Kryptografiset vahvuusvaatimukset luottamuksellisuuden suojaamiseen - kansalliset turvallisuusluokat

1 Johdanto

Tässä dokumentissa kuvataan ne kryptografiset vähimmäisvaatimukset, joita Liikenne- ja viestintävirasto Traficomissa toimiva salaustuotteiden hyväksyntäviranomainen (Crypto Approval Authority, CAA) käyttää arvioidessaan salaimen soveltuvuutta turvallisuusluokitellun tiedon suojaamiseen. Dokumentissa käsitellään vain niitä kryptografisia menetelmiä, jotka Traficomin johtama Kansallinen Kryptotyöryhmä on hyväksynyt kyseiseen käyttöön. Dokumentti on tarkoitettu kryptologian asiantuntijoille, joten alan termistöä ei määritellä.

Lisätietoa salauksen perusteista ja käytäntöön soveltamisesta saa esimerkiksi Tiedonhallintalautakunnan suosituksesta "Suositus turvallisuusluokiteltujen asiakirjojen käsittelystä" (http://urn.fi/URN:ISBN:978-952-367-500-1), jonka liitteenä tätä dokumenttia myös käytetään, sekä salaustuotteiden hyväksyntäviranomaiselta: caa[a]traficom.fi.

Luvussa 2 kerrataan vaatimusten soveltamiseen liittyviä asioita. Luvussa 3 selitetään, mitä kryptografisella vahvuudella tarkoitetaan tässä dokumentissa. Luvussa 4 esitellään Traficomin työryhmän laatimat vähimmäisvahvuustaulukot. Luvussa 5 kerrataan muita salausmenetelmien hyväksyttyyn käyttöön liittyviä asioita.

2 Vaatimusten soveltaminen käytäntöön

Salaustuotteiden hyväksyntäviranomainen tulkitsee ja soveltaa tapauskohtaisesti luvussa 4 esitettyjä taulukoita. Hyväksyntäviranomainen voi poiketa vähimmäisvaatimuksista vain rajatusti tiettyjen erityisehtojen täyttyessä.

Vaatimuksia sovellettaessa huomioidaan järjestelmän käsittelemän tiedon suojaustarve ja käyttöympäristö. Lisäksi on huomioitava, että taulukko on määritelty käyttöympäristöihin, joissa uhkatason arvioidaan olevan *korkea*.

Korkean uhkatason ympäristöksi voidaan käsittää esimerkiksi

- suojaamattomat avoimet tietoverkot, joihin pääsyä ei valvota, kuten yhteydet internetin ylitse
- alemmalle suojaustasolle hyväksytyt järjestelmät tai tietojenkäsittely-ympäristöt.
- viestinnän ilmarajapinnan yli sekä kontrolloitujen alueiden ulkopuolelle vietävät ja muut fyysisten suojauksien ulkopuolella sijaitsevat tietokoneet
- tallennuslaitteet yms. tietovarannot silloin, kun ne ovat fyysisten suojausten ulkopuolella.

3 Kryptografiset vahvuudet

Kryptografisen menetelmän vahvuudella pyritään kuvaamaan kyseisen menetelmän kykyä vastustaa kryptoanalyysiä. Kryptografista vahvuutta rajoittaa tehokkaimman tunnetun hyökkäysmenetelmän laskennallinen vaativuus. Kryptografista vahvuutta voidaan käyttää vertailulukuna suhteessa muihin salausmenetelmiin ja ulkopuolisen hyökkääjän arvioituihin laskentaresursseihin. Kahta menetelmää voidaan pitää yhtä vahvoina, jos salauksen rikkomiseen tarvittava työ- ja resurssimäärä on molemmilla yhtä suuri.

Lisätietoa kryptografisista vahvuuksista ja salausmenetelmien vertailusta löytyy viitteinä käytetyistä ECryptin ja NIST:n julkaisemista dokumenteista.

4 Kryptografiset vahvuusvaatimukset käyttötarkoituksen mukaan

Tässä luvussa kuvattavat vaatimukset on määritetty Liikenne- ja Viestintävirasto Traficomin johtamassa Kansallisessa Kryptotyöryhmässä. Kryptografinen vahvuus määritetään kullekin salausalgoritmille erikseen. Työryhmä arvioi algoritmin kestävyyden kryptoanalyysiä vastaan huomioiden muun muassa sen käyttötarkoituksen sekä tehokkaimpien hyökkäysmenetelmien laskennalliset vaativuudet.

Algoritmit on jaettu ryhmiin vahvuutensa perusteella. Ensimmäisellä rivillä mainittu kryptografinen vahvuus bitteinä tarkoittaa suojaustasolle määriteltyä ohjeellista kryptografista vahvuutta. Seuraavilla riveillä on lueteltu, minkä algoritmien ja avainpituuksien tai vastaavan parametrin arvon katsotaan riittävän tähän ryhmään. Hyökkäysmenetelmien kehittymisen vuoksi voi käydä niin, että jotkin algoritmit ja avaimenpituudet eivät enää täytä vahvuusvaatimusta. Siitä syystä taulukkoa päivitetään tarpeen mukaan. Taulukossa on huomioitu joustovara, ja siten pienet heikennykset (1-3 bittiä) algoritmin vahvuudessa eivät aiheuta muutosta taulukkoon.

