Transport- och kommunikationsverkets bedömningsanvisning för krypteringsprodukter och säkerhetskritiska produkter

Versionshistorik

Datum	Beskrivning/ändring
7.2.2025	Kombination av anvisningarna - *Bedömning och godkännande av krypteringsprodukter utförda av Transport- och kommunikationsverket Traficom – Beställarens perspektiv* (1487/651/2017, 6.3.2020) och - *Bedömning och godkännande av säkerhetskritiska produkter utförda av Transport- och kommunikationsverket Traficom – Beställarens perspektiv* (1487/651/2017, 4.1.2022) Följande läggs till och uppdateras: - villkor för tillverkarens ursprung - fastställande av tillitsnivåerna i bedömningen - bedömningsförfaranden/metoder - beskrivning av bedömningsprocessen - dokumentation som behövs för bedömningen (bilaga) - EU:s och Natos godkännanden av (krypterings-)produkter - utlåtanden och beslut som verket gett som resultat av bedömningen och när informationen om bedömningens resultat kan vara offentlig - behandling av handlingar och material enligt offentlighetslagen

Innehåll

1. Inledning

1.1 Anvisningens syfte

I denna anvisning beskrivs huvudprinciperna för bedömnings- och godkännandeprocesserna för krypteringsprodukter och andra säkerhetskritiska produkter samt olika situationer där Transport- och kommunikationsverket (Traficom) kan göra bedömningar. Anvisningen gäller produkter avsedda för skydd av elektronisk behandling av säkerhetsklassificerad information.

Anvisningen är avsedd för myndigheter och företag som ansvarar för säkerheten i sina informationssystem och som tillverkar krypterings- och säkerhetskritiska produkter. Syftet med anvisningen är att beskriva produkternas bedömningsprocesser och hurdana utlåtanden eller godkännanden Traficom kan ge utifrån bedömningen. Syftet med Traficoms bedömning är att stödja myndigheternas möjligheter att skaffa tillräckligt säkra produkter för att skydda säkerhetsklassificerad information och på så sätt stödja myndigheternas riskhanteringsarbete för att skydda sina informationssystem som behandlar säkerhetsklassificerad information. Bedömningsarbetet främjar indirekt också tillverkarnas konkurrenskraft och möjligheter att i rollen som produktleverantör delta i till exempel EU:s eller Natos informationssystemprojekt för skydd av säkerhetsklassificerad information.

Produktens planerade användningsändamål påverkar bedömningen. En central skillnad är huruvida det är fråga om en bedömning av skyddet av nationellt säkerhetsklassificerad information eller en internationell förpliktelse som gäller informationssäkerhet. Bedömningen påverkas också av huruvida den görs som en självständig produktbedömning eller som en del av utvärderingen av informationssystemet.

När det gäller skydd av nationellt säkerhetsklassificerad information kan den ansvariga myndigheten för informationssystemet besluta om de produkter som används i dess informationssystem utifrån sin riskbedömning och det är frivilligt att utnyttja produktbedömningar. I internationella förpliktelser som gäller informationssäkerhet förutsätts däremot vanligtvis att endast säkerhetskritiska produkter som bedömts och godkänts av den behöriga informationssäkerhetsmyndigheten används för att skydda säkerhetsklassificerad information.

Utöver denna anvisning ger Traficom handledning och råd om detaljerna i bedömningen från fall till fall.

1.2 Bestämmelser som anvisningen grundar sig på

Anvisningen grundar sig på Traficoms bedömningsuppgifter, om vilka föreskrivs i 4 § i lagen om bedömning av informationssäkerheten i myndigheternas informationssystem och datakommunikation (1406/2011, bedömningslagen), 9 § 3 mom. i säkerhetsutredningslagen (726/2014) och 4 § i lagen om internationella förpliktelser som gäller informationssäkerhet (588/2004, internationella informationssäkerhetslagen).

Enligt 4 § i den internationella informationssäkerhetslagen är Traficom nationell godkännandemyndighet för krypteringsprodukter (CAA, Crypto Approval Authority), om vilken det föreskrivs i artikel 10.6 och bilaga IV i EU-rådets säkerhetsbestämmelser EU/488/2013.

Traficom är också nationell säkerhetsmyndighet för kommunikations- och informationssystem (NCSA, National CIS Security Authority), om vilken föreskrivs i punkterna 11 och 13 i bilaga F till Natos säkerhetsbestämmelse C-M(2002)49-

REV1 (se lagen om avtalet mellan parterna i nordatlantiska fördraget om informationssäkerhet samt säkerhetsbestämmelserna (907/2023), FördrS 55/2023, FördrS 56/2023).

Traficoms uppgifter fastställs i lagen om Transport- och kommunikationsverket (23.11.2018/935). Enligt den har Cybersäkerhetscentret vid Transport- och kommunikationsverket till uppgift att stödja, styra och övervaka informationssäkerheten och tillgodoseendet av integritetsskyddet vid elektronisk kommunikation. Cybersäkerhetscentret ska upprätthålla en lägesbild över den nationella cybersäkerheten. Cybersäkerhetscentret ska i sin verksamhet främja och säkerställa informationssäkerheten i informationssystem och datakommunikation.

Bestämmelserna behandlas närmare nedan.

1.3 Anvisningens förhållande till annan produktreglering och bedömning

1.3.1 CRA

Denna anvisning gäller inte produktsäkerhetsbedömningar enligt EU:s cyberresiliensförordning (EU) 2024/2847 (s.k. CRA, Cyber Resilience Act). Enligt artikel 2.7 ska förordningen inte tillämpas på produkter med digitala element som utvecklats eller ändrats uteslutande för ändamål som rör nationell säkerhet eller försvarsändamål eller på produkter som utformats specifikt för att behandla säkerhetsskyddsklassificerade uppgifter. Förordningen hindrar dock inte att en produkt som tillhandahålls på marknaden bedöms i syfte att skydda säkerhetsklassificerad myndighetsinformation. CRA gäller apparater med digitala element och programvara, vilka direkt eller indirekt kan anslutas till en annan enhet eller ett nät.

1.3.2 Bedömningsorgan eller andra bedömningsinstanser

Bedömningsuppgifterna i anslutning till **internationella förpliktelser som gäller informationssäkerhet** föreskrivs i den internationella informationssäkerhetslagen tillhöra Traficom. Utläggning av uppgifter på entreprenad genom avtal eller möjliggörande av kompetens för bedömningsorganet för informationssäkerhet förutsätter att regleringen utvecklas.

Även för uppgiften att skydda **nationellt säkerhetsklassificerad information** i Traficoms produktbedömningar, som görs med stöd av bedömningslagen, skulle en utkontraktering av bedömningen helt eller delvis förutsätta att regleringsgrunden kompletteras.

I princip är det möjligt att ansöka om behörighet för bedömning av produkter som används för behandling av **nationellt säkerhetsklassificerad information** med stöd av lagen om bedömningsorgan för informationssäkerhet (1405/2011, lagen om bedömningsorgan). Detta förutsätter bland annat att kriterierna för påvisande av kompetens utvecklas samt att nödvändig kompetens byggs upp för bedömningsorgan för informationssäkerhet. Traficom stöder vid behov bedömningsorganens bedömningar av krypteringslösningar och andra säkerhetskritiska produkter.

Traficom gör bedömningar enligt avtal på tillverkarens begäran med stöd av ämbetsverkslagen. I detta sammanhang har Traficom ingått ett enskilt avtal av pilotkaraktär med en extern bedömningsinstans. Om parterna avtalar om det från fall till fall kan bedömningsinstansen i fråga testa och inspektera en viss säkerhetskritisk produkttyp under ledning av Traficom och Traficom utnyttjar resultatet av inspektionen i sitt eget utlåtande. Förfarandet förutsätter att tillverkaren ingår ett avtal med bedömningsinstansen i fråga. Transport- och kommunikationsverket är inte part i avtalet mellan tillverkaren och

bedömningsinstansen och bedömningsinstansen är inte heller part i avtalet mellan tillverkaren och Transport- och kommunikationsverket. Traficom granskar produktens bedömningsplan. Bedömningsinstansen följer de kriterier som Traficom fastställt, ger Traficom alla uppgifter om bedömningen och följer Traficoms anvisningar och riktlinjer i alla skeden av bedömningsprocessen. Traficom bedömer om det finns förutsättningar för att avge ett utlåtande och avger ett utlåtande.

1.3.3 Hantering av diffus strålning och kryptografiskt material

I denna anvisning behandlas inte bedömningen av skyddskapaciteten hos krypteringsprodukter eller säkerhetskritiska produkter mot hot som orsakas av diffus strålning (TEMPEST-skyddsåtgärder). De bedöms vid behov enligt egna bestämmelser och anvisningar.

I denna anvisning behandlas inte hantering av krypteringsenheter och annat kryptografiskt material såsom krypteringsnycklar (COMSEC-förfaranden).

1.4 Anvisningens ikraftträdande och tilläggsuppgifter

Denna anvisning träder i kraft 7.2.2025. Anvisningen gäller tills vidare.

Med denna anvisning kombineras och uppdateras de tidigare anvisningarna Bedömning och godkännande av krypteringsprodukter utförda av Transport- och kommunikationsverket Traficom – Beställarens perspektiv (1487/651/2017, 6.3.2020) och Bedömning och godkännande av säkerhetskritiska produkter utförda av Transport- och kommunikationsverket Traficom – Beställarens perspektiv (1487/651/2017, 4.1.2022)

Anvisningen kompletteras och ändras vid behov. De ändrade versionerna av anvisningen finns listade i versionshistoriken på sida 2.

Mer information kan begäras på adressen ncsa@traficom.fi.

2. Definitioner

I detta kapitel definieras de termer som används i anvisningen. Syftet med definitionerna är att underlätta läsningen av anvisningen. I definitionerna har man strävat efter att beakta terminologin i olika författningar, men terminologin i regleringen är inte enhetlig. I den nationella regleringen behandlas inte produkter uttryckligen och det finns skillnader i detaljerna i EU:s och Natos säkerhetsbestämmelser. Vid tolkningen av varje författning ska definitionerna i författningen alltid granskas.

En **krypteringsprodukt** är en produkt eller lösning vars primära och huvudsakliga syfte är att skydda informationens konfidentialitet, integritet, användbarhet, äkthet och/eller obestridlighet med hjälp av en eller flera krypteringsmetoder.

Med **säkerhetskritisk produkt** avses en produkt som i informationssystemet har en kritisk roll i skyddet av säkerhetsklassificerad information. Den kritiska rollen består vanligtvis av att produkten skyddar säkerhetsklassificerad information mot externa aktörer, varvid eventuella säkerhetsbrister i produkten vanligtvis inte kan kompenseras med andra skydd. Typiska exempel är gatewaylösningar som används för att separera miljöer i olika säkerhetsklasser.

En **internationell förpliktelse som gäller informationssäkerhet** innebär vad som föreskrivs i lagen om internationella förpliktelser som gäller informationssäkerhet. Skyddet av till exempel EU:s och Natos säkerhetsklassificerade information är förknippat med skyldigheter gällande godkännande av krypteringsprodukter och vissa andra produkter samt reglering av kraven på produkterna och tillverkningen av dem.

Med **tillverkare** avses ett företag som utvecklar, planerar, tillverkar, sätter ihop och underhåller en produkt.

Med **väsentlig** underleverantör avses ett företag som erbjuder en komponent eller annan del av en produkt som är väsentlig med tanke på produktens egenskaper som ska bedömas.

