

Tillämpning av kryptografiska algoritmer

Detta dokument beskriver vilka kryptografiska nivåer som används och vilka algoritmer som stöds av Apotekens Service.

1 Apotekens Service tillämpning av kryptografiska nivåer

Detta dokument beskriver vilka kryptografiska nivåer som används och vilka algoritmer som stöds av Apotekens Service. Kryptografiska nivåer används för att dela in olika former av kryptografi efter styrka och svårighet att attackera.

Det är informationsklassningen som är styrande för vilken kryptografisk nivå som är tillämplig i olika situationer och avgör exempelvis:

- vilken nivå av kryptografi (nyckellängd / val av krypteringsmetod) som skall tillämpas på en given informationsmängd
- den kryptografiska period som tillåts innan nyckelutbyte skall ske

Nedanstående tabell listar vilka kryptografiska algoritmer, hashalgoritmer samt kryptografisk period som Apotekens Service tillämpar.

Nivå av kryptering	Symmetriska algoritmer	Assymetrisk algoritm	Hashfunktion	Signeringsalgoritm	Kryptografisk period för nycklar Max:
1	3TDEA* RC4**	RSA 2048 bitars nycklar	SHA-256	DSA RSA (PKCS#1, PKCS#7) ECDSA	1 år
2	AES-128 (Rijndael)	RSA 3072 bitars nycklar	SHA-384	DSA RSA (PKCS#1, PKCS#7) ECDSA	5 år
3	AES-256 (Rijndael)	RSA 4096 bitars nycklar	SHA-512	DSA RSA (PKCS#1, PKCS#7) ECDSA	10 år

* - Får endast nyttjas med tre unika 56 bits DES-nycklar, samma DES-nyckel får inte återanvändas för någon av de tre nyckelcontainrarna

** - får endast nyttjas med minst 128 bitars nyckellängd

Det är av yttersta vikt att själva nyckelhanteringen beaktas vid ett givet kryptografiskt scenario eftersom åtkomst till krypteringsnycklar styr åtkomsten till krypterat data.

Nyckelhantering utvärderas i relation till riskbedömning samt den tillit som kan appliceras på nyckelutfärdaren i fråga. Nedanstående bild beskriver de tre huvudsakliga bedömningsområdena för att värdera tillit till en nyckelutfärdare:



Apotekens Service utvärderar ovanstående aspekter som en helhet när man bedömer tilliten till utfärdare av kryptografiska nycklar. Gällande det tekniska skyddet av privata nycklar skall detta redovisas i enlighet med FIPS 140-2 från NIST.

Revisionshistorik

Utgåva	Datum	Kommentar
1.0	2011-12-12	