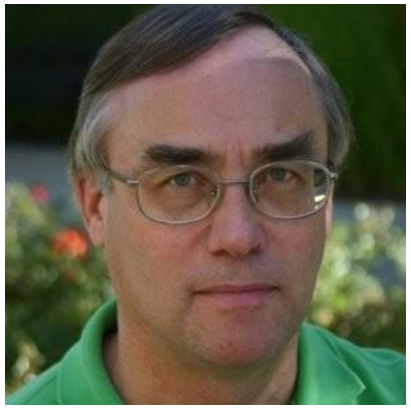
SNIA | Data, Storage & Networking

The Storage Security Shake-Up: Adapt Now or Get Left Behind

Live Webinar
January 28, 2026
12:00 pm PT / 3:00 pm ET

Today's Presenters

Erik Smith
Distinguished Engineer
Dell Technologies
Moderator



Paul Suhler
Principal Engineer
KIOXIA

Eric Hibbard
Director, Product Planning
Samsung

Ramaswamy Chandramouli
NIST

The SNIA Community

200
industry leading organizations

2,000
active contributing members

50,000
IT end users & storage pros worldwide

SNIA | DSN A SNIA Community

SNIA | Data, Storage & Networking

What We Do

Drive the awareness and adoption of a broad set of technologies, including:

- Storage Protocols (Block, File, Object)
- Traditional and software-defined storage
- Disaggregated, virtualized and hyperconverged
- AI, including storage and networking considerations
- Edge implementation opportunities and factors
- Storage and networking security
- Acceleration and offloads
- Programming frameworks
- Sustainability

How We Do It

By delivering:

- Expert webinars and podcasts
- White papers
- Articles in trade journals
- Blogs
- Social Media
- Presentations at industry events

Logistics

- The slides are available under the attachments tab at the bottom of your console.
- Questions are welcome!
- Please rate the session and provide feedback!
- Want more sessions like this or other topics, let us know!
  - JOIN US! We meet on Thursday mornings at 11:00 AM eastern.
  - Email dsn-chair@snia.com if you have questions.

SNIA Legal Notice

- The material contained in this presentation is copyrighted by SNIA unless otherwise noted.
- Member companies and individual members may use this material in presentations and literature under the following conditions:
  - Any slide or slides used must be reproduced in their entirety without modification
  - SNIA must be acknowledged as the source of any material used in the body of any document containing material from these presentations.
- This presentation is a project of SNIA.
- Neither the author nor the presenter is an attorney and nothing in this presentation is intended to be, or should be construed as legal advice or an opinion of counsel. If you need legal advice or a legal opinion please contact your attorney.
- The information presented herein represents the author's personal opinion and current understanding of the relevant issues involved. The author, the presenter, and the SNIA do not assume any responsibility or liability for damages arising out of any reliance on or use of this information.

  NO WARRANTIES, EXPRESS OR IMPLIED. USE AT YOUR OWN RISK.

Agenda

- Storage Security Standardization 101
- Storage Security and Broader Security
- Storage Handling/Disposal
- Future Directions

A Little Traveling Music…

- ISO/IEC 27001:2022 *Information security, cybersecurity and privacy protection — Information security management systems — Requirements*
- ISO/IEC 27002:2022 *Information security, cybersecurity and privacy protection — Information security controls*
- ISO/IEC 27040:2024 *Information technology — Security techniques — Storage security*
- IEEE Std 2883™ *IEEE Standard for Sanitizing Storage*
- IEEE Std 2883.1™ *IEEE Recommended Practice for Use of Storage Sanitization Methods*
- NIST SP 800-88r2 *Guidelines for Media Sanitization*
- NIST SP 800-209 *Security Guidelines for Storage Infrastructure*

A QUICK POLL

What Shake-Up?