Med **kundmyndighet** avses en myndighet som behöver integrera produkten i sitt informationssystem och som därför förordar en bedömning av produkten. Definitionen förutsätter inte att det finns ett upphandlingsavtal.

Krav avser antingen föreskrivna krav eller kriterier som används i bedömningen.

Kriterierna avser på förhand fastställda regler som allmänt används för skydd av säkerhetsklassificerad information eller regler som Traficom preciserar och definierar i sina myndighetsuppgifter och som produkten jämförs med. I internationella förpliktelser som gäller informationssäkerhet fastställs kriterierna enligt de krav som vid respektive tidpunkt föreskrivs i internationella förpliktelser. För att skydda nationellt säkerhetsklassificerad information används inom ramen för de allmänna kraven i informationshanteringslagen och förordningen om säkerhetsklassificering allmän teknisk och god praxis som bestäms av Traficom och där internationell praxis har beaktats.

Med **inspektion** avses konkret observation och testning av produktens och tillverkningens tekniska, funktionella och logiska komponenter såsom en enhet, algoritmer och programkod med olika metoder

Bedömning innebär att man granskar och analyserar dokumentationen, utredningen och inspektionsobservationerna om tillverkaren och produkten och jämför dem med kriterierna och kraven.

Tillitsnivå avser hur kombinationen av bedömningsmetoder som används i bedömningen påverkar hur en tillförlitlig uppfattning om produktens säkerhet kan skapas. Tillitsnivån innebär således inte en klassificering av produktens säkerhet utan i vilken mån den har kunnat bedömas. Tillitsnivåklassificeringen har som sådan ingen direkt motsvarighet i den övriga regleringen, men termen används allmänt inom branschen. Syftet med klassificeringen i denna anvisning är att öka myndigheternas och tillverkarnas information om säker överensstämmelse med kraven som bedömningen ger och att fungera som ett verktyg för att definiera bedömningen.

Överensstämmelse med kraven innebär att produktens egenskaper och omständigheterna i anslutning till skyddet av tillverkningen och underhållet av produkten motsvarar de kriterier som använts i bedömningen. Krypteringsprodukternas och de säkerhetskritiska produkternas överensstämmelse med kraven fastställs alltid enligt någon säkerhetsklass. Överensstämmelse med kraven kan fastställas i förhållande till nationella säkerhetsklasser (SK I–SK IV) och/eller internationella klasser (till exempel EU-R eller NR).

Ett **utlåtande** är Traficoms skriftliga bedömning av om produkten uppfyller kraven för skydd av information enligt den säkerhetsklass som tillämpats i bedömningen.

Godkännande innebär ett skriftligt förvaltningsbeslut av Traficom om att den bedömda produkten uppfyller de krav på skydd av information i en viss säkerhetsklass som tillämpats i bedömningen och som grundar sig på en internationell förpliktelse som gäller informationssäkerhet.

Med **användningspolicy** avses Traficoms utlåtande eller godkännande om de användningssätt som krävs för skydd enligt säkerhetsklass.

3. Bestämmelser

I följande kapitel beskrivs de bestämmelser utifrån vilka Traficom gör produktbedömningar och på vilka denna anvisning grundar sig.

3.1 Produktbedömningar för skydd av nationellt säkerhetsklassificerad information

3.1.1 Myndighetsbegäranden

Traficom gör produktbedömningar som en del av bedömningen av informationssäkerheten i myndigheternas informationssystem eller datakommunikation med stöd av 4 § i lagen om bedömning av informationssäkerheten i myndigheternas informationssystem och datakommunikation (1406/2011, bedömningslagen). Lagen möjliggör endast myndighetsbegäranden, så Traficom kan inte med stöd av denna lag göra bedömningar på tillverkarnas begäran. Bestämmelser om bedömningsgrunderna finns i 7 §.

Bedömningslagen *4 § Kommunikationsverkets uppgifter*

Kommunikationsverket ska i syfte att främja och säkerställa informationssäkerheten i myndigheternas informationssystem och datakommunikation
1) på en myndighets begäran göra en bedömning av överensstämmelse med kraven på informationssäkerhet i fråga om informationssystem eller datakommunikation som myndigheten bestämmer över eller planerar att skaffa,
[…]

Bedömningslagen *7 § Bedömningsgrunder för informationssäkerhet*

Som bedömningsgrunder för informationssäkerheten i myndigheternas informationssystem och datakommunikation kan Kommunikationsverket använda
1) i lag eller förordning föreskrivna krav på informationssäkerheten i myndigheternas verksamhet samt finansministeriets anvisningar om informationssäkerhet,
2) anvisningar om uppfyllande av internationella informationssäkerhetsförpliktelser som meddelats av den nationella säkerhetsmyndighet som avses i lagen om internationella förpliktelser som gäller informationssäkerhet,
3) Europeiska unionens eller något annat internationellt organs bestämmelser och anvisningar om informationssäkerhet,
4) publicerade allmänt eller regionalt tillämpade bestämmelser, föreskrifter eller anvisningar om informationssäkerhet,
5) informationssäkerhetskrav som ingår i en fastställd standard.

Kommunikationsverket utreder om informationssystemet eller datakommunikationen uppfyller de krav angående informationssäkerheten som utgör bedömningsgrunder. Bedömningen kan även vara partiell.

Traficom gör också en bedömning av produkterna som en del av en säkerhetsutredning av företag när den på begäran av skyddspolisen eller huvudstaben gör en utredning enligt 9 § 3 mom. i säkerhetsutredningslagen om nivån på informationssäkerheten i informationssystem och datakommunikation.

Säkerhetsutredningslagen *9 § Behöriga myndigheter*

[…]

Kommunikationsverket gör som ett led i en säkerhetsutredning av företag en utredning om nivån på informationssäkerheten i informationssystem och datakommunikation.

[…]

3.1.2 Tillverkarnas begäranden

Traficom gör produktbedömningar även på tillverkarnas begäran. Även då ska någon myndighet ha behov av produkten. Behandlingen av tillverkarens begäran om bedömning förutsätter ett avtal med tillverkaren. Traficoms möjlighet att ingå avtal grundar sig på lagen om Transport- och kommunikationsverket (935/2018, ämbetsverkslagen). Den lagstadgade uppgiften att främja informationssäkerheten anknyter bland annat till statsrådets förordning om säkerhetsklassificering av handlingar. Om avgifterna för bedömningarna föreskrivs separat.

Ämbetsverkslagen *3 § Cybersäkerhetscentrets uppgifter*

Transport- och kommunikationsverkets cybersäkerhetscenter, nedan Cybersäkerhetscentret, har till uppgift att stödja, styra och övervaka informationssäkerheten och tillgodoseendet av integritetsskyddet vid elektronisk kommunikation. Cybersäkerhetscentret ska upprätthålla en lägesbild över den nationella cybersäkerheten. Cybersäkerhetscentret ska i sin verksamhet främja och säkerställa informationssäkerheten i informationssystem och datakommunikation. Cybersäkerhetscentret är ansvarig myndighet för den offentligt reglerade satellittjänsten och nationellt samordningscentrum enligt artikel 6 i Europaparlamentets och rådets förordning (EU) 2021/887 om inrättande av Europeiska kompetenscentrumet för cybersäkerhet inom näringsliv, teknik och forskning och av nätverket av nationella samordningscentrum. Dessutom ska Cybersäkerhetscentret sörja för kommunikationsbranschens beredskap för störningssituationer under normala förhållanden och för undantagsförhållanden, främja och övervaka funktionssäkerheten i den elektroniska kommunikationen samt inom sitt verksamhetsområde stödja samhällets allmänna beredskap för störningssituationer under normala förhållanden och för undantagsförhållanden. (19.11.2021/1002)

[…]

Transport- och kommunikationsverket kan tillhandahålla sådana offentligrättsliga prestationer eller enligt företagsekonomiska grunder prissatta prestationer som baserar sig på Cybersäkerhetscentrets uppgifter enligt 1 mom., samt ingå avtal om utförandet av sådana prestationer.

3.2 Produktgodkännanden för internationella förpliktelser som gäller informationssäkerhet

Internationella förpliktelser som gäller informationssäkerhet gäller skydd av säkerhetsklassificerad information från en annan stat eller en internationell organisation eller ett internationellt organ i Finland. Bestämmelser om skyldigheter i anslutning till sådant *särskilt känsligt informationsmaterial* finns i lagen om internationella förpliktelser som gäller informationssäkerhet (588/2004, internationella informationssäkerhetslagen). Skyldigheterna gäller alla organisationer och personer som behandlar säkerhetsklassificerad information.

Internationella förpliktelser som gäller informationssäkerhet grundar sig på ett internationellt avtal som är bindande för Finland eller någon annan förpliktelse som gäller Finland. Finlands internationella informationssäkerhetsavtal (GSA, General Security Agreement) finns på utrikesministeriets nationella säkerhetsmyndighets (NSA, National Security Authority) webbplats[1]. EU:s och Natos skyldigheter att skydda säkerhetsklassificerad information grundar sig på EU-rådets säkerhetsbestämmelse EU/488/2013[2] och Natos säkerhetsbestämmelse C-M(2002)49-REV1[3].

[1] https://um.fi/finlands-bilaterala-informationssakerhetsavtal
[2] https://eur-lex.europa.eu/legal-content/SV/TXT/?uri=CELEX%3A32013D0488
[3] Se lagen om avtalet mellan parterna i nordatlantiska fördraget om informationssäkerhet samt säkerhetsbestämmelserna (907/2023), FördrS 55/2023, FördrS 56/2023. Dokumentet C-M(2002)49-REV1 och översättningen till svenska finns i RP 4/2023 rd https://www.eduskunta.fi/SV/vaski/HallituksenEsitys/Documents/RP_4+2023.pdf

Traficoms produktbedömningsuppgift grundar sig i egenskap av utsedd säkerhetsmyndighet på 4 § i internationella informationssäkerhetslagen i ärenden som gäller informationssäkerheten i informationssystem och datakommunikation. I EU:s och Natos säkerhetsbestämmelser och internationella informationssäkerhetsavtal fastställs närmare skyldigheterna att bedöma och godkänna krypteringsprodukter eller andra säkerhetskritiska produkter. I dessa situationer är bedömningen och godkännandet alltså obligatoriskt till skillnad från skyddet av nationellt säkerhetsklassificerad information.

Den internationella informationssäkerhetslagen *4 § Säkerhetsmyndigheterna och deras uppgifter*

Utrikesministeriet är Finlands nationella säkerhetsmyndighet vid uppfyllandet av internationella förpliktelser som gäller informationssäkerhet. Försvarsministeriet, huvudstaben, skyddspolisen och Kommunikationsverket är sådana utsedda säkerhetsmyndigheter som avses i internationella förpliktelser som gäller informationssäkerhet.

Den nationella säkerhetsmyndigheten har till uppgift att i synnerhet styra och övervaka att det särskilt känsliga informationsmaterial som avses i denna lag skyddas och att det hanteras på ett lämpligt sätt.

