Comments on NIST Special Publication 800-57, Recommendation for Key Management - Part 2: Best Practices for Key Management Organization: General

From: "Kazin, Joel" <Joel.Kazin@atosorigin.com>
Date: Mon, 2 May 2005 13:27:44 -0500

The draft document beginning in section 3.2.1.1 makes several references to the RFC 2527 framework. While I agree with the general approach in the draft, RFC 2527 is obsolete having been superceded by RFC 3647 in November of 2003. While the content of the framework of RFC 2527 was not greatly changed by RFC 3647, the organization was. There is a useful set of cross-references between the two frameworks at the back of RFC 3647.

Joel S. Kazin CPA, CISA, CISSP, CISM
Senior Consultant
Atos Origin
40 Old Sleepy Hollow Road
Pleasantville, New York 10570-3802
USA
Phone +1 914-769-8780
Mobile +1 914-564-1484
email joel.kazin@atosorigin.com
www.atosorigin.com

From: Robert Zuccherato <robert.zuccherato@entrust.com>
Date: Fri, 20 May 2005 10:02:37 –0400

Entrust Comments on NIST SP 800-57 Recommendation for Key Management – Part 2: Best Practices for Key Management Organizations

This document does a good job of generalizing the X.509 concepts of Certificate Policies and Certification Practice Statements to all infrastructures that manage cryptographic keys. Entrust's comments are as follows:

1. The text at the beginning of Appendix C states "In purely PKI environments, a PKI Certificate Policy (CP) may serve as the Key Management Policy (KMP), and a PKI Certification Practices Statement (CPS) may serve as a Key Management Practices Statement (KMPS). … The RFC 2527 format **should** be used in purely PKI environments." Similar text also appears elsewhere in the document.
These statements raise the question of what is a "purely PKI environment". Typically applications that make use of an X.509 PKI utilize ephemeral symmetric keys (e.g. for bulk encryption or authentication of session data) or even ephemeral asymmetric keys (e.g. for key agreement). Would environments that use an X.509 PKI but also make use of such applications be considered a "purely PKI environment"?

If the answer is "Yes", then it is not clear that the current definition of a CP and CPS suffices. Currently these documents deal with the management of just the certified public key pair and not the ephemeral symmetric and asymmetric keys. Thus, guidance should be provided about how to include this information in a CP and CPS.

If the answer is "No", then this document would suggest that an additional KMP and KMPS would be required for these keys. Depending upon the application, this may make sense, but for the vast majority of applications this would be somewhat excessive, when the same ends could be achieved by slightly expanding the CP and CPS.

This situation seems to be acknowledged in the second paragraph of Section 3.2.2.11 and the second paragraph of Section D.2.2.6, but otherwise the document appears to be silent on how to handle these keys.
At least additional discussion is needed regarding what is a "purely PKI environment".

Additionally, it should be stressed that RFC 2527 applies to an X.509 PKI as opposed to other types of public key infrastructure that exist (e.g., PGP, SPKI, etc.).

2. The definition of "Random Number Generator (RNG)" on page 18 is not quite right. A deterministic RNG produces a sequence that can, in fact, be described

more efficiently than simply listing the entire string of output. This can be done by providing a description of the algorithm and the seed used. We recommend that the definition from ANSI X9.82 be used.

3. The first sentence of Section 5 doesn't appear to be worded correctly. Should "are key management products" be "use key management products"?

4. In Section A.2.2, Number 6 and also in Section A.3.2, Number 9 it is recommended that the private key associated with a key transport public key be destroyed after its one year validity period. Following this advice would leave the subject with no means to access previously encrypted data. Thus, the advice should be modified to suggest that the private key may be maintained to provide access to encrypted data.

5. Section D.2 refers to characteristics specified in Section B.1.2. It should probably be referring to Section D.1.2.

Robert Zuccherato
Chief Cryptographer
Phone: (613) 270-2598

Entrust
Securing Digital Identities
& Information
http://www.entrust.com

From: "RDavis" <rdavis@femto-second.com>
Date: Mon, 9 May 2005 09:11:14 -0400

Comments:

Recommendation for Key Management Part 2: Best Practices for Key Management Organizations

Overall, there are no major comments on this document. The following minor editorial changes are suggested:

Page 19 Include CKL and LRA to the list of acronyms

Page 22, forth bullet under 2.2 Maintenance and distribution of nodal key compromise lists (CKLs) and/or certificate revocation lists (CRLs), and Use Compromised Key List in front of CKL.

Page 34 (h) procedures.[This sentence doesnt read right.] Suggest removing the comment and structuring the paragraph to address configuration management.

Page 35, second paragraph on the page that KMI. . The KMPS may be Delete the second period.

Dr. Russell J. Davis
Femtosecond Inc.
9747 Water Oak Drive
Fairfax, VA 22031-1029
(703) 282-1837
RDavis@femto-second.com
www.femto-second.com