- Data continue to be the “coin” of the realm
- Attackers seek to destroy, corrupt, and deny access to this data
- Storage is a target

- Cybersecurity community has recognized the need to protect storage
- International standards are being adjusted
- Auditors are explicitly checking on storage

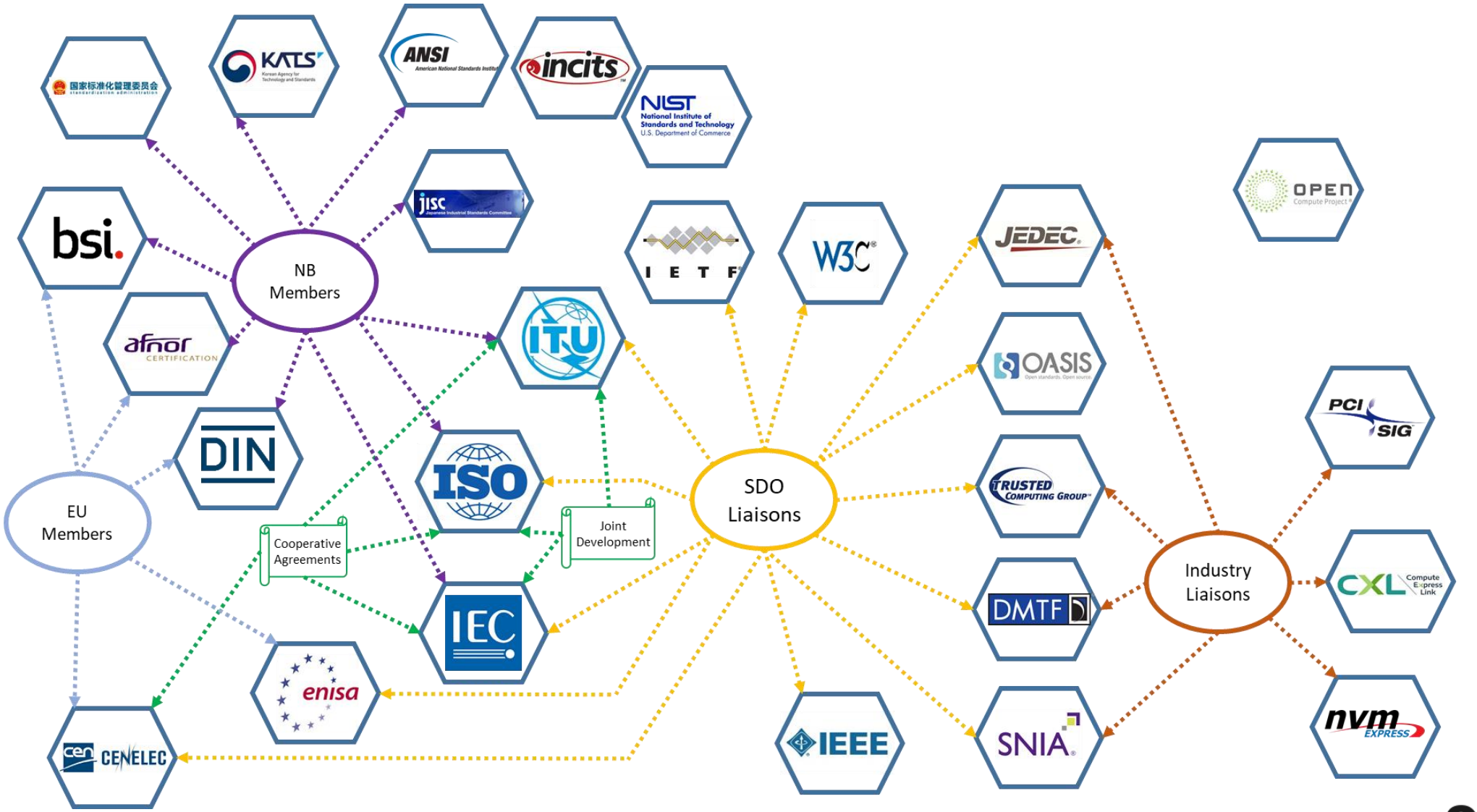
Underpinnings of the Storage Security Shake-Up

- ISO/IEC 27001 & ISO/IEC 27002 published in 2022
  - Includes storage security elements; references ISO/IEC 27040
  - Certifications based on 2013 versions not valid after December 2025

- NIST Special Publication 800-209 published October 2020
- IEEE Std 2883™ published in 2022
- ISO/IEC 27040 (2nd Ed.) published January 2024
- NIST Special Publication 800-88 rev. 2 published September 2025