De utsedda säkerhetsmyndigheterna utför de uppgifter som föreskrivs för dem i denna lag och andra uppgifter som följer av internationella förpliktelser som gäller informationssäkerhet. Försvarsministeriet, huvudstaben och skyddspolisen är den nationella säkerhetsmyndighetens sakkunniga i ärenden som gäller personalsäkerhet, företagssäkerhet och lokalsäkerhet samt Kommunikationsverket i ärenden som gäller informationssäkerhet i fråga om informationssystem och datakommunikation. (19.9.2014/731)

Till Traficoms uppgifter enligt 4 § i internationella informationssäkerhetslagen hör att godkänna krypteringsutrustning enligt EU-rådets säkerhetsbestämmelse (CAA, Crypto Approval Authority)

EU/488/2013 *artikel 10 Skydd av säkerhetsskyddsklassificerade EU-uppgifter i kommunikations- och informationssystem*

6. Om de säkerhetsskyddsklassificerade EU-uppgifterna skyddas med hjälp av kryptoprodukter, ska sådana produkter godkännas på följande sätt:

a) Konfidentialiteten för uppgifter på säkerhetsskyddsklassificeringsnivån SECRET UE/EU SECRET och högre ska skyddas genom kryptoprodukter som har godkänts av rådet i egenskap av kryptogodkännande myndighet på rekommendation av säkerhetskommittén.

b) Konfidentialiteten för uppgifter på säkerhetsskyddsklassificeringsnivån CONFIDENTIEL UE/EU CONFIDENTIAL eller RESTREINT UE/EU RESTRICTED ska skyddas genom kryptoprodukter som har godkänts av rådets generalsekreterare (nedan kallad generalsekreteraren) i egenskap av kryptogodkännande myndighet på rekommendation av säkerhetskommittén.

Trots vad som sägs i led b får säkerhetsskyddsklassificerade EU-uppgifter på säkerhetsskyddsklassificeringsnivån CONFIDENTIEL UE/EU CONFIDENTIAL eller RESTREINT UE/EU RESTRICTED inom medlemsstaternas nationella system skyddas genom kryptoprodukter som har godkänts av en medlemsstats kryptogodkännande myndighet.

Bilaga IV *25. Kryptoprodukter för skydd av säkerhetsskyddsklassificerade EU-uppgifter ska evalueras och godkännas av en medlemsstats nationella kryptogodkännande myndighet.*

Bilaga IV *46. Den kryptogodkännande myndigheten ska ansvara för att kryptoprodukter överensstämmer med nationell kryptopolicy eller rådets kryptopolicy. Den ska bevilja godkännande av en kryptoprodukt för att skydda säkerhetsskyddsklassificerade EU-uppgifter i deras driftsmiljö upp till en fastställd säkerhetsskyddsklassificeringsnivå. När det gäller medlemsstaterna ska den kryptogodkännande myndigheten dessutom ansvara för utvärderingen av kryptoprodukter.*

Jfr Bilaga IV 48. Ackrediteringsmyndigheten för säkerhet; Security Accreditation Authority: g) stödja urval av godkända kryptoprodukter och tempestprodukter som används för säkra ett kommunikations- och informationssystem.

Till Traficoms uppgifter enligt 4 § i internationella informationssäkerhetslagen hör att agera som säkerhetsmyndighet för kommunikations- och informationssystem enligt Natos säkerhetsbestämmelse (NCSA, National CIS Security Authority, CIS, Communications and Information Systems)

C-M(2002)49-REV1 Bilaga F *11. KRYPTOGRAFISK SÄKERHET*
11.1. När kryptografiska produkter eller mekanismer krävs för att tillhandahålla konfidentiellt och icke-konfidentiellt skydd, oavsett om det gäller överföring, behandling eller lagring av information (data i vila), ska produkterna eller mekanismerna vara särskilt godkända för ändamålet och särskilda kryptografiska krav för fysiska, förfarandemässiga och tekniska åtgärder ska genomföras för att nå de säkerhetsmål som krävs.

11.3. Under överföringen ska konfidentialiteten för information som säkerhetsskyddsklassificerats som NATO SECRET eller högre skyddas med kryptografiska produkter eller mekanismer som godkänts av Natos militärkommitté (NAMILCOM).

11.4. Under överföringen ska konfidentialiteten för information som säkerhetsskyddsklassificerats som NATO CONFIDENTIAL eller NATO RESTRICTED skyddas med kryptografiska produkter eller mekanismer som godkänts av antingen Natos militärkommitté (NAMILCOM) eller en medlemsstat i Nato.

13.4. Nationell säkerhetsmyndighet för kommunikations- och informationssystem

13.4.1. Varje medlemsstat i Nato, och i tillämpliga fall stater utanför Nato, ska fastställa en nationell säkerhetsmyndighet för kommunikations- och informationssystem som får inrättas som en byrå inom den nationella säkerhetsinfrastrukturen. Den nationella säkerhetsmyndigheten för kommunikations- och informationssystem svarar för att
a) kontrollera kryptografisk teknisk information i anslutning till skyddet av Natoinformation i staten i fråga,
b) se till att kryptografiska system, produkter och mekanismer som används för att skydda Natoinformation väljs, används och underhålls som sig bör,
c) se till att säkerhetsprodukter som används för att skydda Natoinformation i kommunikations- och informationssystem (CIS) väljs, används och underhålls som sig bör i den egna staten,
[…]

I den preciserande regleringen (AC/35-D/2005-REV3) tas också ställning till förfarandet för bedömning och godkännande av andra säkerhetskritiska produkter (SEP, Security Enforcing Products).

9.3.5 The approval of a security enforcing product is a formal statement, by a National CIS Security Authority (NCSA), supported by an independent review of the conduct and results of an evaluation and/or a certification, approving the use of a product for a specific purpose and under specific conditions. The approval of a security enforcing product for a CIS is a two-step process: while the approval by an NCSA is required to declare the product suitable for the protection of NATO information, the approval by an SAA is related to its use in the context of a specific CIS, as part of the security accreditation process.

4. Bedömningsuppgifternas offentlighet

4.1 Handlingarnas offentlighet och sekretess

Traficom bedömer och avgör alltid från fall till fall om det material och de uppgifter som erhållits i verkets bedömningsuppgift samt de handlingar som verket upprättat utifrån bedömningen är offentliga eller helt eller delvis sekretessbelagda eller även säkerhetsklassificerade.

4.1.1 Material som Traficom erhållit

Material och uppgifter som lämnats till Traficom i samband med bedömningen är myndighetshandlingar som Traficom behandlar i enlighet med lagen om offentlighet i myndigheternas verksamhet (621/1999, offentlighetslagen), informationshanteringslagen och förordningen om säkerhetsklassificering.

Traficom bedömer alltid offentligheten för uppgifterna eller grunderna för sekretess- eller säkerhetsklassificering på tjänstens vägnar och hör vid behov tillverkaren eller kundmyndigheten. I 24 § i offentlighetslagen föreskrivs om grunderna för sekretess för myndighetsuppgifter. Enligt bestämmelsen är näringsidkares affärshemligheter sekretessbelagda. Sekretessbelagda kan också vara till exempel uppgifter om skyddsarrangemang i informations- och kommunikationssystem eller uppgifter om försvaret.

Traficoms produktbedömningar gäller alltid behoven av att skydda säkerhetsklassificerad information. Det detaljerade materialet i anslutning till tillverkarens produkter kan innehålla både uppgifter som kan skyddas som affärshemligheter och uppgifter som påverkar skyddsarrangemangen i informations- och kommunikationssystemen. Till exempel är produktens källkod vanligtvis information som i ljuset av offentlighetslagen ska skyddas både som affärshemlighet och som information som påverkar skyddsarrangemangen i informations- och kommunikationssystemen. På grund av affärshemlighetselementet kunde Traficom enligt offentlighetslagen lämna ut uppgifter till exempelvis kundmyndigheter endast med tillverkarens samtycke, och på grund av skyddsarrangemangselementet ska uppgifterna säkerhetsklassificeras och skyddas i informationssystemen på det sätt som säkerhetsklassen förutsätter.

4.1.2 Handlingar upprättade av Traficom

Offentligheten eller sekretessen för de handlingar som Traficom upprättat under bedömningen och de handlingar som Traficom gett som slutresultat av bedömningen bedöms helt eller delvis i enlighet med offentlighetslagen utifrån uppgifterna i handlingen. I offentligheten av slutresultatet av Traficoms bedömning måste man skilja mellan information om slutresultatet av bedömningen och olika handlingar i anslutning till ärendet, vilka bland annat kan vara själva utlåtandet eller beslutet och användningspolicyn i anslutning till utlåtandet eller beslutet, bedömningsrapporten eller det kryptologiska utlåtandet.

Informationen om slutresultatet av Traficoms bedömning kan vara offentlig eller sekretessbelagd. Detta påverkas bland annat av bedömningens tillitsnivå.

- Slutresultatet av en bedömning med hög tillitsnivå (A) kan i regel vara offentligt. Traficom publicerar då information på sin webbplats om att ett utlåtande eller godkännande har getts för produkten, om inte något annat avtalas av grundad anledning som hänför sig till myndighetens verksamhet. Hela handlingen publiceras inte på webbplatsen, men till den del den är offentlig har vem som helst enligt offentlighetslagen rätt att få den på begäran.

- Slutresultatet av en bedömning på medelhög (B) eller låg tillitsnivå (C) är som standard sekretessbelagt och ges till den myndighet som begärt bedömningen och till produktens tillverkare för kännedom.

- Den användningspolicy eller de anvisningar som Traficom utarbetat i samband med utlåtandet eller godkännandet kan vanligtvis vara sekretessbelagda eller säkerhetsklassificerade. Detsamma gäller bedömningsrapporten och det kryptologiska utlåtandet, eftersom de utan undantag innehåller detaljer som påverkar skyddsarrangemangen.

Som ovan konstaterats kan Traficom göra en produktbedömning på tillverkarens begäran, om tillverkaren och Traficom har haft förutsättningar att ingå ett avtal om produktbedömning. Då är de allmänna villkoren i avtalsmodellen i princip offentliga. Företagets namn och de produkter som bedöms kan däremot vara sekretessbelagd information tills bedömningen är klar. Avtalet och bedömningen av produkten kan vara sekretessbelagd information även efter bedömningen, om det finns ovan beskrivna grunder för sekretess. Enligt avtal görs dock i regel endast bedömningar med omfattande tillitsnivå, varvid det i allmänhet finns förutsättningar för att slutresultatet ska vara offentligt.

4.2 Utlämnande av sekretessbelagda och säkerhetsklassificerade handlingar

Traficom kan vid behov i enlighet med offentlighetslagen lämna ut information om bedömningen av en produkt till en myndighet som är intresserad av att köpa produkten eller till någon annan tredje part. Utlämnande av uppgifter som innehåller affärshemligheter förutsätter tillverkarens samtycke i enlighet med offentlighetslagen. På vissa andra grunder som föreskrivs i 24 § i offentlighetslagen kan Traficom utan tillverkarens samtycke från fall till fall bedöma utlämnandet av sekretessbelagda uppgifter i enlighet med den klausul om skaderekvisit som föreskrivs för varje sekretessgrund i paragrafen. I prövningen bedömer Traficom om utlämnandet av uppgifter kan orsaka skada för det intresse som ska skyddas. Mottagaren av sekretessbelagda uppgifter omfattas av sekretess- och tystnadsplikten i offentlighetslagen.

Traficom kan i samband med bedömningen lämna ut sekretessbelagda och säkerhetsklassificerade handlingar till tillverkaren av krypterings- och säkerhetskritiska produkter.

När handlingarna är säkerhetsklassificerade och Traficom överlåter handlingarna vidare, ska Traficom se till att de säkerhetsklassificerade handlingar och uppgifter som lämnas ut behandlas i enlighet med kraven.

