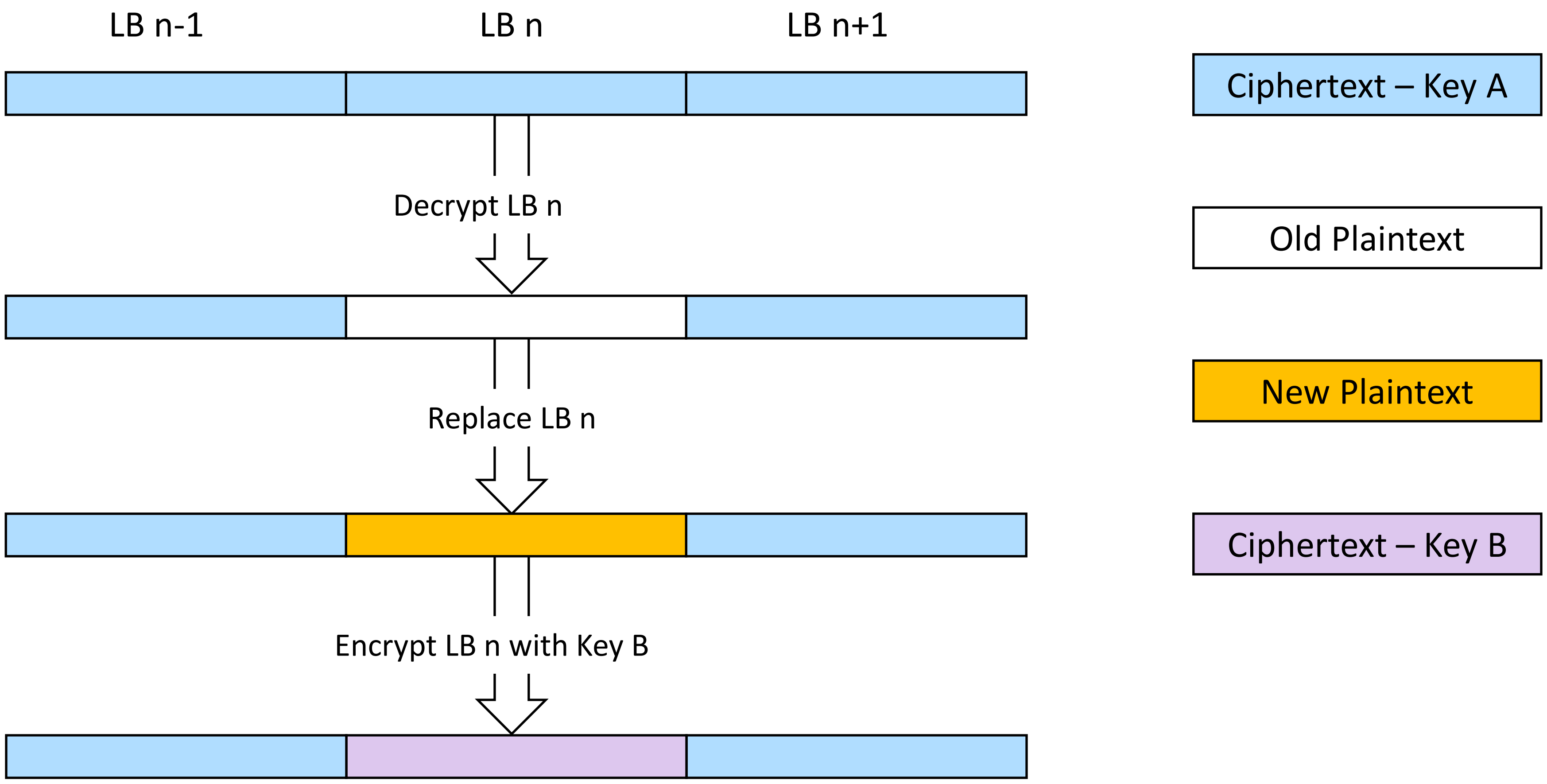
Key A has been used to encrypt the maximum number of AES blocks.

1. Decrypt Logical Block n.
2. Replace Logical Block.
3. See that Key A has reached its Key Scope.
4. Encrypt Data Unit with new key B.

Key A must be retained for decryption.

Key B must be retained for encryption and decryption.

Remember which key is used for each logical block.



IEEE 1619 – Possible Drive Implementations

- Key Scope per namespace – not a big departure from current implementations.
- TCG Opal Configurable Namespace Locking (CNL)
  - Supports up to 1024 different keys for the device, each namespace, LBA ranges within namespaces.
  - Up to 1024 Key Scopes per device.
- Keep a “current key” and do all new encryption with that key, until its Key Scope is maxed out, then add a key.
  - Tracking which key is used for a LBA is resource-intensive.