- More storage security standards and specifications on the way

Many Players Impacting Storage Security



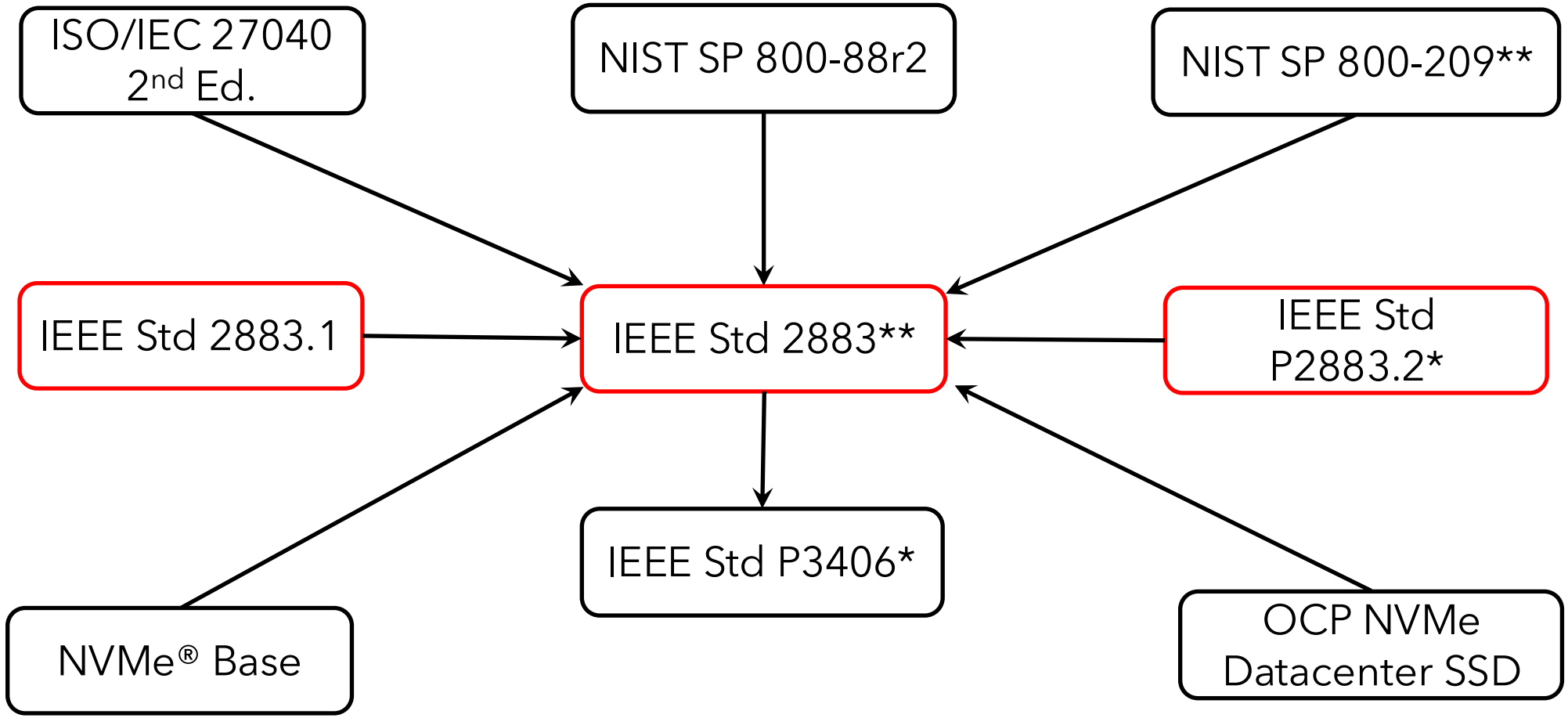
Significance of ISO/IEC Work

- International relevance
- Formal information security management certification
- Storage is now visible to security professionals and auditors
- Storage security requirements
  - Broad coverage of storage technologies and practices
  - Anchor for security compliance claims for storage

Storage Reuse and Disposal

- Destruction of storage devices/media is becoming less acceptable by many organizations
- Maintaining appropriate data confidentiality is paramount
- Eliminating data can be challenging
- Failures can result in costly data breaches

