Public Comments on NIST SP 800-32, *Introduction to Public Key Technology and the Federal PKI Infrastructure*

Comment period: May 10 – June 11, 2021

On May 2021, NIST's Crypto Publication Review Board initiated a review of NIST Special Publication (SP) 800-32, *Introduction to Public Key Technology and the Federal PKI Infrastructure*. This document includes the public comments received during the comment period from May 10 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 19, 2021

Summary

The PKI infrastructure requirements has evolved significantly over the last 10 years. Although the underlying fabric is cryptography, and our current symmetric, asymmetric, and hashing algorithms are strong enough *today* and meet current government standards, such as FIPS 141-3 and FIPS 197, these cryptographic components and standards should dovetail with a through descriptive and in some cases "prescriptive" where applicable for *secure engineer* by design approach to both meet standards and thwart off cyber-attacks. My opinion is, when the PKI system is attacked, it will be because of poor implementation or design, not the cryptography being cracked, making this document critical for our leadership and engineers, and security architects.

While I understand NIST generally does not endorse any technology, we must all work together to ensure all technologies that are "connected and/or work together to form a "system" are secure and meet requirements beyond interoperable protocols. This approach traditional worked in a closed environment; however, the PKI is a system of system, to ensure what would otherwise be two untrusted entities with a TTP doing both internal and external operations and we need an OV and SV for both with all components, to include optional components.

It is critical this document make a recommendation from a standard and base guideline perspective on each PKI component, and the associated risk. Especially as vendors fill the maket with solutions.

This document lacks adequate information on the implementation of a KMS and the process the CRS. Although these CRS is mentioned in 800-15 it is more descriptive in the data structure. These KMS and certificate life cycle management are tow critical areas that need to be mention in this document. The failure in these areas will cripple any PKI infrastructure. We need to ensure this document highlights a KMS requirement compliant with FIPS 140-3

1. As the user community and/or organizational entities across geography boundaries continues to grow, this makes symmetric cryptographic algorithms *inadequate, an "not practical"* for authentication and key distribution for large environments and/or smaller environments designed for "scalability. If this method is preferred, then the current SP 800-32 should prescribe approved **"out of band" *methods*** for key distribution for symmetric where risk is mitigated and should not make any assumptions.
    a. P. 12, section -2.3.4 is not an accurate statement on symmetric algorithms for key distribution, to the contrary, this is satisfied with asymmetric algorithms
    b. P. 12 could be clarified in the security infrastructures chart to ensure that readers understand that the TTP is a hybrid approach that uses both symmetric and asymmetric algorithms, where the asymmetric algorithm is used to transport the symmetric key
        i. A diagram flow with security services for key exchange to support 2.4 discussions with a TTP could clarify.
2. Current documents focus heavily on end users for a PKI, in today's environment the PKI, includes, but not limited to NPE, hardware, software, IOT, etc., and we should account for a different types of authentication certificates, to include internal and external that will have to be authenticated by a CA.
3. The PKI components are basic in this document and should include above and beyond the basic functional elements, to include a technical description, role, requirement, use case, physical and virtual place of each for both the traditional and federal infrastructures and the associated risk with not using each component.
    a. Can we see more description guidance on optional components, such as the attribute authority?
4. I recommend the document try to give more descriptive guidance on virtualize environments, the diagrams for a PKI are very high level and based on a physical environment and make many assumptions.
    a. We need more details on these areas for a virtualized in environment for the separation and security services of all PKI components.
        i. Is there risk on same device?

        ii. Is there a standard and/or requirement

    b. It would also be helpful if we can get both an SV and OV diagram so we can see exactly what is taking place within the typology, for example, on page 21-

        i. It would be help helpful to apply BBP, guidelines, regulations, for the federal infrastructure for security services using an SV overlay to show more detail, although the current document explains briefly what is going on, our environments have matured much more and we can add more detail, services, components, etc.

