

Public Comments on the SP 800-57, Parts 2 and 3

Comment period: July 1, 2025 – September 30, 2025

On July 1, 2025, NIST’s Crypto Publication Review Board initiated a [review](#) of Parts 2 and 3 of SP 800-57, *Recommendation for Key Management*.

The comments received by NIST during the comment period are collected below.

More information about this review is available from NIST’s [Crypto Publication Review Project site](#).

LIST OF COMMENTS

1. Comments from Daniel Cervera and Mark Svancarek (Microsoft Corporation), 10/3/25 2

**1. Comments from Daniel Cervera and Mark Svancarek (Microsoft Corporation),
10/3/25**

Dear NIST SP 800-57 Part 2 and Part 3 Authors:

Microsoft welcomes the opportunity to provide feedback to NIST regarding the request for public comment on the *Recommendation for Key Management: Part 2 – Best Practices for Key Management Organizations* and *Part 3 – Application-Specific Key Management Guidance Drafts*.

After careful review, Microsoft’s Daniel Cervera, PKI Security Assurance Program Manager, has offered the following recommendations for both documents that we believe would increase its effectiveness and improve its use.

Part 2 – Best Practices for Key Management Organizations

Comment	Section/Context	Comment Text
1	Authority (last line re: FISMA/OMB Circular A-130)	Referenced throughout this document. Although still foundational, interpretations may have evolved with FISMA updates and Executive Order 14028 (2021) on improving cybersecurity... still in effect, unamended.
2	<ul style="list-style-type: none"> • Glossary: "Internet Key Exchange (IKE)" • Section 2.1.3: Available Automated Key Management Schemes and Protocols • Appendix D: References 	Suggest noting that RFC 5996 was obsoleted by RFC 7296 wherever RFC 5996 is referred to for clarity.
3	Glossary, "Transport Layer Security (TLS)"	SP 800-52 now mandates TLS 1.3 by 2024. Should omit reference to TLS 1.0.
4	Section 3.1.3 after "IT System Examination"	NEW SECTION: Recommend enhancing integration of key management practices with broader organizational risk management processes. Alternatively, this could fit under section 3.2.1 ("Key Management Planning Process"). This language is also in keeping with Dr. Ron Ross’s presentation on Impact Levels & Security Controls , delivered at the 2014 NIST Cryptographic Key Management Workshop.

Comment	Section/Context	Comment Text
5	Section 5, Footnote 87 (re: NISTIR 7924)	Seems to have been abandoned but would love to see this work finished and published.
6	Section 5, Footnote 91 (re: 800-71 Draft)	Still in Draft status, but with 2018 news post update.
7	Section 6.2.13 Key Backup, Archiving and Recovery (re: OMB Guidance)	Over two decades old.... For an updated authoritative reference, OMB Circular A-130 (July 28, 2016) subsumes earlier directives and requires balancing encryption with data availability; OMB M-07-16 (2007) offers additional encryption requirements which might be pertinent. Alternatively, Executive Order 14144 Section 4 seems to still be in effect, despite amendments made by Executive Order 14306 .
8	Appendix D, References (re: DoD Policy)	Since been updated, but perhaps there's a landing page to replace this with instead: DoD X.509 CP
9	Appendix D, References (re : FIPS 186)	Superseded by FIPS 186-5, which includes updates for digital signatures and recommendations for discrete logarithm-based cryptography (with SP 800-186).
10	Appendix D, References (NISTIR 7924)	Appears to have been abandoned, but please consider reviving, with our support if ever interested.
11	Appendix D, References (re : PDD63)	Might be superseded by HSPD-7 (2003) , and PPD-21 (2013) on critical infrastructure cybersecurity.
12	Appendix D, References (re: SP 800-53)	No longer in draft.
13	Appendix D, References (re: SP 800-53A)	Rev 4 superseded by Rev 5.
14	Appendix D, References (re : SP 800-56C)	Superseded by Rev 2, which refines key-derivation methods, and a new draft up for review for a potential Rev 3.
15	Appendix D, References (re: SP 800-133)	Superseded by Rev 2.4
16	Appendix D, References (re: Treasury KR)	Has since been updated to version 4.0: Certificate Policies

Part 3 – Application-Specific Key Management Guidance Drafts

Comment	Section/Context	Comment Text
1	Section 1.3.2 Cryptographic Negotiation 2 nd paragraph (re: DES & 512 bit RSA)	Consider omitting references to DES & 512-bit RSA—suggest more modern algorithms/key strengths for thought experiments to avoid the appearance of implied approval.
2	Section 2.2.1 Recommended Key Sizes & Algorithms Table 2-1	Per SP 800-131A Revision 2 (2019), RSA/DSA 2048-bit deprecated for signatures after 2030. Should address ongoing transitions to 3072-bit RSA or elliptic curve cryptography (ECC) with P-384/P-521.
3	Section 5.2 Security and Compliance Issues 2 nd paragraph (re: FIPS 140-2)	FIPS 140-2 referenced throughout the document; Superseded by FIPS 140-3.
4	Section 5.2 Security and Compliance Issues Table 5-1 (re: Digital Signatures)	Per SP 800-131A Revision 2 (2019) / NIST SP 800-57, Part 1, [Private Signing Key Originator usage period for] DSA 2048-bit signatures must not persist beyond 2030. Public verification key Recipient Usage Period may persist (until.... ?). Consider clarifying.
5	Section 6.3 Procurement Guidance Item 5 (re: SHA-1)	SHA-1 signing suggested throughout the doc, but deprecated by 2013, fully disallowed for all new uses since 2017. (per SP 800-131A, which emphasizes migration to SHA-2/3 families).
6	Appendix D References (re: SP 800-57 Part 1)	Current version is Revision 5 (March 2020).
7	Appendix D References (re: SP 800-131A)	Superseded by Revision 2 (2019)

Microsoft appreciates the opportunity to contribute to these Special Publications and welcomes opportunities to partner with the agencies on the recommendations discussed.

Sincerely,
 Mark Svancarek
NIST Program Management Office
Microsoft Corporation