IEEE 1619 – Implementation Details

- Deallocated logical blocks – existing in media that has not been erased – still count against the amount of data encrypted with a key.
- Performing a Crypto Erase of a drive requires eradicating all keys.
  - One optimization would be to have the actual media encryption key – the key entered into the encryption engine – generated by XOR-ing each key with a unique key for the device. Eradicating the unique key will effectively eradicate all of the keys in one operation.

IEEE 1619 – Encryption by Host

- Host encrypts data and writes ciphertext to drive.
- Threat: Adversary may snarf ciphertext in flight to drive, and save it for offline analysis.
- Host must be responsible for tracking Key Scopes.

IEEE 1619 – Key Per I/O

- Key Per I/O is an NVM Express capability which allows the host to manage keys.
  - Host gets keys from a key management appliance and injects them into the drive, which keeps them in volatile storage.
    - (Injection uses a mechanism defined by the Trusted Computing Group.)
  - Host specifies in each I/O command which key to use.
  - Power cycling drive erases all keys.
- Host would have to enforce Key Scope requirements.
- It would be very difficult for a drive to enforce compliance with Key Scope requirements.

IEEE 1619 – Call to Action

- Drive vendors: Analyze your new designs.
  - Implement multiple keys.
  - Track Key Scopes
- Host software vendors:
  - Modify host software using Key Per I/O to add tracking of Key Scopes.
  - Modify host software implementing XTS-AES encryption to add tracking of Key Scopes.

