

KOMMISSIONENS GENOMFÖRANDEBESLUT (EU) 2016/650**av den 25 april 2016****om fastställande av standarder för säkerhetsbedömning av kvalificerade anordningar för skapande av elektroniska underskrifter och stämplarna enligt artiklarna 30.3 och 39.2 i Europaparlamentets och rådets förordning (EU) nr 910/2014 om elektronisk identifiering och betrodda tjänster för elektroniska transaktioner på den inre marknaden****(Text av betydelse för EES)**

EUROPEISKA KOMMISSIONEN HAR ANTAGIT DETTA BESLUT

med beaktande av fördraget om Europeiska unionens funktionssätt,

med beaktande av Europaparlamentets och rådets förordning (EU) nr 910/2014 av den 23 juli 2014 om elektronisk identifiering och betrodda tjänster för elektroniska transaktioner på den inre marknaden och om upphävande av direktiv 1999/93/EG⁽¹⁾, särskilt artiklarna 30.3 och 39.2, och

av följande skäl:

- (1) I bilaga II till förordning (EU) nr 910/2014 fastställs kraven på kvalificerade anordningar för skapande av elektroniska underskrifter och kvalificerade anordningar för skapande av elektroniska stämplarna.
- (2) Behöriga standardiseringsorganisationer handhar uppgiften att utarbeta de tekniska specifikationer som behövs för produktion och utsläppande på marknaden av produkter, med beaktande av nuvarande tekniska utvecklingsstadium.
- (3) ISO/IEC (Internationella standardiseringsorganisationen/Internationella elektrotekniska kommissionen) fastställer de allmänna koncepten och principerna för it-säkerhet och anger vilken allmän modell som ska användas som utgångspunkt för bedömning av it-produkters säkerhet.
- (4) Europeiska standardiseringskommittén (CEN) har, inom ramen för kommissionens standardiseringsuppdrag M/460, tagit fram standarder för kvalificerade anordningar för skapande av elektroniska underskrifter och stämplarna, om uppgifterna för skapande av elektroniska underskrifter eller uppgifter för skapande av elektroniska stämplarna bevaras i en helt, men inte nödvändigtvis uteslutande, användarskött miljö. Dessa standarder anses lämpliga för att bedöma om dessa produkter överensstämmer med de relevanta krav som anges i bilaga II till förordning (EU) nr 910/2014.
- (5) I bilaga II till förordning (EU) nr 910/2014 fastställs att endast en kvalificerad tillhandahållare av betrodda tjänster får hantera uppgifter för skapande av elektroniska underskrifter på en undertecknares vägar. Säkerhetskraven med respektive certifieringsspecifikationer skiljer sig åt beroende på om undertecknaren fysiskt äger en produkt eller en kvalificerad tillhandahållare av betrodda tjänster arbetar på uppdrag av undertecknaren. För att ta itu med dessa problem och för att gynna den framtida utvecklingen av produkt- och bedömningsstandarder som är lämpliga för vissa behov, bör standarder för båda situationerna förtecknas i bilagan till detta beslut.
- (6) Vid den tidpunkt då kommissionen väl har antagit detta beslut kommer flera tillhandahållare av betrodda tjänster redan att erbjuda sina kunder lösningar för att hantera anordningar för skapande av elektroniska underskrifter. Certifieringar av produkter är för närvarande begränsade till säkerhetsmoduler i maskinvara som certifierats enligt olika standarder, men som ännu inte särskilt har certifierats enligt kraven på kvalificerade anordningar för skapande av elektroniska underskrifter och stämplarna. Offentliggjorda standarder, som t.ex. EN 419 211 (tillämplig på elektroniska underskrifter som skapats i en helt, men inte nödvändigtvis uteslutande, användarskött miljö) förekommer dock ännu inte på den lika viktiga marknaden för certifierade distansprodukter. Eftersom standarder som kan vara lämpliga för sådana syften för närvarande håller på att utvecklas, kommer kommissionen att komplettera detta beslut när sådana standarder är tillgängliga och bedöms uppfylla kraven i bilaga II till förordning (EU) nr 910/2014. Till dess att förteckningen över sådana standarder har upprättats, kan ett alternativt förfarande användas för att bedöma om sådana produkter överensstämmer med reglerna enligt de villkor som föreskrivs i artikel 30.3 b i förordning (EU) nr 910/2014.
- (7) I bilagan förtecknas EN 419 211 som består av olika delar (1–6) som omfattar olika situationer. EN 419 211 del 5 och del 6 innebär utökade krav i förhållande till miljön för kvalificerade anordningar för skapande

⁽¹⁾ EUT L 257, 28.8.2014, s. 73.

av elektroniska underskrifter, såsom kommunikation med betrodda anordningar för skapande av underskrifter. Det står produktutvecklare fritt att tillämpa sådana utökade krav. Enligt skäl 56 i förordning (EU) nr 910/2014 är certifieringens omfattning enligt artiklarna 30 och 39 i den förordningen begränsad till att skydda uppgifterna för skapande av underskrifter, och anordningar för skapande av signaturer omfattas inte av certifieringen.