5. Can we more use cases on attribute certificates and how we should use them.
6. There are manycommon fields required with the x.509 and some are optional, and it would be good if the next document can provide use case on how the optional fields can be used to **mitigate risk**
7. Extensions are included in version 3; can we get some federal use cases that mitigate risk and map to 800-15.
8. Can we get more “prescriptive” guidance on **certificate issuer,** extension, perhaps a use case, interoperability as it will map to 800-15.
    a. This document makes no mention of new and improved protocols that will fill the gap, or “pain points” with the CRL, such as “certificate pinning?

        i. Can this extension be used for protocols like this?

9. Under sections for suspending and revoking certificates, can we add the reasons codes or reference 800-15?
10. For the federal PKI page 33, section 5.1 can we please update and reference ALL the standards and requirements directly for all security services and PKI components. I am of the mindset this is critical and necessary to mitigate and thwart cyber security attacks, and also ensure PKI security by design and interoperability.
    a. Can we get a more descriptive OV and SV for the federal PKI to include all functional and optional components?

2. Comments from Salko Korac (BSH Hausgeräte GmbH), May 19, 2021

Subject	**Comments on NIST SP 800-32**				**Salko Korac (salko.korac@bshg.com)**
Comment category	**Chapter**	**Page**	**Original Text**	**Proposed Change**	**Explanation**
Not state-of-the-art	2.3.2 Secure Hash	10	The secure hash function takes a stream of data and reduces it to a fixed size through a one-way mathematical function.	The secure hash function takes a stream of data and reduces it to a defined size through a one-way mathematical function.	State-of-the-art hash functions support outputs of arbitrary length (i.e. up to 1 GB hash output). Examples: Blake3, KangarooTwelve, SHAKE.
Not state-of-the-art	2.3.2 Secure Hash	10	The current Federal standard for a secure hash algorithm is SHA-1, which is specified in FIPS 180-1 [NIST 95].	The current Federal standard for a secure hash algorithm is SHA-3, which is specified in FIPS 202 [NIST 15].	SHA-1 was obsolete since 2011 by NIST.
Not state-of-the-art	2.3.2 Secure Hash	10	The RFC 2104 HMAC can be used in combination with any iterated cryptographic hash, such as MD5 and SHA-1.	The RFC 2104 HMAC can be used in combination with any iterated cryptographic hash, such as SHA-2 and SHA-3.	MD5 and SHA-1 are obsolete.
New technology	2.3.2 Secure Hash	10	None	Some hash algorithms like SHAKE support key derivation functions (KDF) and arbitrary output lengths by a extendable output function (XOF).	XOF and KDF functions were established after last publications and 2001.

Not state-of-the-art	2.3.3 Asymmetric (public key) Cryptography	11	Some asymmetric algorithms (e.g., RSA [RSA 78]) can be used to encrypt and decrypt data.	Some asymmetric algorithms (e.g., ECC [ECC xy]) can be used to encrypt and decrypt data.	RSA was withdrawn since TLS 1.3. Better option is to mention Elliptic Curve Cryptography (ECC) as example. In general the document refers several times to RSA, which is still used in practice but not state-of-the-art anymore, since it was removed in TLS. ECC is a better example and should be referred throughout the document.
Wording	2.1 Security Services	7	Services	Goals	Refine wording to "Security goals".
Established standard	-	-		3.1.6 hardware security module (HSM) Hardware security modules are physical devices that store and safeguard secrets in a public key infrastructure. A HSM can perform encryption and decryption functions for digital signatures, authentication attempts or other data without revealing the private key. HSMs rely on a secure crypto processor and several physical and logical protective measures against tampering and unauthorized access. Note that physical intactness of the HSM is required at any time.	Use of HSMs is established industry standard. It is of paramount importance for PKI.

				Security requirements for HSMs are defined in FIPS 140-3.	
New risk	-	-		4.4.6 physical security Unauthorized access, damage or tampering of PKI components can cause severe consequences to business operation and in worst-case compromise the whole PKI chain. The PKI components need adequate physical protection considering their security class. Depending on the assessed risk, protective measures may include amongst others a safe storage, standardized walls, door alarm, 4-eyes principle and use of temper-evident bags. A complete documentation of storage, access and use of the PKI components is necessary.	We invest a lot of effort to protect our assets physically. This measures are the main backbone to protect the company against severe business interruptions and financial loss.