Public Comments on NIST SP 800-15, *MISPC Minimum Interoperability Specification for PKI Components, Version 1*

Comment period: May 10, 2021 – June 11, 2021

On May 10, 2021, NIST's Crypto Publication Review Board initiated a review of NIST Special Publication (SP) 800-15, *MISPC Minimum Interoperability Specification for PKI Components, Version 1*. This document includes the public comments received during the comment period from May 10, 2021 to June 11, 2021.

More details about this review are available from NIST's Crypto Publication Review Project site.

LIST OF COMMENTS

1. Comments from Dr. Dwayne Hodges, USA, (Ret.), May 18, 2021

Responses for NIST SP 800-15 Minimum Interoperability Specification Components (MISPC), Version 1

1. The current version does not address confidentiality key management, this is a critical service for KMS, to support PKI.
2. Although we can assume that the requirement for cryptography is specified in FIPS 141 and FIPS 197, the interoperability and/or standards should be in this document for government systems.
    a. For example, RSA is defined in PKCS #1, and can be used with any hash algorithms, this document has FIPS 180-1 as the current standard, the current standard is FIPS 180-1, the current SHA algorithm is the only variant that should be used, despite RSA can use anyone.
3. NIST 800-15 Minimum Interoperability Specification Components (MISPC) focuses heaving only end users, it does not account for software, NPE, IOT, etc.
4. 800-15 Minimum Interoperability Specification Components (MISPC) only focuses on the 5 main components of the PKI (CA, ORA, Certificate holders, clients, and repositories)
    a. I would like to see a version that dives much deeper into the roles, requirements, use case, to include virtual and physical locations more all the components of the PKI, beyond the basic 5 components in this document to include the federal PKI infrastructure requirement, and for CNSS systems), right now it is very high level, and the document should consider when and where to use the following, rather than offering **definition and description** only, we should move toward **prescriptive** in such a way, the community knows how for **PKI, while the data structures offer the "what", they leave out the how and why; therefore the uncertainty of interoperability increase the chances of the PKI system not being designed securely to cybersecurity attacks.**
        i. Distribution points
        ii. Intermediate Cas,
        iii. Sub Cas
        iv. Additional and/or separate Ras
        v. Additional and/or separate CRLS
        vi. OSCP
5. Document should also answer:
    a. for Sub Cas, intermediate CA, separate RAs, to include technical specifications such as.
    b. When a PKI should have more than once CA and/or sub-CA
    c. When a CA should have more than one RA
    d. When a CA and or sub-CA should have more than once CRL
    e. These details should align with 800-32
    f. This document should in include high level OVs and flows that describe the components, for example on 1-2 PKI 5 components, and this OV should also align, with **NIST SP 800-32**, with current federal use cases.
6. This document does not mention the use of standardized protocols for certificate status, and only discusses trusted entities where the CAs signature is validated, there are lots of ongoing problems and issues with CRL management,
    a. I would love to see more exhaustive technical discussion in this area, to include talking about "certificate pinning" for both **internal and external** operations
    b. This document does not include any protocols for repositories to authenticate users
7. This document assumes that a CA, ORA, certificate holders will be physically separated, - this is a **poor assumption.**
    a. We should assume they are not, cannot- or state the risk, or federal structure
    b. As we move into a virtualized environment, It is foreseeable we can still encourage our engineers to physically separate at the hypervisor level, or entirely, but we should clarify this technical

speciation on OV in the " 5 major components ", my opinion is, it should be in both 800-15 and 800-32- things I would like to address for separation, - this detail is likely more necessary, than in the past, with the rise in cybersecurity attacks, as our novice workforce rely on NIST documentation for implantation!

i. The "***root' CA*** on one VM, the sub-CA on separate hardware, and/or VM
ii. The HSM on one VM, the root CA on separate hardware, VM

8. This document lacks guidance on **"how" and/or a mechanism to update directories,**
9. (.500)directories are the center of gravity for retrieval by all subscribers in a PKI
10. This document can use more technical explanation of the use of extensions. These extensions were introduced in version 3 for x509, and may offer great value in PKI for mutual authentication –
    a. Can we see some federal use cases for the PKI, if they work for the federal infrastructure, IAW 800-32, chances are they are working and/or will work in the industry?
11. Can we get a more specific requirement?
12. This does not document specifically state what the authentication requirement or trusted fusion requirements or "guidelines "are for ORA – Entity out of Band Transaction
13. It would be nice if there were an updated technical guidance, specifically to address CSR from.
14. Although the current document includes details on CSS data structures, I would like to see interoperability and integration with latest and greatest automated technologies for key generation for new and re issue of keys, to include CSR in band and out of band
    a. Client to CA
    b. CA-CA
    c. RA-CA
    d. ORA-CA
15. There are ongoing key management issues, to include certificate management, Solutions Like Venafi say the solve the problem – are there Federal approved solutions for certificate life cycle management, to include key management that is FIPS 141-3 compliant that is in play for the federal infrastructure. I understand NIST does not promote technology, but we can't continue to do CSR from a manual, it is not secure or practical
16. Overall, this document outdated, and references are also outdate to a large degree, and also references deprecated protocols such as DES. I also I would like to review the CONOPS; however, it is not available on CSRC, many of the references are also outdated and have since be revised and updated.