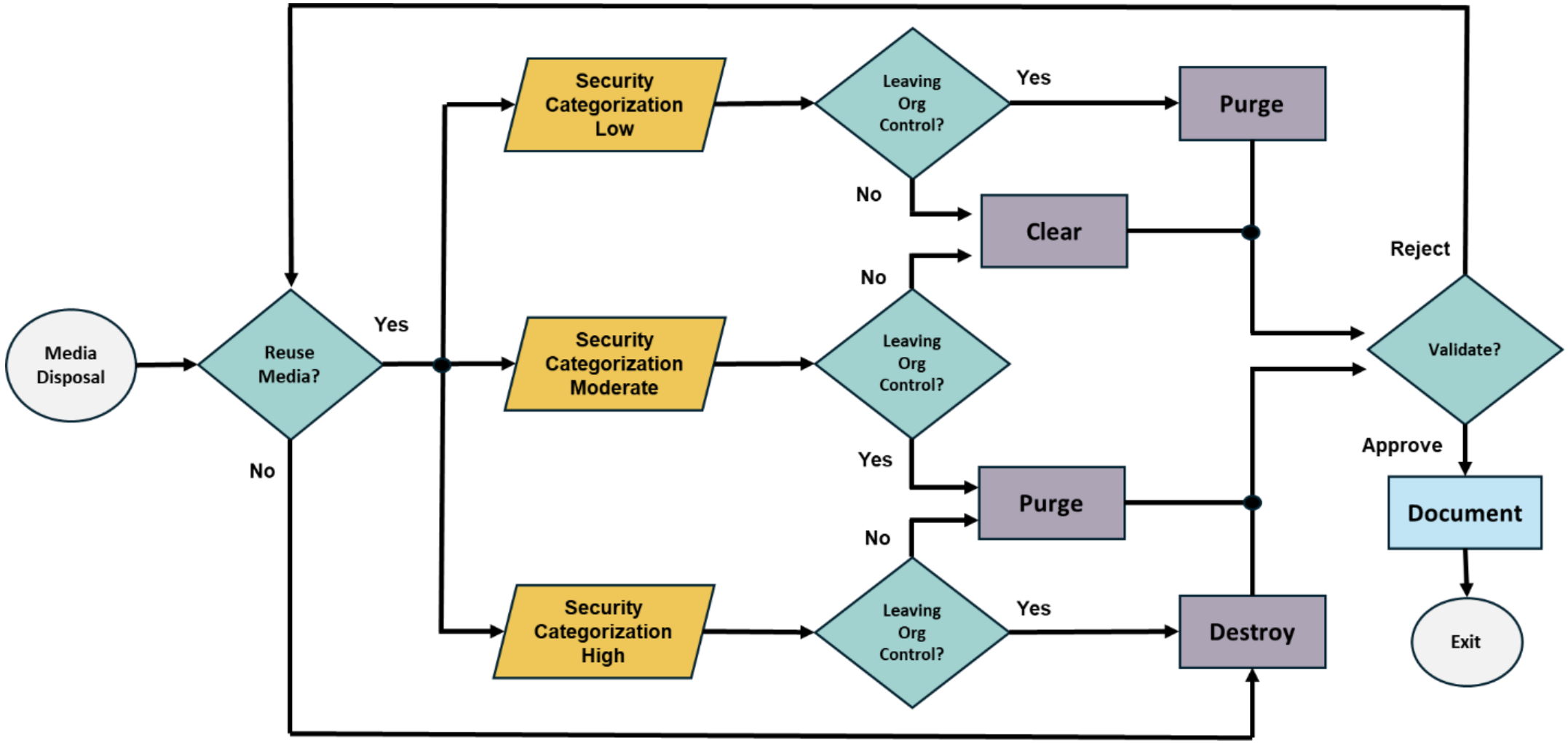
Media & Data Sanitization Standards



* New Document under development
** Revision in progress

SNIA DSN A SNIA Community

Sanitization and Disposition Decision Flow (SP800-88r2)



SNIA DSN A SNIA Community

SNIA | DSN
A SNIA Community

PANEL Q&A

After this Webinar

- Please rate this webinar and provide us with your feedback
- This webinar and a copy of the slides are available at the SNIA Educational Library snia.org/educational-library
- A Q&A from this webinar, including answers to questions we couldn't get to today, will be posted on our blog at sniablog.org
- Follow us on LinkedIn and X @SNIA

SNIA | DSN
A SNIA Community

Thank You

SNIA | DSN
A SNIA Community

Background Slides

References

- ISO/IEC 27001:2022 *Information security, cybersecurity and privacy protection — Information security management systems — Requirements*
- ISO/IEC 27002:2022 *Information security, cybersecurity and privacy protection — Information security controls*
- ISO/IEC 27040:2024 *Information technology — Security techniques — Storage security*
- IEEE Std 2883™ *IEEE Standard for Sanitizing Storage*
- IEEE Std 2883.1™ *IEEE Recommended Practice for Use of Storage Sanitization Methods*
- IEEE Std P2883.2™ *IEEE Recommended Practice for Virtualized and Cloud Storage Sanitization*
- IEEE Std P3406™ *IEEE Standard for a Purge and Destruct Sanitization Framework*
- NIST SP 800-88r2 *Guidelines for Media Sanitization*
- NIST SP 800-209 *Security Guidelines for Storage Infrastructure*
- NIST SP 800-38E *Recommendation for Block Cipher Modes of Operation: The XTS-AES Mode for Confidentiality on Storage Devices*