Viestin salaus symmetrisellä menetelmällä (lohko- ja ketjusalaus)

Kansallinen turvallisuusluokka/ kryptovahvuus	**TL IV**	**TL III**	**TL II**
kryptografinen vahvuus bitteinä	128	192	256
algoritmi: AES	AES-128	AES-192	AES-256
algoritmi: Serpent [avaimenpituus]	Serpent[128]	Serpent[192]	Serpent[256]
algoritmi: ChaCha20	ChaCha20		

Allekirjoitus epäsymmetrisellä menetelmällä (esim. RSA) - "vaativat allekirjoitukset"

Viestin allekirjoitus epäsymmetrisellä menetelmällä, esimerkiksi varmenteiden allekirjoitus. Luku hakasulkeiden sisällä viittaa alla olevan äärellisen kunnan kokoon.

Kansallinen turvallisuusluokka/kryptovahvuus	**TL IV**	**TL III**	**TL II**
kryptografinen vahvuus bitteinä	128	192	256
algoritmi: RSA	RSA[3072]	RSA[7680]	RSA[15360]
algoritmi: ECDSA	ECDSA[256]	ECDSA[384]	ECDSA[512]
algoritmi: EdDSA	EdDSA[256]	EdDSA[384]	EdDSA[512]
algoritmi: ML-DSA	ML-DSA-44	ML-DSA-65	ML-DSA-87
algoritmi: SLH-DSA	SLH-DSA-SHA2-128s, SLH-DSA-SHAKE-128s, SLH-DSA-SHA2-128f,	SLH-DSA-SHA2-192s, SLH-DSA-SHAKE-192s, SLH-DSA-SHA2-192f,	SLH-DSA-SHA2-256s, SLH-DSA-SHAKE-256s, SLH-DSA-SHA2-256f,

	SLH-DSA-SHAKE-128f	SLH-DSA-SHAKE-192f	SLH-DSA-SHAKE-256f

ML-DSA ja SLH-DSA ovat NIST:in standardoimia kvanttiturvallisia allekirjoitusalgoritmeja, kts. [FIPS 204] ja [FIPS 205]. Niitä tulee käyttää lähtökohtaisesti hybridimoodissa, yhdistettynä johonkin tässä ohjeessa kyseiselle turvallisuusluokalle hyväksyttyyn klassiseen (ei-kvanttiturvalliseen) allekirjoitusalgoritmiin. Hybridiyhdistelmät määritellään tyypillisesti eri tietoturvaprotokollissa. Hyväksyntäviranomainen suosittelee siirtymistä kvanttiturvallisten algoritmien käyttöön mahdollisuuksien mukaan mahdollisimman pian.

Tiivistefunktio, käyttötarkoitus digitaaliset allekirjoitukset ja "hash-only" -sovellukset

Tiivistefunktiolla on törmäyksettömyysvaatimus.

Kansallinen turvallisuusluokka/kryptovahvuus	**TL IV**	**TL III**	**TL II**
kryptografinen vahvuus törmäys-hyökkäystä vastaan bitteinä	128	192	256
algoritmi: SHA-2	SHA-256	SHA-384	SHA-512
algoritmi: SHA-3	SHA-3-256	SHA3-384	SHA-3-512
algoritmi: SHAKE	SHAKE-128/256	SHAKE-256/384	SHAKE-256/512

Tiivistefunktio, käyttötarkoitus HMAC, avainten ja satunnaislukujen generointi

Tiivistefunktio, kun suojaustarve on vain alkukuvaan.

Kansallinen turvallisuusluokka/kryptovahvuus	**TL IV**	**TL III**	**TL II**
kryptografinen vahvuus alkukuvahyökkäystä vastaan bitteinä	128	192	256
algoritmi: SHA-2	SHA-224	SHA-224	SHA-256
algoritmi (IPsec HMAC[1]): SHA-2	SHA-256	SHA-384	SHA-512
algoritmi: KMAC	KMAC-128/128	KMAC-256/192	KMAC-256/256
algoritmi: SHA-3	SHA-3-256	SHA-3-384	SHA-3-512
algoritmi: SHAKE	SHAKE-128/128	SHAKE-256/192	SHAKE-256/256

[1] IPsec-spesifikaation (RFC 4868) mukaan toteutetuissa IPsec-ratkaisuissa HMAC:n tiivistefunktioksi on valittava se versio SHA-2:sta, jonka tiivisteen pituus on kaksinkertainen suojaustason kryptografiseen vahvuusvaatimukseen nähden, koska spesifikaation mukaan HMAC:n tuloste puolitetaan lopussa.

4.1 Avaintenvaihto

Luku hakasulkeiden sisällä viittaa alla olevan äärellisen kunnan kokoon.