Förordningen om säkerhetsklassificering *6 § Förutsättningar för utlämnande av en säkerhetsklassificerad handling*

En statsförvaltningsmyndighet ska på förhand säkerställa att en säkerhetsklassificerad handling skyddas på behörigt sätt om myndigheten lämnar ut den till någon annan än en statsförvaltningsmyndighet. Kravet gäller inte utlämnande av information om handlingens innehåll på grundval av en parts rätt att få information.
[…]

Tillverkaren ska förbinda sig att hemlighålla en handling eller uppgift som den erhållit av Traficom och som verket har antecknat eller anmält som sekretessbelagd eller som har säkerhetsklassificerats. Tillverkaren kan överlämna sekretessbelagda handlingar som hänför sig till produkten till den myndighet som behöver dem för eventuell anskaffning eller användning av produkten. Tillverkaren ska på förhand informera om sekretessen och en eventuell säkerhetsklassificering av handlingen så att myndigheten kan överväga hur den ska behandlas. Utlämnande av handlingar och uppgifter till ett annat företag ska utredas från fall till fall tillsammans med Traficom.

Om det finns ett motiverat behov (need-to-know) för tillverkaren att på basis av en internationell förpliktelse som gäller informationssäkerhet överlämna särskilt känsliga, dvs. säkerhetsklassificerade handlingar, förbinder Traficom tillverkaren att behandla och skydda uppgifterna i enlighet med kraven och att använda uppgifterna endast för bedömning och produktutvecklingen i anslutning till den. I praktiken upprättar Traficom innan uppgifterna lämnas ut en förbindelse för att undertecknas av företaget. I förbindelsen specificeras de krav som fastställs utifrån säkerhetsklassen och introduceras företaget i kraven på skydd av information. I

förbindelsen krävs att tillverkaren skyddar och behandlar den utlämnade informationen i enlighet med de nationella bestämmelserna och den uppdaterade versionen av den nationella säkerhetsmyndighetens *anvisning om hantering av internationellt säkerhetsklassificerat informationsmaterial*[4]. Vid behov förutsätts av tillverkaren ett intyg över säkerhetsutredning av företag (FSC, Facility Security Clearance) i enlighet med de uppgifter som lämnas ut.

Internationella informationssäkerhetslagen *6 § Sekretess och användning av information*

Särskilt känsligt informationsmaterial ska sekretessbeläggas, om inte annat följer av en internationell förpliktelse som gäller informationssäkerhet. (22.10.2010/885)

Särskilt känsligt informationsmaterial får användas och lämnas ut endast för angivet ändamål, om inte den som bestämt materialets säkerhetsklass har samtyckt till något annat.

En myndighet som hanterar särskilt känsligt informationsmaterial skall se till att endast personer som behöver informationen för skötsel av sina uppgifter har tillgång till materialet. Dessa personer skall i de fall som den internationella förpliktelsen som gäller informationssäkerhet förutsätter namnges på förhand. Detsamma gäller näringsidkare som avses 1 § 2 mom.

5. Allmänna förutsättningar för bedömningen

5.1 Produktens förutsättningar

En förutsättning för att en produkt ska tas upp till bedömning är att produkten är tekniskt avgränsad och lämplig för kryptering av information eller annat skydd i informations- eller datakommunikationssystem. Vid tolkningen av produkttypens bedömningsduglighet stöder man sig på principerna och tillämpningspraxisen enligt internationella förpliktelser som gäller informationssäkerhet.

Tillverkningen av krypteringsprodukter och andra säkerhetskritiska produkter ska i tillämpliga delar uppfylla följande krav som tolkas i förhållande till den säkerhetsklass som bedöms:

Traficom måste få information om produktutvecklingen av krypteringsprodukten och Traficom måste ha möjlighet att ta ställning och påverka produktutvecklingen. Traficom strävar efter att granska produktutvecklingen av även andra produkter än krypteringsprodukter och vid behov producera information om dem som en del av utlåtandet eller beslutet.

- Traficom ska ha tillgång till produktens alla väsentliga källkoder i Traficoms lokaler eller, om så avtalas separat, i ett annat utrymme som rimligen kan ordnas och som uppfyller säkerhetskraven.
- Kraven gäller den tekniska helheten inklusive utrustningsplattformen och Traficom måste få den tekniska helheten för granskning samt tillräckliga uppgifter om plattformen.
- Arbetet med att utveckla produkten, de immateriella rättigheterna och underhållet av produkten ska under hela livscykeln vara i tillverkarens eller den betrodda underleverantörens juridiska, ekonomiska och faktiska besittning.
- Allmänt tillgängliga komponenter med öppen källkod och andra allmänt tillgängliga allmänna komponenter kan användas även om de inte hör till tillverkarens eller den betrodda underleverantörens egen produktion.

[4] Anvisning om hantering av säkerhetsklassificerat informationsmaterial (på finska) - Utrikesministeriet

5.2 Tillverkarens förutsättningar och kundmyndighetens krav på olika tillitsnivåer

5.2.1 Sammanfattning

I detta kapitel beskrivs alla villkor för bedömningar som ska uppfyllas för att produktbedömningen ska kunna inledas.

Tillverkningens och leveranskedjans ursprungsländer är förknippade med krav som beror på produktens användningsändamål samt säkerhetsklassen för den information som ska skyddas och den som informationen härrör från (*originator*, till exempel EU eller Nato).

Riskerna i anslutning till tillverkningens ursprung bedöms alltid. Kraven på riskhantering beror på säkerhetsklassen och den som informationen ursprungligen härrör från. Hur djupgående bedömningen av hanteringsmetodernas utfall är beror å sin sida på bedömningens tillitsnivå. Vid bedömningar av hög tillitsnivå utreder Traficom detta i behövlig omfattning. Vid bedömningar av lägre tillitsnivåer kan det från fall till fall vara kundmyndighetens ansvar att utreda tillverkningens ursprungsland och bedöma dess betydelse.

Traficoms bedömning förutsätter också alltid information om någon kundmyndighets behov av produkten för att skydda säkerhetsklassificerad information och förordande av bedömningen.

Även kraven på tillverkningsmiljöns säkerhet beror på säkerhetsklassen, och tillförlitligheten hos bedömningen av om kraven uppfylls beror på bedömningens tillitsnivå.

5.2.2 Tillverkarens förutsättningar

I detta kapitel behandlas förutsättningarna för bedömningar på hög tillitsnivå. Detta kan förutsättas till exempel i en situation där målet är att få en krypteringsprodukt till EU:s eller Natos offentliga lista över godkända produkter för skydd av säkerhetsklassificerad information.

Det finns inga uttryckliga bestämmelser om bedömningen av krypteringslösningar eller andra säkerhetskritiska produkter för nationellt säkerhetsklassificerad information eller om kraven på tillverkare eller tillverkning. Enligt förordningen om säkerhetsklassificering ska lösningarna vara *tillräckligt* tillförlitliga. Principen för Traficoms tillämpningspraxis är att ge offentliga utlåtanden endast om produkter vars tillverkning och livscykelhantering Traficom själv kan säkerställa i tillräcklig grad.

En förutsättning för bedömning av produkten är att Traficom kan utreda riskerna för andra staters påverkan i anslutning till tillverkningen av produkten (FOCI, Foreign Ownership and Control Influence). Utredningens omfattning påverkas av produktbedömningens omfattning och säkerhetsklassen för den information som ska skyddas. Dessutom påverkas utredningen av om det är fråga om bedömning av en produkt för skydd av nationellt säkerhetsklassificerad information eller en internationell förpliktelse som gäller informationssäkerhet.

En förutsättning för en hög tillitsnivå för skydd av nationellt säkerhetsklassificerad information är att produkten tillverkas av ett finländskt företag som bedriver verksamhet i Finland. Förutsättningen är att tillverkningen och produktutvecklingen till väsentliga delar sker i Finland. Detta kan påverkas av tillverkarens ägarunderlag och beslutanderätt och ursprunget av leverantörer av väsentliga produktspecifika säkerhetskomponenter (väsentliga underleverantörer).

Omständigheter som gäller tillverkaren och väsentliga underleverantörer kan vid behov påvisas till exempel med ett intyg över säkerhetsutredning av företag eller, om ett sådant inte finns att tillgå, med någon annan tillförlitlig utredning som Traficom enligt sin bedömning kan godkänna. När Traficom ingår ett avtal med ett företag om produktbedömning, bedöms utredningen innan avtalet ingås och fogas till avtalet. Tillverkaren förbinder sig att utan dröjsmål meddela Traficom om ändringar i utredningens innehåll.

Traficom bedömer om utredningen är tillräcklig från fall till fall med beaktande av Finlands sedvanliga förtroendereferensramar till exempel med de nordiska länderna, EU eller Natos medlemsstater. Utredningen bedöms i förhållande till säkerhetsklassen.

Myndigheten kan också begära bedömning eller godkännande från fall till fall för en produkt med utländskt ursprung. För att skydda nationellt säkerhetsklassificerad information måste Traficom och kundmyndigheten komma överens om hur risken för utländsk påverkan ska bedömas. Riskbeslutet hör till kundmyndighetens ansvar. Vid bedömningen av uppfyllandet av internationella förpliktelser som gäller informationssäkerhet bedömer Traficom ärendet och konstaterar det i beslutet om godkännande eller som en del av utlåtandet om godkännande av informationssystemet. Traficom kan också utreda hur man ska beakta ett eventuellt godkännande som utfärdats i en annan stat inom ramen för EU:s eller Natos säkerhetsbestämmelser samt tillgängliga uppgifter om produkten.

En förutsättning för bedömningen av en internationell förpliktelse som gäller informationssäkerhet är att riskerna för andra staters påverkan ska bedömas i enlighet med EU:s eller Natos säkerhetsbestämmelser. Tillverkaren och kundmyndigheten ska vara medvetna om att om det uppstår ett behov av att få Traficoms godkännande för användning av en produkt för skydd av säkerhetsklassificerad information från EU eller Nato, kan tillverkningens beroende av olika stater eller Traficoms kontrollmöjligheter påverka förutsättningarna för godkännande.

5.2.3 Myndigheters behov av bedömning av produkten

Enligt bedömningslagen och ämbetsverkslagen är det Traficoms uppgift att göra bedömningar på myndigheters begäran och främja säkerheten i informationssystemen och datakommunikationen.

Bedömning förutsätter således att det finns ett myndighetsbehov av bedömning av produkten. Om den som ansöker om / begär bedömningen är en myndighet, utreds behovet i begäran/ansökan. Om den som begär bedömningen är tillverkaren, ska en skriftlig utredning om en eller flera myndigheters behov av produkten vid upphandlingar i anslutning till deras informationssystem lämnas till Traficom. Syftet är att utreda att produkten har möjligheter att svara på myndigheternas kända behov, men inget egentligt upphandlingsavtal förutsätts.

Säkerställandet av myndighetens behov kan också ha ett samband med de avgifter som Traficom tar ut för bedömningen. Vid planeringen av bedömningen är det viktigt att tydligt på förhand fastställa om tillverkaren eller myndigheten ansvarar för avgifterna.

5.2.4 Bedömning av tillverkningsmiljön

Produkttillverkningsmiljön och tillverkningen av köpta komponenter påverkar produktens tillförlitlighet. Tillverkningsmiljöns ändamålsenlighet kan säkerställas genom olika förfaranden, till exempel följande:

- Tillverkarens självbedömning, varvid Traficom i allmänhet förutsätter att Katakri-kriterierna används,
- säkerhetsavtal mellan kundmyndigheten och tillverkaren
- Traficoms syn eller inspektion
- intyg över säkerhetsutredning av företag som omfattar verksamhetsmiljön.