SDC 24

Post Quantum Cryptographic Algorithms

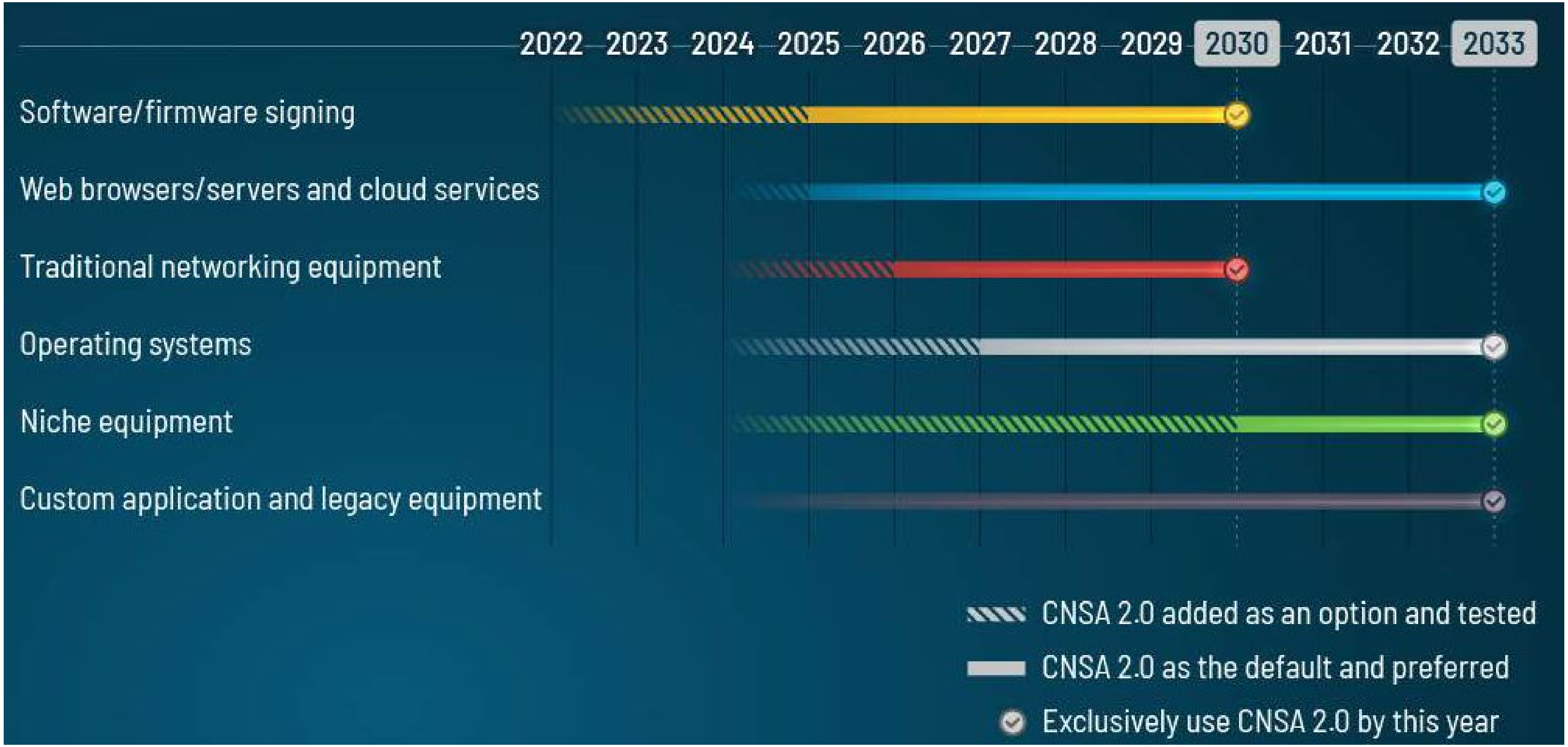
The Problem

- In 1994, Peter Shor devised an algorithm that a future quantum computer could use to find prime factors of integers in polynomial time.
- This breaks asymmetric encryption algorithms that are at the heart of public key infrastructure protocols used for authentication:
  - RSA (Rivest-Shamir-Adleman)
  - Finite field Diffie-Hellman key exchange
  - Elliptic curve Diffie-Hellman key exchange
- “Cryptographically relevant” quantum computers are on the horizon.
- Quantum-resistant (or PQC) algorithms have been developed and implemented in commercial products.

Post Quantum Cryptography (PQC) Overview

- US government deadlines for support by products
- PQC algorithms in CNSA 2.0 suite
- PQC algorithms in other standards

Commercial National Security Algorithm (CNSA) Suite 2.0 Timeline



Source: "Transitioning National Security Systems to a Post Quantum Future", Morgan Stern, Fourth PQC Standardization Conference, 2022-11-30

Products Must Meet the Timeline

- CNSA 2.0 requires products to be sold to the US government to implement algorithms that include post quantum cryptography (PQC).
- Products are often expected to have a seven-year lifetime.
- In principle, products implementing PQC must be certified and ready to ship seven years before the deadlines.

Commercial National Security Algorithm (CNSA) Suite 2.0

- Applies to National Security System (NSS) owners and operators (and vendors).
- Includes algorithms resistant to attacks by cryptographically relevant quantum computers.
  - FIPS 197 – Advanced Encryption Standard: 256-bit keys required (128-bit and 192-bit keys deprecated)
  - FIPS 203 – Module-Lattice-Based Key-Encapsulation Mechanism Standard (ML-KEM) (CRYSTALS-Kyber)
  - FIPS 204 – Module-Lattice-Based Digital Signature Standard (ML-DSA) (CRYSTALS-Dilithium)
  - FIPS 180-4 – Secure Hash Algorithm (SHA): SHA-384 or SHA-512 required
  - SP 800-208 – Signing firmware and software: Leighton-Micali Signature (LMS) and Xtended Merkle Signature Scheme (XMSS)
- **Deprecated**: RSA, Diffie-Hellman (DH), and elliptic curve cryptography (ECDH and ECDSA)
  - Quantum computer can quickly factor products of large primes (Shor's algorithm).
- Deadline: Transition to QR algorithms for NSS to be complete by 2035.
- Details: NIST.CSWP.29.pdf

PQC Algorithms

- Newly published:
  - FIPS 203: Module-Lattice-Based Key-Encapsulation Mechanism Standard (ML-KEM) (CRYSTALS-Dilithium)
  - FIPS 204: Module-Lattice-Based Digital Signature Standard (ML-DSA) (CRYSTALS-KYBER)
- Not part of CNSA 2.0:
  - FIPS 205: Stateless Hash-Based Digital Signature Standard (SLH-DSA) (SPHINCS+)
- Upcoming:
  - FIPS 206: FFT (fast-Fourier transform) over NTRU-Lattice-Based Digital Signature Algorithm (FN-DSA) (Falcon)

Transition to PQC: Hybrid Algorithms

- "Hybrid" algorithms will allow PQC and non-PQC devices to interoperate during a transition period.
  - Certificate signing
  - TLS key exchange
- PCQ keys are large and will be integrated into certificates and protocols.
- Most work is being done by the Internet Engineering Task Force (IETF).
  - Terminology for Post-Quantum Traditional Hybrid Schemes
  - Hybrid key exchange in TLS 1.3
  - Post-Quantum Traditional (PQ/T) Hybrid Authentication in the Internet Key Exchange Version 2 (IKEv2)
  - PQ/T Hybrid KEM: HPKE with JOSE/COSE
  - Enhancing Security in EAP-AKA' with Hybrid Post-Quantum Cryptography

Change in Focus of Standardization Activities

- Most activity had been on specifying the PQC algorithms.
- Now the focus is shifting to protocols that use PQC algorithms (SPDM, DICE, etc.)
- Vendors shouldn’t assume they’ll be given a pass.