Kansallinen turvallisuusluokka/ kryptovahvuus	**TL IV**	**TL III**	**TL II**
kryptografinen vahvuus bitteinä	128	192	256
menetelmä: DH äärellisissä kunnissa	DH/MQV [3072] (esim. DH-ryhmä[2] 15)	DH/MQV [7680] (esim. DH-ryhmä 18)	DH/MQV [15360]
menetelmä: ECDH	ECDH/ECMQV [256] (esim. DH-ryhmä 19)	ECDH/ECMQV [384] (esim. DH-ryhmä 20)	ECDH/ECMQV [512] (esim. DH-ryhmä 21)
menetelmä: X25519	X25519		
menetelmä: X448		X448	
sessioavaimen jakelu hybridisalauksessa RSA:lla	RSA [3072]	RSA [7680]	RSA [15360]
menetelmä: ML-KEM	ML-KEM-512	ML-KEM-768	ML-KEM-1024

ML-KEM on NIST:in standardoima kvanttiturvallinen avaintenmuodostusmenetelmä, kts. [FIPS 203]. Sitä tulee käyttää lähtökohtaisesti hybridimoodissa, yhdistettynä johonkin klassiseen (ei-kvanttiturvalliseen) menetelmään, joka on tässä dokumentissa hyväksytty kyseiselle turvallisuusluokalle. Hybridiyhdistelmät määritellään tyypillisesti eri tietoturvaprotokollissa. Hyväksyntäviranomainen suosittelee siirtymistä kvanttiturvallisten menetelmien käyttöön mahdollisuuksien mukaan mahdollisimman pian.

5 Muuta huomioitavaa salauksen vahvuudesta

Tiedon luottamuksellisuuden turvaamisessa on tärkeää, että salaustuote arvioidaan kokonaisuutena. Kryptografisten primitiivien oikeellisen toteutuksen ja käyttötavan arvioiminen, tietoliikenne- ja tietoturvaprotokollien oikea valinta ja toteutus sekä muut tuotteen turvallisuuteen olennaisesti vaikuttavat seikat otetaan huomioon salaustuotteen arvioinnissa. Näitä asioita ei käsitellä tässä dokumentissa yksityiskohtaisemmin.

Tietoliikenne- ja tietoturvaprotokollat: On syytä varmistaa, että ajantasaiset versiot ovat käytössä. Viestintäviraston salaustuotteiden hyväksyntäviranomainen suosittelee, ja salaustuotearvioinneissa voi edellyttää, että yleisimmistä protokollista käytetään uusinta vakaata (stable) versiota.

Tällaisia protokollia ovat esimerkiksi TLS ja IPsec, joista jälkimmäiseen kuuluu avaintenhallintaprotokolla IKE. Vaikka TLS-protokollasta puhuttaessa käytetään joskus sitä edeltäneen SSL-protokollan nimeä, ei SSL-protokollan versioita 1.0, 2.0 ja 3.0 tule enää käyttää. TLS-yhteyksien muodostamiseen suositellaan TLS-protokollan versiota 1.2 tai 1.3.

[2] Ryhmien numeroilla tarkoitetaan IANA:n IKEv2-spesifikaation numeroita (http://www.iana.org/assignments/ikev2-parameters/ikev2-parameters.xhtml).

Myös IPsec-protokollakokonaisuudesta on syytä käyttää uusimpia saatavilla olevia versioita. Erityisesti IKE:stä on huomioitava, että useimmiten ainoastaan IKEv2 mahdollistaa edellä mainitut kryptografiset vahvuusvaatimukset.

Salasanatiivisteet: Tiivistefunktioiden suhteen on huomioitava, että taulukossa luetellut standardoidut kryptografiset tiivistefunktiot eivät ole sellaisenaan suositeltavia salasanojen tallentamiseen. Suositeltavia salasanatiivistealgoritmeja ovat esimerkiksi scrypt, bcrypt ja PBKDF2.

6 Viitteitä

ECRYPT-CSA Algorithms, Key Size and Protocols Report (2018), Revision 1.0. 28 February 2018. https://www.ecrypt.eu.org/csa/documents/D5.4-FinalAlgKeySizeProt.pdf

NIST Special Publication 800-131A Revision 2. Transitioning the Use of Cryptographic Algorithms and Key Lengths. March 2019. https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-131Ar2.pdf

[FIPS 203] National Institute of Standards and Technology (2024) Module-Lattice-Based Key-Encapsulation Mechanism Standard. (Department of Commerce, Washington, D.C.), Federal Information Processing Standards Publication (FIPS) NIST FIPS 203. https://doi.org/10.6028/NIST.FIPS.203

[FIPS 204] National Institute of Standards and Technology (2024) Module-Lattice-Based Digital Signature Standard. (Department of Commerce, Washington, D.C.), Federal Information Processing Standards Publication (FIPS) NIST FIPS 204. https://doi.org/10.6028/NIST.FIPS.204

[FIPS 205] National Institute of Standards and Technology (2024) Stateless Hash-Based Digital Signature Standard. (Department of Commerce, Washington, D.C.), Federal Information Processing Standards Publication (FIPS) NIST FIPS 205. https://doi.org/10.6028/NIST.FIPS.205