

Public Comments on the Proposal to Withdraw NIST Special Publication 800-15

Comment period: August 4, 2021 – September 3, 2021

On May 10, 2021, NIST’s Crypto Publication Review Board [initiated a review](#) of SP 800-15 *Minimum Interoperability Specification for PKI Components, Version 1*. After the review, NIST [proposed to withdraw](#) the standard. This document includes the public comments received during the comment period from August 4, 2021 to September 3, 2021.

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

LIST OF COMMENTS

1. Comments from Yuna, Joseph D. (CTR, AST-SSE).....2

1. Comments from Yuna, Joseph D. (CTR, AST-SSE) ¹

Item #	1	2
DOCUMENT UNDER REVISION	NIST SP800-15 Comments	NIST SP800-15 Comments
Requires Team Lead Review	Yes	Yes
COMMENT DATE	31-Aug-21	31-Aug-21
COMMENT SOURCE	Yuna, Joseph D. (CTR, AST-SSE)	Yuna, Joseph D. (CTR, AST-SSE)
COMMENT TYPE	Administrative	Substantive
PAGE	All	All
PARA	All	All
LINE	All	All
REVIEWER COMMENT	As the US Army seeks to replace PKI with other means such as Blockchain and biometrics, this standard remains basically unchanged from its original format and content.	This standard is of little use for the User of PKI, but a great resource for those responsible for its use within the trusted systems development, security and operational use.
REVIEWER RATIONALE	Observation with respect to PKI supporting the current CAC and CA processes.	Nothing here that would require a change in our SSECG v4.0 in my opinion. No further comments are offered at this time.

¹ Table was reformatted to fit in this paper.