Transport- och kommunikationsverket
Cybersäkerhetscentret

Datum

Cybersäkerhetsmärkets överensstämmelse med krav

Användning av blanketten

Denna blankett ger information om IoT-produktens säkerhet till den nationella cybersäkerhetsmyndigheten och till tekniskt orienterade konsumenter. Blanketten publiceras som en del av konsumentens infopaket när ett nytt märke beviljas.

Del 1 ger allmän information om produkten som fått märket och om det omgivande ekosystemet så som mobilapplikationer och molntjänster som tredje parter tillhandahåller. Del 2 behandlar säkerhetshot som är relevanta för konsumenter samt sådana säkerhetskrav som anlitas för att avvärja hoten. Kraven åtföljs av tabeller som kan användas vid ifyllandet av blanketten när det är möjligt och vettigt. På blanketten ges också exempel på de sätt med vilka det är möjligt att beskriva produktens informationssäkerhetsegenskaper.

Hänvisningarna till ETSI i denna text hänför sig till kraven i standarden

ETSI EN 303 645 "CYBER; Cyber Security for Consumer Internet of Things". Standarden finns tillgänglig på adressen https://www.etsi.org/deliver/etsi_en/303600_303699/303645/02.01.01_60/en_303645v020101p.pdf

Kontaktuppgifter

Företagets namn:	
FO-nummer	
Kontaktperson:	
E-post:	
Telefon:	

Sänd ansökan till adressen tietoturvamerkki@traficom.fi

Transport- och kommunikationsverket
Cybersäkerhetscentret

1 Produktbeskrivning

Beskriv produkten eller produktfamiljen (Produkt) som märket ansöks om. Beskriv också ekosystemet som tillverkaren eller tredje parter tillhandahåller (Tjänst) och som är relevant för produktens funktion.

1.1 Stödperiod

Tillverkaren ska för användaren publicera angiven stödperiod för produkten på ett tillgängligt och transparent sätt (ETSI 5.3-13). Ange stödperioden och berätta hur informationen finns tillgänglig.

1.2 Riktlinjer för informationssäkerheten

Tillverkaren ska tillhandahålla användare anvisningar för hur de kan börja använda Produkten (ETSI 5.12-2). Berätta var säkerhetsanvisningarna finns tillgängliga på finska.

Transport- och kommunikationsverket
Cybersäkerhetscentret

1.3 Övriga certifikat och märken

Ange andra certifikat vars krav Produkten uppfyller. Till exempel CE-märket och/eller FCC-märket; Produkten har certifikat X (t.ex. UK:s säkerhetsmärke, ge länk); Y har verifierat tjänstekomponenterna i produkten

2 Skydd mot typiska IoT-hot

Produkten har skyddats mot typiska IoT-hot såsom beskrivs i delarna nedan.

2.1 Svaga, enkla eller hårdkodade lösenord

Kravnivån på lösenord är följande. Visa överensstämmelse med varje krav med hjälp av checklistorna.

	Överensstämmer med kraven	Kan inte användas	Vet inte	Uppfyller inte kravet
Produktens lösenord måste alltid vara unika per apparat eller definierade av användaren om Produkten inte är i fabriksinställningsläge (ETSI 5.1-1).	☐	☐	☐	☐

Beskriv hur Produkten är skyddad mot hoten som svaga eller hårdkodade lösenord medför. Beskriv hur informationssäkerhetsnivån som motsvarar starka och unika lösenord har uppnåtts. Ett exempel: om produkten till exempel är skyddad på något annat sätt än med identifiering av en användare eller om identifieringen sker på något annat sätt än med lösenord.

Transport- och kommunikationsverket
Cybersäkerhetscentret

2.2 Användning av osäkra eller gamla komponenter

Kraven på användningen av osäkra eller gamla komponenter är följande.

Visa överensstämmelse med varje krav med hjälp av checklistorna.

	Överensstämmer med kraven	Kan inte användas	Vet inte	Uppfyller inte kravet
När apparaten har en mycket begränsad kapacitet ska den ha en uppdateringsmekanism som möjliggör säker installation av uppdateringar. (ETSI 5.3-2).	☐	☐	☐	☐
Det ska vara enkelt för användaren att installera uppdateringarna (ETSI 5.3-3).	☐	☐	☐	☐
Uppdateringarna ska levereras inom skälig tid (ETSI 5.3-8).	☐	☐	☐	☐
Tillverkaren ska klart och begripligt informera användaren om de krävda säkerhetsuppdateringarna samt om riskerna som uppdateringarna skyddar mot. (ETSI 5.3-11).	☐	☐	☐	☐
Tillverkaren ska göra sin policy för hantering av sårbarheter offentligt tillgänglig (ETSI 5.2-1).	☐	☐	☐	☐

Tillverkaren ska kontinuerligt monitorera, identifiera och avlägsna säkerhetssårbarheter i de produkter och tjänster som den säljer, producerar eller har producerat (ETSI 5.2-3).☐	☐	☐	☐	☐

Beskriv hur Produkten eller Tjänsten är skyddad mot hotet om osäkra eller gamla komponenter. Beskriv till exempel hur uppföljningen av sårbarheterna utförs över underleveranskedjor för alla komponenter, inklusive opertivsystem, nättjänster och programbibliotek. Beskriv hur rättidighet, enkel installation, kvalitetssäkring och säker dataöverföring och installation har säkerställts i uppdateringen av Produkten. Typiska uppdateringsintervaller är 30–90 dagar, men detta kan variera betydligt beroende på typ av produkt.

