Liikenne- ja viestintävirasto Traficomin suorittamat salaustuotearvioinnit ja -hyväksynnät

Tilaajan näkökulma

Johdanto

EU:n neuvoston turvallisuussäännöstön[1] mukaan jäsenvaltioiden on nimettävä kansallinen salaustuotteiden hyväksyntäviranomainen (CAA, Crypto Approval Authority). Traficom toimii Suomen kansallisena salaustuotteiden hyväksyntäviranomaisena ja sen tehtäviin kuuluu muun muassa salaustuotteiden arviointi ja hyväksyntä kansallisen ja kansainvälisen turvallisuusluokitellun tiedon suojaamiseksi. Hyväksynnän tuloksia on mahdollista hyödyntää ja käyttää pohjana, mikäli tilaaja hakee samalle tuotteelle EU-salaustuotehyväksyntää[2]. Tässä ohjeessa kuvataan Traficomin salaustuotearviointi- ja hyväksyntäprosessi tilaajan näkökulmasta.

Arvioinnin ja hyväksynnän edellytykset sekä perittävät maksut

Arvioinnin tilaajalta edellytetään, että se toimittaa riittävät tiedot arviointisuunnitelman tekoa varten, nimeää vähintään yhden soveltuvan teknisen yhteyshenkilön vastaamaan arvioinnissa esiin tuleviin kysymyksiin sekä sitoutuu arviointiprojektin aikatauluun. Tilaajalta edellytetään myös, että se omalta osaltaan mahdollistaa arviointiprojektin kannalta tarvittavat resurssit, joihin tyypillisesti sisältyy testattavan tuotteen ja pyydetyn dokumentaation toimittaminen, tuotteeseen liittyvä koulutus sekä soveltuvat henkilöstö- ja tilavaraukset.

Traficom veloittaa arvioinnista työmäärään perustuvan maksun[3]. Ennen arviointiprosessin aloittamista tilaajalla on oikeus saada Traficomilta arvio työmäärästä ja maksun suuruudesta.

[1] Neuvoston päätös turvallisuussäännöistä EU:n turvallisuusluokiteltujen tietojen suojaamiseksi (2013/488/EU). URL: https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2013:274:0001:0050:FI:PDF.

[2] https://www.consilium.europa.eu/en/general-secretariat/corporate-policies/classified-information/information-assurance/

[3] https://www.finlex.fi/fi/laki/alkup/2019/20191453

Arviointiprosessin vaiheet

Arviointiprosessi koostuu seitsemästä keskeisestä vaiheesta sekä näitä täydentävistä osavaiheista. Seuraavassa kuvataan keskeiset vaiheet sillä tarkkuudella, että se antaa tilaajalle selkeän yleiskuvan siltä vaadittavista toimista. Arviointiprosessin kulku on havainnollistettu kuvassa 1.

1 Pyyntö tai yhteydenotto Traficomille

Arviointiprosessi alkaa tilaajan sähköpostiyhteydenotolla Traficomin Kyberturvallisuuskeskukseen[4]. Yhteydenotossa tulee ilmetä minkälaisesta tuotteesta on kyse, missä vaiheessa tuotteen kehitys on (suunnitteilla, valmisteilla, tuotannossa) sekä tuotteelle tavoiteltu suojaustaso. Tarvittaessa Traficom pyytää lisätietoja tilaajalta.

2 Pyynnön tarkastus ja Traficomin vastaus

Vastaanotettuaan pyynnön Traficom pyrkii vastaamaan pyynnön tekijälle kahden viikon kuluessa. Edellyttäen että tuote ja sen kehitysvaihe ovat arviointiprosessin kannalta sopivalla tasolla, toimittaa Traficom tilaajalle ehdotuksen esipalaverin ajaksi sekä listan esipalaveriin vaadittavista dokumenteista.

3 Esipalaveri valmistajan ja Traficomin välillä

Esipalaveri pidetään valmistajan ja Traficomin arvioijien kesken.