- (8) För att säkerställa att de elektroniska underskrifter och stämplat, som genereras med en kvalificerad anordning för skapande av underskrifter eller stämplat, på ett tillförlitligt sätt är skyddade mot förfälskning, i enlighet med bilaga II till förordning (EU) nr 910/2014, är lämpliga kryptografiska algoritmer, nycklar och hashfunktioner en förutsättning för den certifierade produktens säkerhet. Eftersom denna fråga inte har harmoniserats på EU-nivå, bör medlemsstaterna samarbeta för att enas om vilka kryptografiska algoritmer, nycklar och hashfunktioner som ska användas när det gäller elektroniska underskrifter och stämplat.
- (9) Antagandet av detta beslut innebär att kommissionens beslut 2003/511/EG⁽¹⁾ blir ogiltigt. Det bör därför upphävas.
- (10) De åtgärder som föreskrivs i detta beslut är förenliga med yttrandet från den kommitté som avses i artikel 48 i förordning (EU) nr 910/2014.

HÄRIGENOM FÖRESKRIVS FÖLJANDE.

Artikel 1

1. I bilagan till beslutet förtecknas de standarder för säkerhetsbedömning av informationsteknikprodukter som gäller för certifiering av kvalificerade anordningar för skapande av elektroniska underskrifter eller kvalificerade anordningar för skapande av elektroniska stämplat i enlighet med artikel 30.3 a eller artikel 39.2 i förordning (EU) nr 910/2014, i de fall de uppgifter som genereras för skapande av elektroniska underskrifter eller av elektroniska stämplat bevaras i en helt, men inte nödvändigtvis uteslutande, användarskött miljö.

2. Intill dess att kommissionens upprättat en förteckning över standarder för den säkerhetsbedömning av informationsteknikprodukter som gäller för certifiering av kvalificerade anordningar för skapande av elektroniska underskrifter eller kvalificerade anordningar för skapande av elektroniska stämplat, i de fall en kvalificerad tillhandahållare av betrodda tjänster åt en undertecknare eller skapare av stämplat förvaltar sådana uppgifter som genereras för skapande av elektroniska signaturer eller uppgifter för skapande av elektroniska stämplat, ska certifieringen av sådana produkter bygga på en process som, i enlighet med artikel 30.3 b, använder säkerhetsnivåer jämförbara med dem som krävs enligt artikel 30.3 a och som anmälts till kommissionen av de offentliga eller privata organ som avses i artikel 30.1 i förordning (EU) nr 910/2014.

Artikel 2

Beslut 2003/511/EG ska upphöra att gälla.

Artikel 3

Detta beslut träder i kraft den tjugonde dagen efter det att det har offentliggjorts i *Europeiska unionens officiella tidning*.

Utfärdat i Bryssel den 25 april 2016.

På kommissionens vägnar
Jean-Claude JUNCKER
Ordförande

⁽¹⁾ Kommissionens beslut 2003/511/EG av den 14 juli 2003 om offentliggörande av referensnummer till allmänt erkända standarder för produkter för elektroniska signaturer i enlighet med Europaparlamentets och rådets direktiv 1999/93/EG (EUT L 175, 15.7.2003, s. 45).

BILAGA

FÖRTECKNING ÖVER DE STANDARDER SOM AVSES I ARTIKEL 1.1

- ISO/IEC 15408 – Information technology – Security techniques – Evaluation criteria for IT security, delarna 1–3 i nedanstående förteckning:
 - ISO/IEC 15408-1:2009 – Information technology – Security techniques – Evaluation criteria for IT security – Del 1. ISO, 2009
 - ISO/IEC 15408-2:2008 – Information technology – Security techniques – Evaluation criteria for IT security – Del 2. ISO, 2008
 - ISO/IEC 15408-3:2008 – Information technology – Security techniques – Evaluation criteria for IT security – Del 3. ISO, 2008

och

 - ISO/IEC 18045:2008: Information technology – Security techniques – Methodology for IT security evaluation

och

 - EN 419 211 – Skyddsprofil för säker signaturanordning, delarna 1–6 – på tillämpligt sätt – i nedanstående förteckning:
 - EN 419211-1:2014 – Skyddsprofil för säker signaturanordning – Del 1: Översikt
 - EN 419211-2:2013 – Skyddsprofil för säker signaturanordning – Del 2: Signaturanordning med nyckelgenerering
 - EN 419211-3:2013 – Skyddsprofil för säker signaturanordning – Del 3: Signaturanordning med nyckelimport
 - EN 419211-4:2013 – Skyddsprofil för säker signaturanordning – Del 4: Anslutning av signaturanordning med nyckelgenerering och säker kommunikation till applikation för certifikatsgenerering
 - EN 419211-5:2013 – Skyddsprofil för säker signaturanordning – Del 5: Anslutning av signaturanordning med nyckelgenerering och säker kommunikation till applikation för signaturgenerering
 - EN 419211-6:2014 – Skyddsprofil för säker signaturanordning – Del 6: Anslutning av signaturanordning med nyckelimport och säker kommunikation till applikation för signaturgenerering
-