Certificate Policy Comparison

Bill Burr
NIST
william.burr@nist.gov
9 Feb. 2000

Crypto Module Requirements

US FBCA Rud.	BCA: FIPS 140 L3, Agency CA: FIPS 140 L1 (6.1.1)
US FBCA Basic	BCA: FIPS 140 L3, Agency CA: FIPS 140 L2 (6.1.1)
US FBCA Med.	BCA:FIPS 140 L3, Agency CA: FIPS 140 L2 (6.1.1)
US FBCA High	BCA: FIPS 140 L3, Agency CA: FIPS 140 L3 (6.1.1)
GOC Rud. Sig.	No Stipulation
GOC Basic Sig.	CA FIPS 140 L2, RA & EE FIPS 140 L1 (6.8)
GOC Med. Sig.	CA sig. & key storage FIPS 140 L2 *H*, otherwise FIPS 140 L2; RA sig. & key storage FIPS 140 L1 *H*, otherwise FIPS 140 L1; End Entities FIPS 140- L1 (6.8)
GOC High Sig.	CA sig. & key storage FIPS 140 L3 *H*, otherwise FIPS 140 L2; RA sig. & key storage FIPS 140 L2 *H*, otherwise FIPS 140 L1; End Entities FIPS 140- L2 (6.8)
DoD Class 2	Subscriber & RA FIPS 140-1 L1, CA 140-1 L2 (*H or S*) (6.2.1)
DoD Class 3	Subscriber & RA FIPS 140-1 L1, CA 140-1 L2 (*H*) (6.2.1)
DoD Class 4	Subscriber FIPS 140-1 L2, RA & CA 140-1 L2 (*H*) (6.2.1)
GSA Aces	No Stipulation

Cert. Validity & Key Usage Periods

US FBCA Rud.	BCA & Agency CA 10 years (6.3.2); rekey between .9 and 1.0 of validity period (3.2)
US FBCA Basic	same as Rudimentary
US FBCA Med.	same as Rudimentary
US FBCA High	same as Rudimentary
GOC Rud. Sig.	1 year if no CRL, 6 years with CRL
GOC Basic Sig.	All 1024 bit keys no more than 6 years (6.3.2) Suggested: CA: pub. 6 years, priv. 2years EE: pub. enc. key & cert. 4 years, priv. decrypt. key no expiry
GOC Med. Sig.	All 1024 bit keys no more than 2 years, all 2048 bit keys no more than 20 years (6.3.2) Suggested: <u>1024</u> CA pub 2 y., priv. 1 y. EE pub. 1 y., priv. 6 mo. <u>2048</u> CA pub 20 y., priv. 8 y. EE pub. 12 .y, priv. 2 y.

Cert. Validity & Key Usage Periods

GOC High Sig.	All 2048 bit keys no more than 20 years (6.3.2) Suggested: CA pub. 20 y., CA priv. 8y. EE pub. 12 y., priv. 2 y.
DoD Class 2	Sig. rekey after 5 y., Conf. rekey after 5 y. (3.2.1)
DoD Class 3	Sig. rekey after 3 y., Conf. rekey after 3 y. (3.2.1)
DoD Class 4	Sig. rekey after 3 y., Conf. rekey after 3 y. (3.2.1)
GSA Aces	specified in applicable certificate profile (6.3.2), renewal within 90 days of expiration (3.2)

Algorithms & Key Sizes

US FBCA Rud.	min. 1024 DSA or RSA (PKCS#1), with SHA-1 (6.1.5, 7.1.3)
US FBCA Basic	min. 1024 DSA or RSA (PKCS#1), with SHA-1 (6.1.5, 7.1.3)
US FBCA Med.	min. 1024 DSA or RSA (PKCS#1), with SHA-1 (6.1.5, 7.1.3)
US FBCA High	min. 1024 DSA or RSA (PKCS#1), with SHA-1 (6.1.5, 7.1.3)
GOC Rud. Sig.	CA: 1024 RSA (PKCS #1) & SHA-1, EE: 512 & 1024 RSA & DSA, MD5, SHA-1 (7.1.3)
GOC Basic Sig.	CA: 1024 RSA (PKCS #1) & SHA-1, EE: 512, 1024 & 2048 RSA, DSA, MD5, SHA-1 (7.1.3)
GOC Med. Sig.	CA: 1024 (RSA or DSA) or 2048 RSA (PKCS #1) with SHA-1, EE: 1024/2048 RSA (PKCS #1), DSA, MD5, SHA-1 (7.1.3)
GOC High Sig.	CA: 2048 bit RSA (PKCS #1) with SHA-1, EE: 1024 & 2048 RSA (PKCS #1), DSA, MD5, SHA-1 (7.1.3)

Algorithms & Key Sizes

DoD Class 1	Subscriber DSA x=160, p=1024, RSA 1024 (PKCS #1), KEA 1024 (6.1.3, 7.1.3)
DoD Class 2	Subscriber DSA x=160, p=1024, RSA 1024 (PKCS #1), KEA 1024 (6.1.3, 7.1.3)
DoD Class 3	Subscriber DSA x=160, p=1024, RSA 1024 (PKCS #1), KEA 1024 (6.1.3, 7.1.3)
DoD Class 4	Subscriber DSA x=160, p=1024, RSA 1024 (PKCS #1), KEA 1024 (6.1.3, 7.1.3)
GSA Aces	Specified in contract or profile

Conclusion

- Crypto Module requirements not too different
  - DoD only goes up to Level 2 for CAs
- Differences in Cert Validity & Usage Periods
- Canadians more permissive about algorithms
  - 2048 bit for high assurance
- Specified in different places