Esipalaverissa keskustellaan asiakkaan toimittamasta dokumentaatiosta, joita ovat muun muassa:

- Tuotteen toiminnallinen kuvaus - Käydään läpi tuotelupaus, tuotteen suorituskyky sekä toiminnallisuus. Lisäksi käydään läpi tuotteen kokonaisarkkitehtuuria ja sitä ympäröiviä elementtejä sekä uhkamalleja.
- Tuotteen salaustekniikka - Käydään läpi tuotteen salaustekniset ominaisuudet ja ratkaisut sekä avaintenhallinta.
- Arvioinnin tavoitetaso - Käydään läpi arvioinnin tavoitetaso ja sen saavutettavuus tuotteella aiotussa käyttötarkoituksessa.
- Aikaisemmat arvioinnit ja testaukset - Käydään läpi aiemmin tehdyt arvioinnit ja testaukset.
- Yritysturvallisuuteen ja tuotekehitykseen liittyvät turvallisuusasiat - katselmoidaan valmistajan tietoturvallisuusjärjestelyt ja tilaajan/viranomaisen mahdollinen tarve hakea valmistajasta yritysturvallisuusselvitystä

[4] Sähköpostiosoite caa@traficom.fi

- Viestintä - Keskustellaan asiakkaan kanssa voiko tuotteesta tai sen käynnissä olevasta arvioinnista viestiä esimerkiksi sidosryhmille.

Tarkempi kuvaus kaikista tuotearviointiin vaadittavista materiaaleista esitetään liitteenä olevassa listassa. Ennen arviointisuunnitelman laatimista ja sopimuksen tekoa tulee asiakkaan toimittaa dokumentaatio listan kohdista 1-4. Ensimmäinen esipalaveri voidaan kuitenkin järjestää, vaikka tarkkaa dokumentaatiota em. kohdista ei olisi toimitettu. Mikäli arviointisuunnittelun edellyttämiä tietoja ja dokumentaatiota ei saada järjestettyä esipalavereihin tai niitä ei pystytä toimittamaan esipalaverien jälkeen, arvioidaan arviointiprosessin päättäminen tapauskohtaisesti.

4 Arviointisuunnitelma ja sopimuksenteko

Traficom laatii arviointisuunnitelman, jossa kuvataan yleisellä tasolla kyseisen tuotteen arviointiin liittyvät asiakokonaisuudet sekä arvioinnin aikataulutus. Tilaajalle annetaan mahdollisuus kommentoida arviointisuunnitelmaa ja suunnitelma viimeistellään yhteistyössä tilaajan kanssa.

Kun Traficom on alustavasti arvioinut salaustuotearvioinnin laajuuden ja työmäärän, solmitaan sopimus arvioinnista Traficomin ja tilaajan välillä.

5 Arviointi

Tuotteen arvioinnin tarkoituksena on tutkia täyttääkö tuote sille asetetut tietoturvavaatimukset sekä toimiiko tuote kuvatulla tavalla.

Arvioinnin edetessä tilaajalle tai valmistajalle raportoidaan keskeisiä havaintoja, joiden pohjalta valmistajan on mahdollista tehdä tuotteeseen muutoksia. Mahdollisten muutosten jälkeen testit uusitaan tarvittavin osin sekä jatketaan tuotteen testaamista arviointisuunnitelman mukaisesti.

Arviointi voidaan aloittaa, kun asiakas on toimittanut materiaalin liitteenä olevan listan kohdista 5-8.