Incorporation into Other Standards

- Distributed Management Task Force (DMTF)
  - Security Protocols and Data Models (SPDM) 1.4.0 will probably add FIPS 203 ML-KEM and FIPS 204 ML-DSA by early 2025. (DSP0274)
- Trusted Computing Group (TCG)
  - Device Identifier Composition Engine (DICE)
  - Core architecture
  - Opal family of standards
  - Enterprise SSC
  - Key Per I/O

Trends in Sanitization Techniques

Sanitization Trends – Terminology

- IEEE Std 2883™-2022 defines three techniques for purging user data:
  - **Cryptographic Erase**: All data is encrypted on the media and Crypto Erase eradicates all media encryption keys. The fastest technique.
  - **Block Erase**: All media in an SSD that contains user data is erased. Time depends on how many media erase blocks can be erased at the same time.
  - **Overwrite**: Writes a known pattern to all media. This is a holdover from HDDs, and is the slowest technique. Increases write amplification for NAND-based SSDs, reducing drive lifetime.

Sanitization Trends – Interesting Use Cases

- Post-Sanitize Media Verification:
  - Customers may require reading sanitized media to confirm that previous data is not accessible.
  - Problem: Crypto Erase and Block Erase techniques leave sanitized media with invalid ECC, causing read errors.
  - Allows successful reads of media sanitized by Crypto Erase or Block Erase.
  - NVM Express 2.1 family of specifications defines the mechanism.
- Single-Namespace Purge:
  - Crypto Erase is the only generally-applicable technique.
  - Media encryption keys are not shared by namespaces.
  - Media may contain user data from different namespaces, most of which must remain valid.
  - Some HDD implementations may be able to support the Overwrite technique.

Sanitization Trends – Use Cases for Crypto Erase

- Large storage devices:
  - The Overwrite and Block Erase techniques take a long time.
  - The larger the device, the greater the advantage of Crypto Erase.
- Distributed and virtualized storage systems:
  - One user's data may be scattered across multiple physical devices and intermixed with other users' encrypted data.
  - Crypto Erase avoids the need to purge data on multiple devices.
  - Dispersed namespaces (NVM Express) can be considered a form of virtualized storage.

Sanitization and Sustainability

- Organizations with highly-sensitive data – e.g., the National Security Agency – still rely on destruction ("shredding") of devices that are no longer used.
- They have found instances in which a device sanitize command reports successful completion, but the user data can still be extracted.
- Disassembly of devices prior to shredding to feed different components into separate recycling streams is too labor intensive, and does not scale.
- Lack of provable data eradication is an impediment to adopting methods other than Destruct.

New Standards and Standards Setting Organization Interactions

Standards Relationships

- ISO/IEC 27040 uses content defined in:
  - IEEE 2883 (current)
  - IEEE P2883.1 (future)
  - IEEE P2883.2 (future)
- NIST SP800-38E (new) will use content defined in the new IEEE 1619.
- NSA Commercial National Security Algorithm (CNSA) 2.0 Suite will use content defined in various NIST standards.
- NVM Express Base Specification 2.1 uses definitions from IEEE 2883.

Emerging IEEE Standards

- P2883.1 – Recommended Practice for the Use of Storage Sanitization Methods
- P2883.2 – Recommended Practice for Virtualized and Cloud Storage Sanitization
  - SISWG is soliciting participation by system vendors. Contact the speaker.
- P3406 – Standard for a Purge and Destruct Sanitization Framework
- P1667 – Standard for Discovery, Authentication, and Authorization in Host Attachments of Storage Devices (revision of 2018 standard)
- P2883 – Standard for Sanitizing Storage (revision of 2022 standard).

Call to Action

Call to Action

- Understand which standards apply to the products you sell or buy.
- Evaluate the needed changes to your product specifications and purchase specification.
- Implement the changes in your storage devices and host software.
- Make your voice heard in the standards groups.

- Contact the speaker for assistance.

Please take a moment to rate this session.

Your feedback is important to us.

