



Föreskrift

OM KRAV PÅ TILLFÖRLITLIGHET OCH INFORMATIONSSÄKERHET I VERKSAMHET HOS LEVERANTÖRER AV IDENTIFIERINGSTJÄNSTER OCH CERTIFIKATUTFÄRDARE SOM TILLHANDAHÅLLER KVALIFICERADE CERTIFIKAT

Meddelad i Helsingfors den 20 oktober 2010

Kommunikationsverket har med stöd av 8 § 3 mom. och 42 § 2 mom. i lagen av den 7 augusti 2009 om stark elektronisk autentisering och elektroniska signaturer (617/2009) meddelat följande föreskrift:

1 §

Tillämpningsområde

Denna föreskrift tillämpas på leverantörer som tillhandahåller tjänster för stark autentisering och på certifikatutfärdare som tillhandahåller kvalificerade certifikat. Båda kallas nedan tjänsteleverantör.

2 §

Hantering av informationssäkerhet

Organisering av informationssäkerheten

En tjänsteleverantör ska skriftligen definiera organisationen av informationssäkerheten med uppgifter om ansvar och rapporteringsförhållanden. Definitionerna ska upprätthållas och granskas åtminstone en gång om året. Informationssäkerhetsansvar för personer som innehar ledningsuppgifter inom informationssäkerheten ska framgå av deras befattningsbeskrivningar.

Styrdokument för informationssäkerhet

Tjänsteleverantören ska ha en skriftligen definierad och av ledningen fastställt uppfattning om mål och principer för samt genomförande av informationssäkerhet. Uppfattningen ska delges hela personalen som arbetar med att tillhandahålla tjänster för identifiering och kvalificerade certifikat.

Tjänsteleverantören ska dessutom skriftligen dokumentera hur följande specialområden beaktas i den mån de lämpar sig för den tjänst som tillhandahålls:

- 1) administrativ säkerhet
- 2) personalsäkerhet
- 3) fysisk säkerhet
- 4) maskin- och programvarusäkerhet
- 5) telekommunikationssäkerhet
- 6) datamaterialsäkerhet
- 7) driftssäkerhet och
- 8) ingripande i kränkningar och missbruk av informationssäkerheten.

Riskhantering

Tjänsteleverantören ska göra upp en plan för bedömning av riskerna som hänför sig till tjänsten. Tjänsteleverantören ska identifiera och bedöma sådana informationssäkerhetsrisker i funktioner, uppgifter och system som är viktiga för tillhandahållandet av identifieringstjänster och kvalificerade certifikat. Tjänsteleverantören ska ha ett förfarande för att acceptera sådana betydande risker som inte blir föremål för hanteringsåtgärder på basis av bedömningen av riskerna. Riskhanteringen ska vara systematisk, regelbunden och dokumenterad.

Informationssäkerhetsåtgärder

Tjänsteleverantören ska på basis av riskanalysens resultat göra upp en plan som definierar åtgärder, ansvar och tidsscheman för hantering av identifierade risker. Tjänsteleverantören ska regelbundet följa upp hur åtgärderna lämpar sig för användningsändamålet.

Tjänsteleverantören ska definiera tillräckligt detaljerade anvisningar för enskilda rutiner som är väsentliga för informationssäkerheten. Tjänsteleverantören ska se till att personal som medverkar vid tillhandahållandet av identifieringstjänster och kvalificerade certifikat får utbildning i givna anvisningar.

Tjänsteleverantören ska använda ett system för klassificering av datamaterial som är viktigt för den tjänst som tillhandahålls.

Tjänsteleverantören ska se till att händelser som är väsentliga för informationssäkerheten upptäcks. Tjänsteleverantören ska ingripa i upptäckta problem.

Uppföljning av hanteringen av informationssäkerheten

Genomförandet av föreskriftens skyldigheter ska granskas regelbundet och alltid vid behov.

3 §

Inledande identifiering och registrering av sökande

En leverantör av identifieringstjänster ska identifiera den som ansöker om ett identifieringsverktyg i enlighet med 17 § i lagen om stark autentisering och elektroniska signaturer. En certifikatutfärdare som tillhandahåller kvalificerat certifikat ska identifiera den som ansöker om kvalificerat certifikat i enlighet med lagens 35 §. Syftet med den inledande identifieringen är att trygga att identifieringsverktyget eller det kvalificerade certifikatet har korrekt och tillförlitligt datainnehåll samt att de relaterade elektroniska tjänsterna kan användas på ett korrekt och tillförlitligt sätt.