2.3 Otillräckligt dataskydd

Kravet på dataskydd är följande. Visa överensstämmelse med varje krav med hjälp av checklistorna.

	Överensstämmer med kraven	Kan inte användas	Vet inte	Uppfyller inte kravet
Tillverkaren ska tillhandahålla konsumenter klar och transparent information om vilken personuppgift som behandlas, hur den används, vem som använder den och för vilka ändamål. Detta gäller också tredje parter som kan vara involverade, såsom annonsörer (ETSI 6.1).	☐	☐	☐	☐

Transport- och kommunikationsverket
Cybersäkerhetscentret

Beskriv hur identifierbar personuppgift i en Produkt eller Tjänst behandlas och lagras på ett transparent sätt och så att den begränsas bara till sådan omfattning som är nödvändig för funktionaliteten.

Du kan använda följande tabell för att beskriva identifierande personuppgifter.
Förteckningen hjälper vid bedömningen av uppgifterna.

Identifierbar personuppgift	Produkt/Tjänst/Komponent	Syfte	Personuppgiftsbiträde

2.4 Osäker dataöverföring och -lagring

Kraven på dataöverföring och lagring är följande. Visa överensstämmelse med varje krav med hjälp av checklistorna.

Överensstämmer med kraven	Kan inte användas	Vet inte	Uppfyller inte kravet

	Överensstämmer med kravet	Kan inte användas	Vet inte	Uppfyller inte kravet
Sensitiva säkerhetsparametrar i permanent lagring ska sparas i apparaten på ett säkert sätt (ETSI 5.4-1).	☐	☐	☐	☐
Konsument-IoT-enheter ska använda bästa kryptografiska praxis för säker kommunikation (ETSI 5.5-1).	☐	☐	☐	☐
Tillverkaren ska följa informationssäkra hanteringsprocesser vid behandlingen av apparatens kritiska säkerhetsparametrar (ETSI 5.5-8).	☐	☐	☐	☐

Beskriv hur Produkten och/eller Tjänsten och kommunikationen mellan dem är skyddade mot hot som beror på läckor i krypteringen och åtkomsthanteringen. För skyddet av lösenord används här i allmänhet hashfunktioner.

2.5 Osäkra nättjänster och ekosystemgränssnitt

Kraven på nättjänster och ekosystemgränssnitt är följande. Visa överensstämmelse med varje krav med hjälp av checklistorna.

	Överensstämmer med kravet	Kan inte användas	Vet inte	Uppfyller inte kravet
Ändringar som görs via nätet och är relevanta för informationssäkerheten kräver autentisering. (ETSI 5.5-5).	☐	☐	☐	☐
Alla nätverksgränssnitt och logiska gränssnitt som inte är nödvändiga för funktionaliteten ska avlägsnas. (ETSI 5.6-1).	☐	☐	☐	☐

Transport- och kommunikationsverket
Cybersäkerhetscentret

Programvaran bör arbeta med så få behörigheter som möjligt, med beaktande av både informations-säkerhet och funktionalitet. (ETSI 5.6-7).	☐	☐	☐	☐
IoT-konsumentenheten ska validera datainput via olika användargränssnitt. Speciellt de som kommer via användargränssnitt (API) och nätverksgränssnitt (ETSI 5.13-1).	☐	☐	☐	☐

Beskriv hur Produkten är skyddad mot hot i öppna nättjänster, såsom webb-gränssnitt och distansadministration. Beakta också radiogränssnitten.

Beskriv hur de öppna webbgränssnitten i Produkten är skyddade mot hot såsom otillåtet intrång eller dataläckage.

Dessa gränssnitt hänför sig typiskt till molntjänster och fjärradministration.

Du kan använda följande tabell när du svarar på punkterna 2.4 och 2.5. Att göra upp en förteckning över de verktyg och metoder som används vid testningen av Produkten och/eller Tjänsten hjälper i bedömningen.

Nätverksport/ Radioteknologi	Kryptering/ Åtkomsthantering	Användning

Transport- och kommunikationsverket
Cybersäkerhetscentret

2.6 Osäkra standardinställningar

Kravet på osäkra förvalda inställningar är följande. Visa överensstämmelse med varje krav med hjälp av checklistorna.

	Överensstämmer med kraven	Kan inte användas	Vet inte	Uppfyller inte kravet
Installation och underhåll av IoT-konsumentenheter ska innebära minimala beslut av användaren. Dessutom ska man iaktta bästa säkerhetspraxis för tillgänglighet (ETSI 5.12-1).	☐	☐	☐	☐

Beskriv hur Produkten och/eller Tjänsten är skyddad mot osäkra fabriks- eller standardinställningar. Beskriv också hur användaren vägleds att upprätthålla säkra inställningar.