Traficom fastställer ändamålsenliga förfaranden från fall till fall.

5.2.5 Allmänna råd till myndigheter

Vid valet av krypteringsprodukter eller andra säkerhetskritiska produkter som behövs för myndighetens informationssystem och datakommunikationsarrangemang ska åtminstone följande omständigheter övervägas:

- Skyddas nationellt säkerhetsklassificerad information med produkten eller information enligt någon internationell förpliktelse som gäller informationssäkerhet?
- Är någon produkt som Traficom redan tidigare har bedömt och som finns i förteckningen på Traficoms webbplats lämplig för behovet?[5] Då är det nödvändigt att utreda det exakta innehållet i bedömningen, eventuella begränsningar och innehållet i användningspolicyn.
- Det är bra att komma ihåg att informationshanteringsenheten, dvs. myndigheten, ansvarar för riskbedömningen och beslutet om ibruktagande av produkten och att Traficoms eventuella utlåtande är avsett som stöd för informationshanteringsenhetens egen riskbedömning och eventuella beslut om ibruktagande.
- Vid elektronisk behandling av säkerhetsklassificerad information inom EU och Nato förutsätter skyddet av information med en krypteringslösning Traficoms godkännande (*approval*), dvs. ett godkännandebeslut för produkten eller ett systemspecifikt godkännande som en del av ackrediteringen av informationssystem (*accreditation*). Även då fattas det egentliga beslutet om användningen av produkten i informationssystemet av den myndighet som ansvarar för systemet.
- Vid ett ömsesidigt behov av att skydda elektronisk dataöverföring som grundar sig på bilaterala avtal mellan stater kan en produkt som godkänts av någondera parten eller en produkt som godkänts gemensamt inom ramen för EU eller Nato komma i fråga.
- Lämpar sig någon produkt som finns på EU:s eller Natos offentliga produktlista för behovet?[6] Då är det nödvändigt att utreda innehållet i och den eventuella avgränsningen av föremålet för godkännandet samt om det finns närmare information om godkännandet. Traficom stöder i mån av möjlighet erhållandet av andra länders godkännandebeslut och användningspolicyer (SecOps) till Finlands myndighets förfogande. Det är

[5] https://www.kyberturvallisuuskeskus.fi/sv/var-verksamhet/ncsa/krypteringslosningar-som-godkanns-av-transport-och-kommunikationsverket
https://www.kyberturvallisuuskeskus.fi/sv/var-verksamhet/ncsa/sakerhetskritiska-produkter-godkanda-av-ncsa-verksamheten-vid-transport-och

[6] EU:s LAPC, allmänt: https://www.consilium.europa.eu/en/general-secretariat/corporate-policies/classified-information/information-assurance/ och List of Approved Cryptographic Products https://www.consilium.europa.eu/media/x0ebv5jn/st09931en24.pdf
Natos NIAPC, Nato Information Assurance Product Catalogue: https://www.ia.nato.int/NIAPC

bra att observera att EU:s och Natos säkerhetsklassificerade uppgifter ska skyddas från en annan organisation liksom från andra utomstående aktörer och tredje parter, vilket särskilt påverkar krypteringslösningarna.

6. Bedömningskrav och kriterier

6.1 Nationella krav på myndigheter: informationshanteringslagen och förordningen om säkerhetsklassificering

Myndigheternas behov av bedömning av produkter grundar sig på myndigheternas skyldigheter att skydda elektronisk behandling av säkerhetsklassificerad information. Bestämmelser om skyldigheterna finns i 13 § och 14 § i lagen om informationshantering inom den offentliga förvaltningen (906/2019, informationshanteringslagen) och i statsrådets förordning om säkerhetsklassificering av handlingar inom statsförvaltningen (1101/2019, förordningen om säkerhetsklassificering). I dessa författningar ställs krav på skydd av information och krypteringsprodukter som används för elektroniskt skydd av information. Bedömningsskyldigheten föreskrivs inte.

Informationshanteringslagen *13 § Informationssäkerhet i fråga om informationsmaterial och informationssystem*

En informationshanteringsenhet ska följa upp informationssäkerhetens tillstånd i sin verksamhetsmiljö och säkerställa informationsmaterialens och informationssystemens informationssäkerhet under hela deras livscykel. Informationshanteringsenheten ska identifiera relevanta risker som är förenade med informationsbehandlingen och dimensionera informationssäkerhetsåtgärderna utifrån riskbedömningen.

De med tanke på skötseln av en myndighets uppgifter relevanta informationssystemens feltolerans och funktionella användbarhet ska regelbundet säkerställas genom tillräcklig testning.

Myndigheten ska planera informationssystemen, informationslagrens strukturer och informationsbehandlingen i samband med dem på ett sådant sätt att handlingsoffentligheten utan svårighet kan genomföras.

Myndigheten ska vid sina upphandlingar säkerställa att de aktuella informationssystemen har lämpliga säkerhetsåtgärder.

Angående bedömning av informationssäkerheten i myndigheters informationssystem och datakommunikation föreskrivs särskilt.

Informationshanteringslagen *14 § Informationsöverföring i datanät*

Om en myndighet överför sekretessbelagd information i det allmänna datanätet ska informationen överföras i ett krypterat eller på annat sätt skyddat format. Dessutom ska överföringen ordnas så att mottagaren verifieras eller identifieras på ett tillräckligt informationssäkert sätt, innan mottagaren kommer åt att behandla den överförda sekretessbelagda informationen.

[…]

Informationshanteringslagen *15 § Tryggande av säkerheten i fråga om informationsmaterial*

…

Förordningen om säkerhetsklassificering *11 § Krav som gäller informationssystem och datakommunikationsarrangemang*

Informationssystem och datakommunikationsarrangemang som används för behandling av säkerhetsklassificerade handlingar ska genomföras så att

1) de med beaktande av säkerhetsklassen för de handlingar som behandlas i dem avskiljs på ett tillräckligt tillförlitligt sätt från informationssystem eller datakommunikationsarrangemang på lägre säkerhetsnivå,

[…]

7) de krypteringslösningar som används är tillräckligt säkra med beaktande av säkerhetsklassen för de handlingar som behandlats i informationssystemen eller datakommunikationsarrangemangen.

[…]

Förordningen om säkerhetsklassificering *12 § Överföring av en handling via datanätet*

Bestämmelser om överföring av sekretessbelagd information i det allmänna datanätet finns i 14 § i informationshanteringslagen.

Säkerhetsklassificerade handlingar får överföras från en myndighets skyddade säkerhetsområde i andra datanät än det allmänna datanätet eller överföras via informationssystem eller datakommunikationsarrangemang som har en lägre säkerhetsnivå än säkerhetsklassen i fråga endast om handlingarna krypterats. Om säkerhetsklassificerade handlingar överförs inom ett säkerhetsområde i andra datanät än det allmänna datanätet och uppgifterna kan skyddas tillräckligt med hjälp av metoder för fysiskt skydd, får okrypterad överföring eller kryptering på lägre säkerhetsnivå användas.

Förordningen om säkerhetsklassificering *13 § Transport av en handling*

Säkerhetsklassificerade handlingar får transporteras från säkerhetsområden om de elektroniska datamedierna skyddas med tillräcklig kryptering.

[…]

Förordningen om säkerhetsklassificering *15 § Förstöring av en handling*

En säkerhetsklassificerad handling som inte längre behövs ska förstöras på ett sådant sätt att det för säkerhetsklassen i fråga tillräckligt tillförlitligt går att förhindra att informationen helt och hållet eller delvis återställs eller sammanställs på nytt.

[…]

6.2 Kriterier för skydd av nationellt säkerhetsklassificerad information

I detta kapitel beskrivs hur Traficom definierar de kriterier som används vid bedömningen av en produkt.

Traficom har publicerat en del av de kriterier som tillämpas i bedömningen. Dessutom tillämpar Traficom sina sekretessbelagda eller säkerhetsklassificerade kriterier. Kriterierna hänför sig till säkerhetsklasser, typiska risker i behandlings- eller förvaringsmiljön och i dem följer man upp väsentliga internationella kriterier som allmänt konstaterats vara goda. Principen i bedömningen är att ju allvarligare risker man kan se, desto strängare säkerhetsmekanismer behövs. Nedan listas de viktigaste offentliga kriterierna som tillämpas i bedömningen:

Kryptografiska anvisningar

- *Kryptografiska krav på konfidentialiteten - nationella skyddsnivåer* (anvisning 190/651/2015, 9.12.2024, på finska)[7]
- *Godkända TLS-cipher suites för säkerhetsklasserna IV–III* (promemoria i diabilder 13.10.2022, på finska)[8]

[7] *Kryptografiset_vahvuusvaatimukset_-_kansalliset_turvallisuusluokat_1.pdf*
[8] *TLS cipher suitet suojaustasoille IV-III*

Vid bedömningen av krypteringsanordningar och säkerhetskritiska produkter tillämpas i tekniskt tillämpliga delar Katakri

- *Katakri – verktyg för informationssäkerhetsauditering för myndigheter* (nationella säkerhetsmyndighetens anvisning)[9]

För vissa typer av säkerhetskritiska produkter har Traficom publicerat anvisningar som också tillämpas i Traficoms bedömningar

- *Tömning och återanvändning av lagringsutrustning* (28.6.2024, på finska)[10]
- *Guide om planeringsprinciper och lösningsmodeller för gatewaylösningar* (2.12.2021, på finska)[11]

Anvisning om säker produktutveckling och bedömning av säkerhetskritiska produkter som tillämpas på flera produkter och bedömningar av dem

- *Säker produktutveckling: Motmed sikte på godkännande* (anvisning 2018, på finska)[12]

Man har strävat efter att definiera kriterierna för bedömningen av skyddet av nationellt säkerhetsklassificerad information så enhetligt som möjligt med internationell praxis.

Målet är att resultaten av bedömningen av en produkt för att skydda nationellt säkerhetsklassificerad information ska kunna utnyttjas och användas som underlag, om kundmyndigheten eller tillverkaren ansöker om godkännande av samma produkt för skydd av EU:s eller Natos säkerhetsklassificerade information. I praktiken kan bedömningen av skyddet av nationellt säkerhetsklassificerad information och en internationell förpliktelse som gäller informationssäkerhet också genomföras parallellt.

6.3 Internationella krav på informationssäkerhet

6.3.1 Bilaterala informationssäkerhetsavtal

I staternas bilaterala informationssäkerhetsavtal är huvudregeln ömsesidighetsprincipen, varvid säkerhetsklassificerad information från en annan stat skyddas på samma sätt som nationell information i motsvarande säkerhetsklass. De behöriga myndigheterna i medlemsstaterna, i Finland Traficom, avtalar sinsemellan om de krypteringslösningar som används vid dataöverföring mellan stater. Krypteringslösningarna kan vara förknippade med avtals- eller projektspecifika krav.

Exempel på avtalsbestämmelser

Överenskommelsen mellan Republiken Finland och Konungariket Belgien om ömsesidigt skydd av säkerhetsklassificerad information (FördrS 8 och 9/2022)[13].