Existing Standards

- ISO/IEC 27001 provides requirements for media handling and disposal and leverages ISO/IEC 27002 for security controls
- ISO/IEC 27002 provides some guidance on storage security topics and defers to ISO/IEC 27040 for additional controls
- ISO/IEC 27040 provides requirements and guidance for storage security
- NIST SP 800-209 provides guidance for storage infrastructure
- NIST SP800-88r2 provide guidance to organizations about sanitization and refer to IEEE Std 2883 for specific sanitization requirements.
- IEEE Std 2883™-2022 defines requirements for sanitization methods and techniques.
- IEEE Std 2883.1-2025 provides guidance to organizations for choosing sanitization methods. It refers to IEEE Std 2883.

Standards Under Development

- NIST SP 800-209r1 will provide update guidance for storage infrastructure
- IEEE Std 3406 will provide requirements for implementing the Purge and Destruct techniques.
- A new version of IEEE Std 2883 will refer to IEEE Std 3406.
- IEEE Std 2883.2 will provide guidance for sanitizing data in cloud and virtual storage systems. It will refer to IEEE Std 2883.

Relevant Industry Specifications

- NVM Express® Base Specification refers to IEEE Std 2883 for Purge requirements.
- Open Compute Project Datacenter NVMe® SSD Specification refers to IEEE Std 2883 for Purge requirements
- Open Compute Project L.O.C.K. (Layered Open-source Cryptographic Key management) Specification identifies fuse-based sanitization
- Trusted Computing Group Storage Feature Set: MEK Multiparty Authorization provides for external keys to be used for access control and sanitization

Storage Security Summary

- Storage threats and risks
- Covers organizational, people, physical, and technological controls for storage
- Addresses common practices as well as design and implementation of storage systems and ecosystems
- Broad coverage for all major types storage technology and protocols
- Includes cloud storage, data archives and data repositories
- Addresses secure multi-tenancy and secure autonomous data movement

Sanitization Standards

- Sanitization of data in storage devices uses the Clear, Purge, and Destruct methods.
  - Clear prevents sanitized data from being read over the interface.
  - Purge makes recovery of the sanitized data resistant to “advanced laboratory techniques”. It leaves the device potentially operational.
  - Destruct is the most certain method but is expensive and creates waste.
  - All sanitization techniques under “clear” and most techniques under “Purge” comes under Logical Sanitization while 100% under “Destruct” comes under Physical Sanitization.
- Organizations evaluate the sensitivity of their data and the risk of an opponent recovering the data and decide on which method to use. (The decision process is illustrated through the following diagram)

Sanitization Standards – Open Questions

- What are the differences between clear and purge methods?
- Should “resistant to advanced laboratory techniques” remain the threshold for the Purge method?
- Is degaussing a purge or destructive technique?
- What constitutes “proof” of sanitization?

XTS-AES Encryption Algorithm

- This algorithm is used in most self-encrypting drives (SED).

- IEEE Std 1619-2025 defines the algorithm.
- NIST SP 800-38E stated that XTS-AES as defined in 1619-2007 was acceptable if additional requirements were met.
- FIPS 140-3 Implementation Guidance (IG) for XTS-AES refers to SP 800-38E.

- Previous versions of IEEE Std 1619 allowed essentially unlimited amounts of data to be encrypted with the same key (“key scope”) but warned that large amounts of data increase the risk of brute-force discovery of the key.
- Drives are now large enough and decryption tools are fast enough that the risk is high.

XTS-AES Encryption

- The 2025 revision of IEEE Std 1619 places limits on the key scope:
  - Recommends 1 TiB maximum
  - Requires 256 TiB maximum
- SP 800-38E is being revised to approve the requirements in IEEE Std 1619-2025 without having to add additional requirements.

- This may require changes to most SEDs.
- Be alert for changes to FIPS 140-3 IG after SP 800-38E is updated.

Encryption Standards