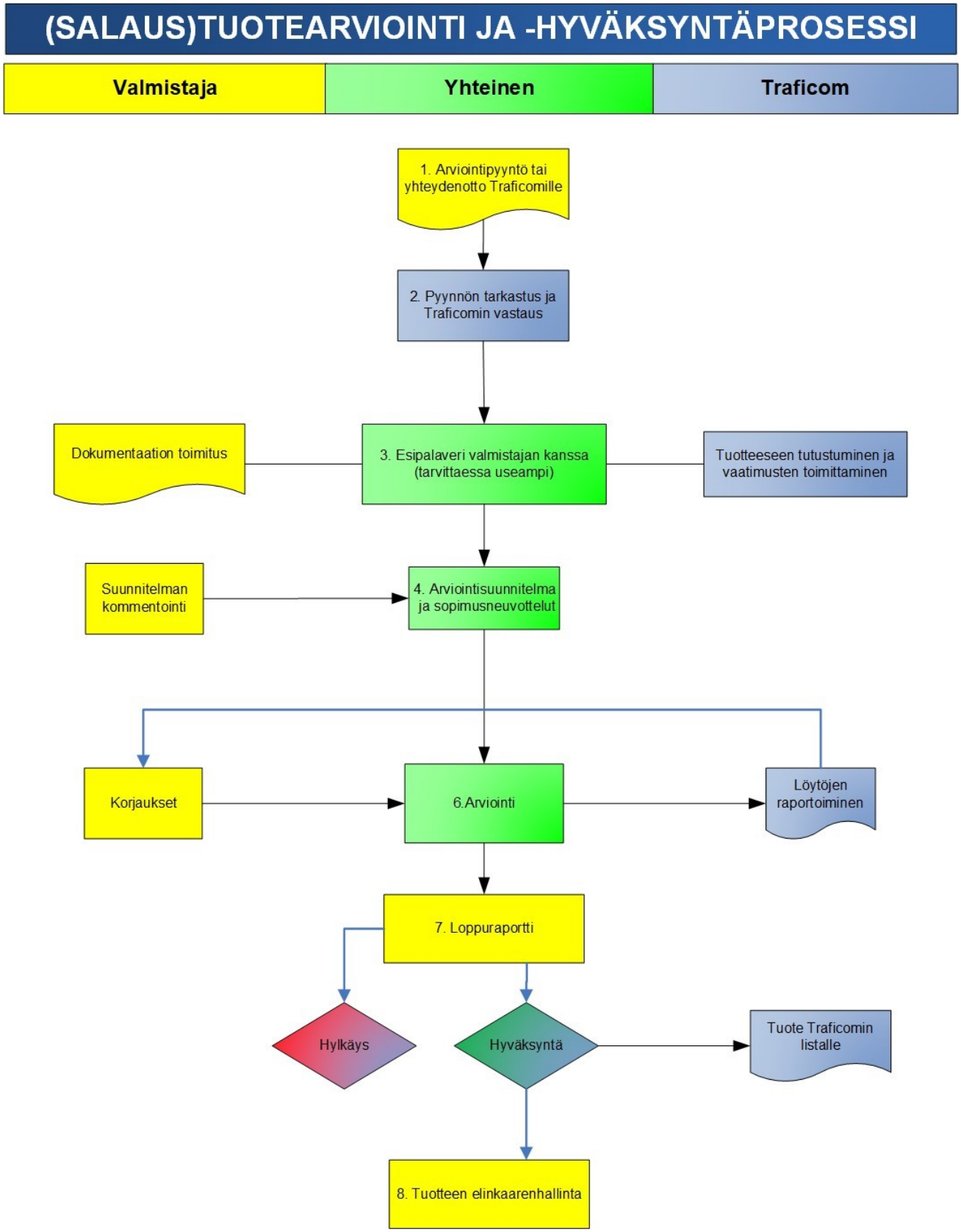
6 Loppuraportti

Kun arviointi on saatu päätökseen, annetaan arvio tuotteen vaatimustenmukaisuudesta. Vaatimustenmukaisille tuotteille myönnettävä hyväksyntä koskee tiettyä tuoteversiota ja on voimassa toistaiseksi. Hyväksytyt salaustuotteet lisätään Traficomin ylläpitämälle hyväksyttyjen salaustuotteiden listalle[5], ellei arvioinnin tilaaja tai valmistaja halua pitää hyväksyntää poissa julkisuudesta.

[5] https://www.kyberturvallisuuskeskus.fi/sites/default/files/media/file/NCSA_salausratkaisut.pdf

7 Tuotteen elinkaarenhallinta

Hyväksytyn tuotteen uudet ohjelmisto- tai tuoteversiot eivät automaattisesti ole hyväksyttyjä. Mikäli muutetulle tuotteelle halutaan hyväksyntää, tulee asiasta olla yhteydessä Traficomin Kyberturvallisuuskeskukseen. Arviointiprosessin aikana voidaan kuitenkin sopia valmistajan kanssa siitä, millaisia muutoksia hyväksynnän saaneelle tuotteelle voidaan tehdä ilman erillistä yhteydenottoa. Kriittisten ohjelmistohaavoittuvuuksien korjaamisen tulisi tapahtua mahdollisimman nopeasti ja asiasta tulisi olla välittömästi yhteydessä Kyberturvallisuuskeskukseen.