Artikel 5 Skydd av säkerhetsklassificerad information
1. Parterna ska vidta alla relevanta åtgärder i enlighet med sina nationella lagar och bestämmelser för att skydda säkerhetsklassificerad information som avses i denna

[9] https://um.fi/katakri-verktyg-for-informationssakerhetsauditering-for-myndigheter
[10] https://www.kyberturvallisuuskeskus.fi/sites/default/files/media/file/Tallennusv%C3%A4lineiden%20tyhjennys%20ja%20uusiok%C3%A4ytt%C3%B6.PDF
[11] https://www.kyberturvallisuuskeskus.fi/sites/default/files/media/file/Yhdyskaytavaratkaisuohje.pdf
[12] https://www.kyberturvallisuuskeskus.fi/sites/default/files/media/publication/Turvallinen_tuotekehitys_Suomi_J003_2018.pdf
[13] https://www.finlex.fi/sv/sopimukset/sopsteksti/2022/20220009/20220009_2

överenskommelse. De ska skydda denna information på samma nivå som egen information i motsvarande säkerhetsklass.
[…]

Artikel 7 Överföring av säkerhetsklassificerad information
[…]
2. Säkerhetsklassificerad information ska på elektronisk väg förmedlas mellan den utlämnande och den mottagande parten endast på ett sådant säkert sätt som de behöriga säkerhetsmyndigheterna sinsemellan har kommit överens om.

6.3.2 EU och Nato

I de principer (policy) och riktlinjer (guidelines) som utfärdats med stöd av artikel 6 i EU:s säkerhetsbestämmelse EU/488/2013 och i de direktiv och anvisningar som ingår i Natos säkerhetsbestämmelser preciseras kraven på krypteringslösningar och andra säkerhetskritiska produkter och bedömningen av dem på olika sätt. Handlingarna är i regel sekretessbelagda eller säkerhetsklassificerade. Utlämnande av uppgifter om dessa behandlas i kapitel 4.2 i anvisningen.

Utöver EU:s eller Natos ovan nämnda handlingar kan Traficom vid behov komplettera de kriterier som fastställts för skydd av nationell information.

6.4 Sammanställning av de krav som används i bedömningarna

De krav som används i bedömningarna åskådliggörs i tabell 1.

Tabell 1. Krav som används i bedömningarna.

Krav på produkten och dess livscykel	Exempel
Offentliga krav på produktens tekniska egenskaper	Kryptografisk styrka Säkerhetsfunktionerna i gatewaylösningen
Sekretessbelagda krav på produktens tekniska egenskaper	Mer detaljerade tekniska krav Krav som grundar sig på produktspecifik hotmodellering
Krav på tillverkning och utveckling av produkten	Skydd av åtkomstkontroll och integritet i produktutvecklingsmiljön Kontroll av tillverkningen
Hantering av risker i anslutning till tillverkningen av produkten och leveranskedjorna under påverkan av andra stater (FOCI, Foreign Ownership and Control Influence)	Begränsningar i behandlingen av uppgifter om vissa säkerhetsklasser och/eller myndigheter som lämnar ut uppgifter (originator)
Kundmyndighetens behov och förordande	Myndighetens uttryckta behov av att använda produkten i fråga samt förordande av produktbedömningen

7. Bedömningsförfaranden och bedömningens tillitsnivåer

7.1 Bedömningarnas innehåll

Bedömningens innehåll beror på säkerhetsklassen så att produkter avsedda för skydd av uppgifter i högre säkerhetsklasser samt produkter för skydd under informationens hela livscykel omfattas av mer omfattande och strängare krav och en högre hotmiljö. Även produktens struktur och bedömningen av hotbilden påverkar testningens innehåll.

Säkerhetsklassens inverkan på bedömningens innehåll i ett fall där en produkt bedöms med hög tillitsnivå åskådliggörs på hög nivå i tabell 2. De detaljerade bedömningsmetoder som används väljs dock från fall till fall när bedömningsarbetet planeras.

Tabell 2. Säkerhetsklassens inverkan på minimiinnehållet i en bedömning av hög tillitsnivå.

Bedömningsförfarande	SK II	SK III	SK IV
Granskning av allmän och teknisk dokumentation	X	X	X
Granskning av inställningar och livscykelhantering	X	X	X
Detaljerad granskning av allmän och teknisk dokumentation	X	X	
Begränsad granskning av källkoden (krypteringskod)	X	X	X
Granskning av delar som påverkar källkodens säkerhet	X	X	
Helhetsgranskning av källkoden	X		
Begränsad testning av lösningen	X	X	X
Normal testning av lösningen	X	X	
Omfattande testning av lösningen	X		
Kontroll av utvecklingsprocessen av CAA	X	X	

Testningsnivåerna bestämmer de vanligaste bedömningsmetoderna. Bedömningens omfattning påverkas också av användningsfallet, hotmiljön och produktens struktur.

Syftet med **den begränsade testningen** är att förstå produktens funktion och inställningar för att kunna bedöma eventuella risker och verifiera centrala faktorer i anslutning till säker användning. Målet är att testa att produkten inte har några uppenbara problem vid normal användning.

Vid begränsad testning bedöms produktens korrekta funktion genom ytlig testning via användargränssnittet och externa gränssnitt samt uppföljning av funktionen. Dessutom säkerställer man att det inte finns kända och lättillgängliga svagheter i produktens interna eller externa gränssnitt och säkerhetskontroller.

Syftet med **den normala testningen** är att utöver den begränsade testningen säkerställa säkerheten i produktens interna genomförande. Vid testningen säkerställs inställningarna och funktionerna på en noggrannare nivå än vad som syns till exempel för anordningens administratörer, till exempel härdningarna av operativsystemet. Produkten genomgår en kartläggning av riskerna för avancerade angrepp och vid testningen kontrolleras också hur produkten reagerar på avancerade angrepp. Testningen kan omfatta separat testning av enskilda kritiska komponenter.

Syftet med **den omfattande testningen** är att bedöma produktens tekniska funktion på djupet. Enskilda komponenter testas som enskilda delar. I testningen genomförs en omfattande testning av enskilda komponenter utan komponenternas skyddsmekanismer. Som testmetoder används också särskilt avancerade angrepp.

7.2 Bedömningens tillitsnivåer

Ju mer omfattande man gör bedömningen av uppfyllandet av kraven, som utvidgas och skärps enligt säkerhetsklass, desto större säkerhet kan man få om produktens funktion och tillförlitlighet. Detta beskrivs med begreppet tillitsnivå. Tillitsnivån uttrycker inte produktens överensstämmelse med kraven, utan uttryckligen tillförlitligheten i bedömningen av huruvida kraven på produkten uppfylls.

Bedömningens tillitsnivåer åskådliggörs i tabell 3. Produktbedömningens höga tillitsnivå (A) är utgångspunkten för bedömningsarbetet. Det är också en förutsättning för internationella produktgodkännanden och offentliga utlåtanden om nationella produkter. Bedömningar på lägre tillitsnivå är avsedda som stöd för myndighetens riskbedömning och beslutsfattande. De görs utifrån myndigheternas behov när det i användningsfallet inte finns eller annars är möjligt att utnyttja en produkt som bedömts på hög nivå.

Tabell 3. Bedömningens tillitsnivåer.

Tillitsnivå	Bedömningens djup (tillförlitlighet)
Låg (C)	Låg
Medelnivå (B)	Normal
Hög (A)	Djupgående

Bedömningar på olika tillitsnivåer förutsätter olika uppgifter och material av produktens tillverkare. Vid bedömningar på C-nivå bedöms produkten i huvudsak utifrån dokumentationen i anslutning till den. Vid bedömningar på B-nivå ska ett fungerande exemplar av produkten levereras för bedömning. För bedömningar på A-nivå ska de mest omfattande uppgifterna och materialet om produkten, inklusive källkoden, lämnas in.

7.3 Val av bedömningsförfaranden

Traficom fastställer och väljer de förfaranden som ska användas vid bedömningen i enlighet med kraven på produkten enligt säkerhetsklass, bedömningen av

hotbilden och den eftersträvade tillitsnivån. De förfaranden som används vid produktbedömningen avtalas i bedömningens planeringsskede.

7.4 Tillitsnivåns inverkan på utlåtandets eller beslutets offentlighet

Utgångspunkten är att produktbedömningarna görs på en hög tillitsnivå. Då är utlåtandet offentligt, om myndighetens behov inte förutsätter att det hålls hemligt. Utlåtanden om bedömningar av lägre tillitsnivåer är i allmänhet sekretessbelagda.

Traficom beslutar från fall till fall om utlåtandet eller beslutet är offentligt. Vid bedömningen av offentligheten beaktas kundmyndighetens och tillverkarens motiverade behov.

Detta förfarande beror på att man inte vill att produktanvändarna ska missta sig om innehållet i bedömningen när de gör val för sina system. Oberoende av begränsningarna kan Traficoms offentliga bedömning lätt misstas som allmängiltig och konsekvenserna av bedömningens begränsningar förbises av en myndighetsanvändare. Traficom ger alltså ett offentligt utlåtande om att kraven uppfylls endast i sådana situationer där Traficom har tillräckliga uppgifter om tillverkningen och det tekniska genomförandet av produkten samt möjlighet att få tillgång till resurser och information som är väsentliga för granskningen och bedömningen.

Detta i kombination med behovet av att kontrollera tillverkningen innebär att man i regel endast kan göra bedömningar av höga tillitsnivåer för utländska produkter med säkerhetsklasserna IV/NR/EU-R.

7.5 Tillgodoräknande av andra godkännanden eller certifikat

Traficom kan efter eget övervägande som en del av utredningen i anslutning till bedömningen beakta en bedömning som en myndighet eller certifieringsorganisation i en annan stat gjort på produkten. Utnyttjandet av bedömningen beror på för vilket ändamål och på vilka grunder bedömningen har gjorts och vilka uppgifter som finns tillgängliga om dess innehåll.

Bedömningarna av produkter för skydd av säkerhetsklassificerad information är alltid förknippade med skydd av nationellt säkerhetsklassificerad information eller uppfyllande av internationella förpliktelser som gäller informationssäkerhet. Dessa skyldigheter är inte förknippade med föreskrivna skyldigheter om ömsesidigt erkännande eller tillgodoräknande av bedömningar (med undantag av bilaterala internationella informationssäkerhetsavtal), så Traficom överväger från fall till fall hur andra bedömningar kan utnyttjas i dess egen bedömning.

8. Bedömningsprocessen

I detta kapitel beskrivs de centrala skedena i bedömningsprocessen. Bedömningsprocessen åskådliggörs i bilaga 1.

8.1 Traficoms, kundmyndighetens och tillverkarens trepartsbedömning

Bedömningen av produkten inleds vid Traficom på en kundmyndighets eller tillverkares begäran. Det här beskrivs i följande kapitel. Oavsett på vems begäran bedömningsprocessen formellt inleds är det i allmänhet viktigt att utreda bedömningsprocessens mål och huvuddrag mellan alla parter.

Alla parter ska ha samma uppfattning om på vilken tillitsnivå det är möjligt att göra bedömningen och om det är meningen eller möjligt att det uppstår offentlig information om resultatet av bedömningen eller myndighetsspecifik information för ett visst system. Själva tekniska bedömningsprocessen består i allmänhet i huvudsak av dialog och åtgärder mellan Traficom och tillverkaren, men det är bra att identifiera behoven av rapportering och informationsutbyte mellan alla parter. Det är också viktigt att skapa en gemensam uppfattning om avgifterna i anslutning till bedömningen.

8.2 Begäran om bedömning eller godkännande

För att produkten ska kunna bedömas vid Traficom måste en myndighet eller en tillverkare göra en begäran om bedömning.

