
Department: UW Medicine Information Technology Services
Policy Number: SEC-05.03.01 – Encryption Guideline
Effective Date: December 18th, 2007
Review Date: December 4th, 2007

Purpose

This guideline lists cryptographic algorithms that are currently considered secure and that can be used to satisfy requirements in *SEC-05.03 Encryption Standard*.

Definitions

See UW Medicine Information Security policy: *SEC-REF UW Medicine Information Security Program Glossary of Terms*.

Guideline

Any of the recommended algorithms will provide adequate security for their intended purpose. System Owners and end users should feel free to select whichever recommended algorithms are available in the products they are using.

I. Recommended Encryption Algorithms

- A. Advanced Encryption Standard (AES) (FIPS PUB 197)
- B. Blowfish (http://en.wikipedia.org/wiki/Blowfish_%28cipher%29)
- C. Serpent – AES competition finalist (http://en.wikipedia.org/wiki/Serpent_%28cipher%29)
- D. Triple Data Encryption Standard (3DES) (FIPS PUB 46-3)
- E. Twofish – AES competition finalist based on Blowfish (<http://en.wikipedia.org/wiki/Twofish>)

II. Recommended Digital Signature Algorithms

- A. Digital Signature Algorithm (DSA) (FIPS 186-2 Digital Signature Standard)
- B. RSA (FIPS 186-2 Digital Signature Standard)

III. Recommended Digital Hash Algorithms

- A. Secure Hash Algorithm (SHA-1) (FIPS 180-2 Secure Hash Standard)
- B. Secure Hash Algorithm (SHA-256, SHA-384, SHA-512). Newer, more robust hash algorithms (<http://en.wikipedia.org/wiki/Sha-1>).

References:

- I.** International Organization for Standardization /International Electrotechnical Commission (ISO/IEC) 17799 Section 8, Communications And Operations Management
- II.** Federal Information Processing Standards (FIPS) Publications - Advanced Encryption Standard (AES) (FIPS PUB 197)
- III.** Federal Information Processing Standards (FIPS) Publications - Triple - Data Encryption Standard (DES) (FIPS PUB 46-3)
- IV.** Federal Information Processing Standards (FIPS) Publications - Digital Signature Algorithm (DSA) (FIPS 186-2 Digital Signature Standard)
- V.** Federal Information Processing Standards (FIPS) Publications - RSA (FIPS 186-2 Digital Signature Standard)
- VI.** Federal Information Processing Standards (FIPS) Publications - Secure Hash Algorithms (SHA-1) (FIPS 180-2 Secure Hash Standard)

UW Medicine IT Services: _____ Date: _____

Ira Kalet, Director of Security
