X-Sieve: CMU Sieve 2.2
Subject:
Date: Thu, 23 Dec 2004 11:33:02 -0800
X-MS-Has-Attach: yes
X-MS-TNEF-Correlator:
Thread-Index: AcTpJjfBscjlL47xTuuJlnBVN7Bx/g==
From: "Guido Appenzeller" <appenz@voltage.com>
To: <draftfips201@nist.gov>
Cc: "Luther Martin" <martin@voltage.com>,
"Terence Spies" <terence@voltage.com>, "Mark Schertler" <mark@voltage.com>
X-MailScanner:
X-MailScanner-From: appenz@voltage.com

Dear Sirs,

please find attached our comments on FIPS 201 from Voltage Security. For questions or clarifications please feel free to contact either Luther Martin <luther@voltage.com> or myself.

Regards,

Guido Appenzeller

Co-founder and CTO
Voltage Security
1070 Arastradero Road, Suite 100
Palo Alto, CA 94304
650-543-1280 ext 120
650-543-1279 fax
www.voltage.com


Voltage Comments.xls

Cmt #	Organization	Point of Contact	Comment Type (G-General, E-Editorial, T-Technical)	Section, Annex, etc., and Page No.	Comment (Include rationale for comment)	Proposed Change
1	Voltage Security	Guido Appenzeller, (650) 543-1280 x120, guido@voltage.com	E	FIPS 210, section 4.3, p. 27	In the draft of FIPS 201, on p. 27, section 4.3, Cryptographic Specifications, we have that "All cryptographic operations using the PIV keys shall be performed on-card; the PIV card need not implement any additional cryptographic functionality (e.g. hashing, signature verification, etc.) on-card. When used to protect access to sensitive data and systems, this functionality may be augmented (e.g. with hash algorithms and signature verification) by a validated software cryptographic module." Just to make sure that there is no dispute over exactly what additional functionality is covered by the "etc." and "e.g.," add a few words to clarify this.	"All cryptographic operations using the PIV keys shall be performed on-card; the PIV card need not implement any additional cryptographic functionality (e.g. hashing, signature verification, ***key management***, etc.) on-card. When used to protect access to sensitive data and systems, this functionality may be augmented (e.g. with hash algorithms and signature verification ***or other types of off-card processing***) by a validated software cryptographic module."
2	Voltage Security	Guido Appenzeller, (650) 543-1280 x120, guido@voltage.com	T	FIPS 201, section 4.3, p. 29	In the draft of FIPS 201, on p. 29, in section 4.3, we have that "The PIV card shall import and store a corresponding X.509 certificate to support validation of the key management key. Section 5.2.3 of this document specifies the certificate format and the key management infrastructure for key management keys." There are public key technologies that do not use public key certificates, like identity-based encryption and related technologies, and use of these technologies is apparently disallowed by this wording. The use of certificate-less public key technologies is potentially important in future PKI architectures, the possibility of using this technology should not be inadvertently disallowed by such wording.	"The PIV card shall import and store a corresponding X.509 certificate to support validation of the key management key. Section 5.2.3 of this document specifies the certificate format and the key management infrastructure for key management keys. ***This requirement does not apply to public key technologies that do not use public key certificates.***"

D = Document,1 = FIPS201, 2 = SP800-73
T=Type of Comment, E = editorial, T = technical

Cmt #	Organization	Point of Contact	Comment Type (G-General, E-Editorial, T-Technical)	Section, Annex, etc., and Page No.	Comment (Include rationale for comment)	Proposed Change
4	Voltage Security	Guido Appenzeller, (650) 543-1280 x120, guido@voltage.com	T	FIPS 201, section 5.1.2, p. 40	In the draft of FIPS 201, on p. 40, in section 5.1.2, we have that "Since the lifetime of authentication certificates is typically long, typically several years, a certificate revocation mechanism is necessary." There are many advantages to using short-lived keys and corresponding short-lived certificates, and if the validity period of a short-lived certificate is no longer than the update period for a CRL, then no revocation mechanism is necessary to attain the same level of security that longer-lived certificates provide. The possibility of federal agencies using short-lived keys is currently excluded from consideration as a possible technology because of the assumption that the lifetime of all certificates will be relatively long. Allowance for the use of short-lived keys should be included in this document to allow federal agencies to take advantage of the potential efficiencies that the use of the technology allows if it meets their security needs.	Add the text "Short-lived keys also allow the possibility of providing up-to-date certificate validation information without the overhead of creating and updating a CRL or operating an OCSP responder, and as long as the validity period of a short-lived key is no greater than the CRL update interval, short-lived keys can be used without compromising the timeliness of the validity information. In this case, the requirements of maintaining an LDAP directory to hold the CRLs for the short-lived certificates or operating an OCSP responder for the short-lived certificates are not applicable."
5	Voltage Security	Guido Appenzeller, (650) 543-1280 x120, guido@voltage.com	T	FIPS 201, section 5.2.3.3, p. 45	In the draft of FIPS 201, on p. 45, in section 5.2.3.3, we have that "CAs that issue certificates corresponding to PIV private keys shall issue CRLs every 18 hours, at a minimum." This language is somewhat ambiguous and the precise meaning of this statement should be clarified. Is the 18-hour period the maximum interval between CRL updates or is it the minimum interval between CRL updates? In any event, the use of short-lived keys should be allowed, and the issuance of only short-lived certificates should eliminate the requirements for issuing CRLs and operating an OCSP responder.	Change the quoted text to be "CAs that issue certificates corresponding to PIV private keys shall issue CRLs ***no less frequently than once every 18 hours.***" Further, to allow for the possibility that short-lived keys will be used, add the text "A CA that issues only short-lived certificates that have a validity period of no more than 18 hours shall be exempt from issuing CRLs and operating an OCSP responder. CAs that issue both long-lived and short-lived certificates are not required to manage the revocation of certificates with a validity period of no more than the CRL update interval."

D = Document,1 = FIPS201, 2 = SP800-73
T=Type of Comment, E = editorial, T = technical