Det är bra att kontakta Traficom redan i produktplaneringsskedet så att Traficom kan ge råd i ärendet, beakta olika behov i prioriteringen, planera resursfördelningen för bedömningarna och vid behov delta i produktutvecklingen från början (se ovan, gäller säkerhetsklasserna II och III).

En bedömning som görs på tillverkarens begäran förutsätter ett avtal mellan Traficom och tillverkaren om produktbedömning och en utredning av myndighetens behov.

En myndighet kan med stöd av bedömningslagen begära bedömning av ett informationssystem, och bedömningen kan också gälla en del av informationssystemet. Myndigheten kan begära en bedömning av en produkt för skydd av nationellt säkerhetsklassificerad information eller godkännande för skydd av EU:s eller Natos säkerhetsklassificerade information. Begäran kan gälla bedömning av en produkt så att resultatet av bedömningen kan publiceras som allmängiltig (med beaktande av villkoren för tillverkningens ursprung) eller så att produkten bedöms eller godkänns endast från fall till fall i myndighetens informationssystem.

Vid behov bedömer Traficom alltså produkten **som en del av myndighetens systemhelhet.** På myndighetens begäran kan man också bedöma en krypteringslösning eller produkt vars anskaffning endast planeras.

Myndigheten kan också begära bedömning eller godkännande från fall till fall för en produkt med utländskt ursprung. För att skydda nationellt säkerhetsklassificerad information måste Traficom och kundmyndigheten komma överens om hur risken för utländsk påverkan ska bedömas. Riskbeslutet hör till kundmyndighetens ansvar. Vid bedömningen av uppfyllandet av internationella förpliktelser som gäller informationssäkerhet bedömer Traficom ärendet och konstaterar det i beslutet om godkännande eller som en del av utlåtandet om godkännande av informationssystemet. Traficom kan också utreda hur man ska beakta ett eventuellt godkännande som utfärdats i en annan stat inom ramen för EU:s eller Natos säkerhetsbestämmelser samt tillgängliga uppgifter om produkten.

Av begäran om bedömning ska framgå hurdan produkt det är fråga om, i vilket skede produktens utveckling är (under planering, beredning, produktion) och vilken säkerhetsklass som eftersträvas för produkten.

Traficom kan begära komplettering för att utreda förutsättningarna för bedömningen. Vid behov underrättar Traficom både tillverkaren och kundmyndigheten skriftligen om bedömningsprocessens karaktär och huvuddrag (t.ex. tillitsnivå och om resultatet kan vara offentligt). Traficom meddelar också om produkten inte kan bedömas och ger motiveringar till detta.

Den som begär bedömningen förutsätts lämna tillräckliga uppgifter för utarbetandet av bedömningsplanen, utse minst en lämplig teknisk kontaktperson för att svara på de frågor som framkommer i bedömningen och förbinda sig till bedömningsprojektets tidtabell. Beställaren förutsätts också för egen del möjliggöra de resurser som behövs för bedömningsprojektet, i vilka vanligtvis ingår leverans av den produkt som testas och den begärda dokumentationen, utbildning i anslutning till produkten samt lämpliga personal- och lokalbokningar.

En begäran om utlåtande som inkommit till Traficom från ett godkänt bedömningsorgan för informationssäkerhet inom bedömningsorganets uppdrag behandlas i anvisningen om bedömningsorgan.

8.3 EU- och Natogodkännanden

8.3.1 Godkännande av krypteringsprodukter för skydd av EU-information

Traficom är behörig att godkänna krypteringsprodukter för behandling av EU:s säkerhetsklassificerade information i nationella system i säkerhetsklasserna EU-R och EU-C. I de högre säkerhetsklasserna förutsätts dessutom alltid att ett s.k. AQUA[14]-land gör en andra bedömning (SPE, Second Party Evaluation) och rådets godkännande.

För att föra in krypteringsprodukter på EU:s lista över godkända krypteringsprodukter (LACP[15]) krävs alltid AQUA-landets SPE-bedömning med avseende på alla säkerhetsklasser utöver den nationella CAA-myndighetens bedömning och godkännande.

I tabell 5 beskrivs Traficoms (CAA-verksamhetens) behörighet i EU-krypteringsproduktgodkännanden.

Tabell 4. Behörighet vid godkännande av EU-krypteringsprodukter.

EU-säkerhetsklass (FördrS 77/2015 artikel 2)	**motsvarande nationell säkerhetsklass** (FördrS 77/2015 bilaga)	**Traficoms CAA-uppgift vid godkännande av krypteringsprodukter** EU/488/2013 EU-rådets säkerhetsbestämmelse, artikel 10.6
TRES SECRET UE / EU TOP SECRET (TS-UE/EU-TS)	ERITTÄIN SALAINEN YTTERST HEMLIG (SK I)	• **godkännandebehörighet hos rådet** på rekommendation av säkerhetskommittén • godkännandet grundar sig på AQUA-landets andra bedömning (SPE, Second Party Evaluation) och rekommendation • nationell CAA gör den första bedömningen (FPE, First Party Evaluation)
SECRET UE / EU SECRET (S-UE/EU-S)	SALAINEN HEMLIG (SK II)	• **godkännandebehörighet hos rådet** på rekommendation av säkerhetskommittén • godkännandet grundar sig på AQUA-landets andra bedömning (SPE, Second Party Evaluation) och rekommendation • nationell CAA gör den första bedömningen (FPE, First Party Evaluation)

[14] AQUA = Approriately Qualified Authority
[15] LACP = List of Approved Cryptographic Products

CONFIDENTIEL UE / EU CONFIDENTIAL (C-UE/EU-C)	LUOTTAMUKSEL-LINEN KONFIDENTIELL (SK III)	• **nationell CAA kan godkänna krypteringslösningen i det nationella systemet** • i det nationella systemet kan man också använda en krypteringslösning som godkänts av rådet
RESTREINT UE / EU RESTRICTED (R-UE/EU-R)	KÄYTTÖ RAJOITETTU BEGRÄNSAD TILLGÅNG (SK IV)	• **nationell CAA kan godkänna krypteringslösningen i det nationella systemet** • i det nationella systemet kan man också använda en krypteringslösning som godkänts av rådet

8.3.2 Godkännande av krypteringsprodukter för godkännande av Natos säkerhetsklassificerade information

Traficom är behörig att godkänna krypteringsprodukter för behandling av Natos säkerhetsklassificerade information i säkerhetsklasserna NR (Nato Restricted) och NC (Nato Confidential). I de högre säkerhetsklasserna förutsätts alltid dessutom en annan bedömning av SECAN-byrån (SPE, Second Party Evaluation) och godkännande av Natos militärkommitté.

Ett företag kan ansöka om att lägga till sin krypteringsprodukt på NIAPC[16]-listan, men för att lägga till uppgifter om godkännande av produkten behövs stöd från den nationella NCSA-myndigheten. På NIAPC:s webbplats finns blanketter för att ansöka om inkludering i listan.

I tabell 6 beskrivs Traficoms (NCSA-verksamhetens) behörighet i Nato-krypteringsproduktgodkännanden.

Tabell 5. Behörighet vid godkännande av Nato-krypteringsprodukter.

Natos säkerhetsklass	**motsvarande nationell säkerhetsklass**	**Traficoms NCSA-uppgift vid godkännande av krypteringsprodukter** **C-M(2002)49-REV1 Bilaga F artikel 11**
COSMIC TOP SECRET (CTS)	ERITTÄIN SALAINEN YTTERST HEMLIG (SK I)	• **godkännandebehörighet hos militärkommittén (NAMILCOM)** • godkännandet grundar sig på en andra bedömning (SPE, Second Party Evaluation) av ett Nato-organ • nationell NCSA gör den första bedömningen (FPE, First Party Evaluation)
NATO SECRET (NS)	SALAINEN HEMLIG (SK II)	• **godkännandebehörighet hos militärkommittén (NAMILCOM)** • godkännandet grundar sig på en andra bedömning (SPE, Second Party Evaluation) av ett Nato-organ • nationell NCSA gör den första bedömningen (FPE, First Party Evaluation)
NATO CONFIDENTIAL (NC)	LUOTTAMUKSEL-LINEN KONFIDENTIELL (SK III)	• **nationell NCSA kan godkänna krypteringslösningen i det nationella systemet** • i det nationella systemet kan man också använda en krypteringslösning som godkänts av militärkommittén (NS eller CTS)

[16] NIAPC = Nato Information Assurance Product Catalogue

NATO RESTRICTED (NR)	KÄYTTÖ RAJOITETTU BEGRÄNSAD TILLGÅNG (SK IV)	• **nationell NCSA kan godkänna krypteringslösningen i det nationella systemet** • i det nationella systemet kan man också använda en krypteringslösning som godkänts av militärkommittén (NS eller CTS)

8.3.3 Security Enforcing Products i Natos säkerhetsbestämmelser

I flera av Natos säkerhetsbestämmelsehandlingar nämns säkerhetskritiska produkter, dvs. Security Enforcing Products (SEP-produkter). I bestämmelserna fastställs vissa kategorier av säkerhetskritiska produkter som alltid kräver NCSA-godkännande i nationella system. Som en del av systemkontrollen kan man kräva NCSA-godkännande även för produkter utanför dessa definierade produktkategorier.

Godkännandet kan ses som en tudelad process:

- godkännande av produktens lämplighet för behandling av Natos säkerhetsklassificerade information i det nationella systemet (NCSA:s produktgodkännande)
- godkännande av användning av en produkt som en del av ett visst system (som en del av SAA-verksamhetens godkännandeutlåtande).

För en del produkter fastställs särskilda krav i säkerhetsbestämmelserna. I övrigt tillämpas nationella krav som vid behov kompletteras med tillämpliga Natodokument. Utlämnande av uppgifter till tillverkaren behandlas i kapitel 4.2.

SEP-produkter kan också föras på NIAPC-listan. På NIAPC:s webbplats finns blanketter för att ansöka om inkludering i listan. Ett företag kan ansöka om att lägga till sin produkt på NIAPC-listan, men för att lägga till uppgifter om godkännande av produkten behövs stöd från den nationella NCSA-myndigheten.

8.4 Traficoms prioriteringsprinciper

Vid prioriteringen av begäran om bedömning av produkter följer Traficom samma principer som föreskrivs i bedömningslagen i som vid begäran om bedömning av informations- och datakommunikationssystem.

Bedömningslagen *4 § Kommunikationsverkets uppgifter*
3 mom. Kommunikationsverket utför de uppgifter som avses i denna lag inom ramen för de resurser som står till buds och med beaktande av uppfyllandet av internationella förpliktelser som gäller informationssäkerhet och de begärda åtgärdernas betydelse för en allmän förbättring av informationssäkerheten i myndigheternas informationssystem och datakommunikation.

Vid prioriteringen av bedömnings- och godkännandeuppgifterna beaktas alltså iakttagandet av internationella förpliktelser som gäller informationssäkerhet samt de begärda åtgärdernas betydelse för den allmänna förbättringen av informationssäkerheten i myndigheternas informationssystem och datakommunikation, dvs. myndighetens behov av produkten. För att en produkt ska kunna bedömas av Traficom ska det finnas ett myndighetsbehov av produkten och potential att svara på myndighetens behov.

En förutsättning för att produkter som särskilt är avsedda för skydd av nationellt säkerhetsklassificerad information ska kunna bedömas är att Traficom har tillräckliga personalresurser för detta.