(SALAUS)TUOTEARVIOINTI JA -HYVÄKSYNTÄPROSESSI
Valmistaja
Yhteinen
Traficom
1. Arviointipyyntö tai yhteydenotto Traficomille
2. Pyynnön tarkastus ja Traficomin vastaus
Dokumentaation toimitus
3. Esipalaveri valmistajan kanssa (tarvittaessa useampi)
Tuotteeseen tutustuminen ja vaatimusten toimittaminen
Suunnitelman kommentointi
4. Arviointisuunnitelma ja sopimusneuvottelut
Korjaukset
6.Arviointi
Löytöjen raportoiminen
7. Loppuraportti
Hylkäys
Hyväksyntä
Tuote Traficomin listalle
8. Tuotteen elinkaarenhallinta

Appendix: Materials required for a full cryptographic product evaluation

1 Evaluation reports of previous certifications (FIPS, CC, etc. if relevant)

2 Functional description

A functional description must be supplied to enable an overall understanding of what the cryptographic product is intended to provide. This encompasses the following information:

(a) a system description in the context of the operating environment (to estimate the threats the cryptographic product is exposed to, and to determine the strength level;)
(b) an overview of the functionality including the use-cases relevant for the evaluation;
(c) a high level description of the architecture;
(d) high level design documentation;
(e) any external (non standard-) interfaces; and
(f) any other relevant security functionality.

3 Cryptographic specification

All cryptographic functions as part of the security functions of the cryptographic product are to be described in detail. In particular the following information is required:

(a) cryptographic algorithm for data encryption;
(b) cryptographic algorithm for key encryption;
(c) cryptographic algorithm initialisation;
(d) authentication and integrity mechanisms;
(e) random number generation;
(f) protocol descriptions where cryptographic information is involved, such as cryptographic synchronisation and key exchange mechanisms; and
(g) test data and test keys for verification of the correct implementation of the cryptographic algorithm(s).

4 Key management scheme

Description covering the following functions: key generation, key material fabrication, key protection, key registration, key establishment, key distribution, key storage, key archiving, key revocation, key renewal/replacement, key recovery, key destruction, crypto-period of key and type of certificate. Description of the procedure and/or mechanism for emergency erasure of keys.

Description of the distribution, handling and crypto-periods of physical keys (keycards) is not required at this point.

5 Testing keys and encryption samples

As an example: given a set of pre-defined root keys (these are keys in the top of the key architecture chain) and other similar material such as Diffie-Hellman secrets, samples of encrypted data (with pre-defined plaintext) must be provided.

6 Source code

All source code of the product must be of good quality and well documented and commented, including cryptographic functions and key management. When read together with the documentation, the source code must be understandable to a person who is not familiar with the product code base beforehand, but has an understanding of cryptography and programming

in general. Some of the documentation may be external to the source code, for example API descriptions.

In practice this includes, but is not limited to, the following:

- the purpose of functions, their parameters, return values, and error handling is described;
- naming of functions, variables, data structures etc. is descriptive and consistent;
- non-trivial data structures, variables, and code logic are described;
- well-known algorithms used/implemented are identified, proprietary algorithms are described in more detail (both crypto and other algorithms);
- unusual or otherwise unexpected decisions/logic/algorithms used in the code are justified;
- unused code is identified or removed altogether;
- coding style is consistent and the code is logically structured;
- duplication of cryptographic code is avoided;
- heavy re-use of functions which includes intense branching which in turn makes the code harder to interpret is avoided;
- secure coding practices are followed.

The source code of the product will be reviewed as part of the evaluation. The scope of the review depends on the desired protection level but at a minimum, the source code of the implementation of cryptographic functions and key management will be reviewed.

It will be beneficial if the source code can be compiled at the CAA unit as this will enable static testing of the code which may reduce the amount of code review necessary. CAA does not need to be able to build the whole product for this purpose, just to compile as much of the code as possible for instrumentation.

7 Description of product development processes

The description should outline at least the following processes:

(a) software development process that should include a general description of
- requirements,
- architecture and design,
- implementation,
- testing methodologies,
- deployment,
- maintenance;

(b) manufacturing process;
(c) product lifetime management process;
(d) vulnerability management process.

8 Functional equipment and instruction manuals

Typically the CAA unit will want to test the product in practice. The security architecture of the device will be reviewed and the testing will concentrate on the security controls of the device. The testing may include e.g. basic use cases, vulnerabilities, penetration testing and dynamic testing (fuzzing). In addition to this, code/script/settings of security controls, such as mandatory access control rules and firewall rules, will be statically reviewed. A device with debug software and/or firmware dump capability will help to speed up testing.

For further information concerning this list, please contact the National Cryptographic Approval Authority at TRAFICOM by email: caa@traficom.fi or ncsa@traficom.fi.