Vid prioriteringen beaktas bedömningens omfattning och säkerhetsklassen för den information som skyddas med produkterna. I bedömnings- och godkännandeuppgifterna prioriteras produkter vars bedömning kan genomföras på en hög tillitsnivå. Lagen innehåller inga bestämmelser om ursprunget för tillverkningen av produkter, men i praktiken uppfylls förutsättningarna för bedömning med en hög tillitsnivå främst inom den inhemska tillverkningen, som omfattas av Finlands jurisdiktion. En begränsad bedömning är avsedd att genomföras endast i begränsade fall, såsom som en del av bedömningen av ett informationssystem. Prioriteringen påverkas i regel också av tillgången till motsvarande produkter. I begäran om bedömning ska man kontrollera om motsvarande produkter finns till exempel på Traficoms lista över godkända produkter eller om det finns behov av att bedöma en ny produkt.

I regleringen har man inte beaktat en situation där tillverkaren själv ansöker om EU- eller Natogodkännande för sin produkt. EU:s och Natos säkerhetsbestämmelser tar inte ställning till nationella förvaltningsprocesser. Traficom prioriterar i enlighet med bedömningslagen myndigheternas behov i anslutning till informationssystem och datakommunikation.

8.5 Förhandsmöte mellan tillverkaren och Traficom

Förhandsmötet hålls mellan tillverkaren och Traficoms bedömare. Vid behov kan även kundmyndigheten tas med så att man kan säkerställa produktens användningsbehov och så att bedömningsprocessen som helhet kan gås igenom mellan alla parter. Under förhandsmötet kommer man överens om praxis för bedömningsarbetet.

Under förhandsmötet diskuteras de uppgifter som kunden lämnat in på förhand, vilka i tillämpliga delar är bland annat:

- Funktionell beskrivning av produkten:
    - genomgång av produktlöftet, produktens prestanda och funktionalitet
    - genomgång av produktens övergripande arkitektur och de omgivande elementen samt hotmodellerna.
- Produktens kryptografi:
    - genomgång av produktens kryptografiska egenskaper och lösningar samt nyckelhantering.
- Bedömningens målnivå:
    - genomgång av den eftersträvade säkerhetsklassen och bedömningens tillitsnivå samt förutsättningarna för dessa i produktens planerade användningsändamål.
- Tidigare bedömningar och testningar:
    - genomgång av eventuella tidigare bedömningar och testningar.
- Säkerhetsfrågor i anslutning till företagssäkerhet och produktutveckling:
    - granskning av tillverkarens informationssäkerhetsarrangemang och beställarens/myndighetens eventuella behov av att ansöka om en säkerhetsutredning av företaget (tillverkaren).

Under förhandsmötet diskuterar man med tillverkaren och kundmyndigheten om man vill ge information om produkten eller dess pågående bedömning till andra myndigheter.

Den dokumentation som behövs för bedömningen beskrivs i bilaga 2. Innan bedömningsplanen utarbetas ska den dokumentation som krävs lämnas in till Traficom till tillräckliga delar. Det första förhandsmötet kan dock ordnas även om noggrann dokumentation om alla punkter inte har lämnats in. Om de uppgifter som krävs för bedömningsplaneringen inte kan lämnas in till förhandsmötet eller inom rimlig tid efter det, kan Traficom avbryta processen och använda de reserverade resurserna för andra bedömningar.

8.6 Uppskattad arbetsmängd

Traficom gör upp en uppskattning av arbetsmängden för varje produkt och produktversion, där man på en allmän nivå beskriver den tid som går åt till att bedöma produkten i fråga inom olika delområden samt arbetsmängden i sin helhet.

Tillverkaren och kundmyndigheten ges möjlighet att kommentera den uppskattade arbetsmängden. Uppskattningen uppdateras vid behov under bedömningens gång, om det sker väsentliga ändringar i den.

Syftet med den uppskattade arbetsmängden är att hjälpa till att förutse tidtabellen och den avgift som tas ut för bedömningen, vilket behandlas i följande kapitel.

8.7 Traficoms avgifter

Traficom tar ut en avgift för bedömningen enligt självkostnadsvärdet i enlighet med den gällande avgiftsförordningen (Kommunikationsministeriets förordning om avgifter som tas ut för Transport- och kommunikationsverkets prestationer som gäller elektronisk kommunikation)[17]. Avgiften grundar sig på den arbetsmängd och tid som använts för granskning, bedömning och beredning och meddelande av utlåtande eller godkännande.

Avgiften tas enligt förordningen också ut för väsentliga prestationer som hänför sig till behandlingen av ändringar eller avvikelser. Avgiften tas också ut för den tid som använts för en avbruten bedömning.

Betalningsskyldigheten gäller åtgärder som har vidtagits under giltighetstiden av tillverkarens avtal, även om avtalet har upphört.

Den som i sista hand ansvarar för betalningen är antingen tillverkaren, inom ramen för vars avtal begäran om bedömning behandlas, eller den myndighet, på vars begäran (på ansökan enligt bedömningslagen) bedömningen har anhängiggjorts och tagits upp till Traficoms behandling. Tillverkaren och kundmyndigheten kan dock sinsemellan komma överens om betalningsansvaret och vilka kontaktuppgifter för faktureringen som lämnas in till Traficom.

8.8 Bedömning

Syftet med produktbedömningen är att undersöka om produkten uppfyller de informationssäkerhetskrav som ställs på den och om produkten fungerar på det sätt som beskrivs.

När bedömningen framskrider rapporteras centrala observationer till tillverkaren och vid behov till kundmyndigheten. Utifrån dessa kan tillverkaren göra ändringar i produkten. Efter eventuella ändringar genomförs de test som behövs igen, och testningen av produkten fortsätter enligt planen. Ändringar och reparationer av

[17] https://finlex.fi/sv/laki/ajantasa/2018/20180935

produkter under bedömningen kan påverka både bedömningens tidtabell och kostnader.

Bedömningen kan inledas när kunden har lämnat in tillräcklig information om den produkt som ska bedömas under utvecklingsfasen.

8.9 Utlåtande eller beslut om godkännande och andra handlingar

När bedömningen har slutförts ger Traficom ett utlåtande eller ett beslut om godkännande

- Utlåtande om att kraven uppfylls vid skydd av uppgifter i säkerhetsklassen [SK IV–SK II]
- Utlåtande om partiellt uppfyllande av kraven [SK IV–SK II] vid skydd av uppgifter
- (Utlåtande om att kraven inte uppfylls eller enbart en bedömningsrapport av vilken detta framgår)
- Beslut om godkännande av en produkt för skydd av uppgifter [i EU:s eller Natos specificerade säkerhetsklass]
- Beslut om godkännande av en produkt (från fall till fall) för skydd av uppgifter [i EU:s eller Natos specificerade säkerhetsklass] [i myndighetens informationssystem X]
- (Vid behov beslut om att kraven inte uppfylls)

Traficoms utlåtande eller beslut om godkännande kan omfatta bland annat följande bilagor

- Bedömningsrapport
- Kryptologiskt utlåtande
- Användningspolicy (SecOps)

8.10 Produktens livscykelhantering

8.10.1 Tidsbegränsning av utlåtanden och godkännanden samt bedömning av ändringar

Traficoms utlåtande eller godkännandebeslut för en produkt som uppfyller kravet är alltid tidsbundet och gäller i regel i högst 3 år. Därefter kan bedömningens giltighetstid förlängas om produktens säkerhet fortfarande motsvarar de krav som ställs på den. Tidsfristen kan också vara kortare.

Tillverkaren ska aktivt upprätthålla produktens säkerhet. Kritiska programsårbarheter ska korrigeras så snabbt som möjligt och Traficom ska kontaktas i ärendet utan dröjsmål.

Utlåtandet eller godkännandet gäller i allmänhet endast en viss produktversion. Nya program- eller produktversioner kan således kräva bedömning. Om man vill ha ett utlåtande eller godkännande för den ändrade produkten ska man kontakta Traficom. Under bedömningsprocessen kan man dock komma överens med tillverkaren om vilka ändringar som kan göras i en produkt som godkänts utan separat kontakt.

Det ovan beskrivna upprätthållandet av ändringar gäller situationer där det för produkten har utarbetats ett utlåtande om uppfyllandet av kraven för skydd av nationellt säkerhetsklassificerad information och informationen om utlåtandet har

publicerats. Upprätthållandet gäller också situationer där Traficom har godkänt användningen av produkten för att skydda internationell säkerhetsklassificerad information och informationen har publicerats.

I situationer där Traficom har gett ett utlåtande till myndigheten om skydd av nationellt säkerhetsklassificerad information eller ett godkännande enligt en internationell förpliktelse som gäller informationssäkerhet för systemspecifik användning av en produkt som en del av ett informationssystem, ansvarar den ansvariga myndigheten för informationssystemet för uppföljningen av ändringar i produktens informationssäkerhet och t.ex. för installationen av uppdateringar.

Anmälan om tekniska ändringar kan i regel klassificeras på följande sätt:

1) Innan en planerad ändring genomförs ska den alltid anmälas till Traficom för bedömning och godkännande, om ändringen kan påverka produktens krypteringsegenskaper, användningssäkerhet, programvaruarkitektur eller andra faktorer som är centrala med tanke på produktens säkerhet.

   Beroende på ändringens omfattning undersöker och verifierar Traficom produktens säkerhetsegenskaper helt eller delvis.

2) Den planerade ändringen och dess detaljer ska anmälas till Traficom minst fyra veckor före den planerade tidpunkten för genomförandet av ändringen, när avsikten är att genomföra mindre ändringar i en godkänd produkt, till exempel konfigurationsändringar som inte har några säkerhetseffekter.

   Traficom bedömer ändringens karaktär och informerar produktens tillverkare om huruvida ändringen kan genomföras och distribueras utan separat bedömning eller om ändringen förutsätter en inspektion av Traficom innan den kan genomföras och distribueras.

   Efter ändringen ska produkten fortfarande till sina krypteringsegenskaper och centrala informationssäkerhetsegenskaper motsvara godkännandet och kunna användas i enlighet med användningspolicyn. Om programvarans faktiska funktionalitet inte förändras till följd av ändringen är det fråga om en liten ändring och den kan göras utan Traficoms bedömning.

3) Traficom ska utan dröjsmål underrättas så noggrant som möjligt om att ändringen distribueras till produkten och om innehållet i ändringen när det görs informationssäkerhetsuppdateringar i produkten.

   Beroende på informationssäkerhetsuppdateringens omfattning och innehåll bedömer Traficom ändringen antingen före eller efter uppdateringen.

   Informationssäkerhetsuppdateringar av produkten ska göras och distribueras till kunderna utan dröjsmål.

4) Traficom ska utan dröjsmål underrättas om att ändringen distribueras till produkten och om innehållet i ändringen när det görs ytliga ändringar i anslutning till varumärket eller motsvarande ändringar i produkten som inte hänför sig till eller påverkar krypteringsegenskaperna.

   Sådana ändringar kan göras och distribueras utan Traficoms bedömning.

   Efter ändringen ska produkten fortfarande till sina krypteringsegenskaper och centrala informationssäkerhetsegenskaper motsvara det ursprungliga utlåtandet och kunna användas i enlighet med användningspolicyn.

Bilagor

1. Beskrivning av bedömningsprocessen
2. Dokumentation som behövs vid bedömningen (Materials required for evaluation). (Denna bilaga är indelad i två delar, en offentlig och en säkerhetsklassificerad bilaga. Den säkerhetsklassificerade delen överlåts separat till dem som behöver den.)
3. Blankett för begäran om bedömning av en krypteringsprodukt
4. Blankett för begäran om bedömning av en säkerhetskritisk produkt