Den inledande identifieringen ska göras i samband med att en sökande vill skaffa ett identifieringsverktyg eller ett kvalificerat certifikat. Identitet hos och övriga uppgifter om den som ansöker om ett identifieringsverktyg eller ett kvalificerat certifikat ska granskas omsorgsfullt innan verktyget eller certifikatet första gången överläts till sökanden.

Leverantören av identifieringstjänster ska lagra uppgifter om den inledande identifieringen av sökanden och om den handling som använts vid identifieringen.

Om identifieringsmetoden baserar sig på ett certifikat eller om det är fråga om ett kvalificerat certifikat, ska tjänsteleverantören samla in och lagra alla uppgifter som hänför sig till certifikatets datainnehåll. Om en certifikatutfärdare inte skapar ett nyckelpar ska certifikatutfärdaren kontrollera att sökanden förfogar över en privat nyckel som svarar mot den öppna nyckeln, som certifieras.

Certifikatutfärdaren som tillhandahåller kvalificerade certifikat ska registrera uppgifter om sökanden i samband med ansökan om kvalificerat certifikat. Uppgifter som ska införas i registret är sökandens namn och tillräckliga uppgifter för att olika personer med samma namn ska kunna skiljas från varandra. I registret ska också införas uppgifter om den inledande identifieringen, behövliga uppgifter om de handlingar som använts vid identifieringen samt andra uppgifter som är relevanta för utfärdandet av det kvalificerade certifikatet.

4 §

Skapande av identifieringsverktyg och kvalificerade certifikat

Ett identifieringsverktyg eller kvalificerat certifikat kan skapas bara om ansökan om dem uppfyller de villkor som uppställts för kvalificerade certifikat eller identifieringsverktyg. Identifieringsverktyget eller det kvalificerade certifikatet får inte skapas före inledande identifiering av den sökande.

En tjänsteleverantör ska lagra uppgift om att ett identifieringsverktyg och kvalificerat certifikat har skapats.

Vid skapande av identifieringsverktyg och kvalificerade certifikat ska de av tjänsteleverantören använda systemen bevara uppgifternas tillförlitlighet och integritet.

Tjänsteleverantören ska på ett tillräckligt tillförlitligt sätt säkerställa att endast innehavaren av ett identifieringsverktyg eller kvalificerat certifikat kan använda det.

Algoritmer och nycklar som använts vid identifieringsmetoden och det kvalificerade certifikatet ska vara trygga och överensstämna med allmänt godkända standarder eller rekommendationer.

5 §

Distribution av certifikat

En tjänsteleverantör och innehavare av certifikat kan komma överens om att certifikatet görs tillgängligt för alla som förlitar sig på certifikatet. Om tjänsteleverantören offentliggör certifikaten i en offentlig katalog, ska katalogen vara tillgänglig dygnet runt.

Tjänsteleverantören får inte kopiera hemliga uppgifter som hänför sig till certifikatet, eftersom endast den sökande bör veta om eller ha tillgång till sådana uppgifter.

6 §

Tillhandahållande av tjänsten**Handlingar som hänför sig till tillhandahållandet av tjänsten**

I fråga om certifikat ska en tjänsteleverantör hålla sin certifikatpolicy och certifieringsstandard allmänt tillgängliga och uppdaterade och i fråga om identifieringstjänster ska tjänsteleverantören hålla sina principer för identifiering allmänt tillgängliga och uppdaterade.

Parternas informationssäkerhets- och certifikatpolicy, principer för identifiering samt informationssäkerhetsrutiner och certifieringsstandard ska motsvara varandra vid krosscertifieringen.

Återkallande av identifieringsverktyg och kvalificerade certifikat och kontroll av deras giltighet

Tjänsteleverantören ska behandla begäran om återkallanden av identifierings- och signaturverktyg utan dröjsmål och på ett sådant sätt att alla begäran identifieras och behandlas tillräckligt noggrant.

Tjänsteleverantören ska lagra uppgift om att ett identifierings- eller signaturverktyg har satts i avbrottsläge, tagits i bruk igen eller återkallats. Uppgiften ska vara tillgänglig för den som förlitar sig på tjänsten utan dröjsmål efter det att tjänsteleverantören har fått veta orsaken till återkallandet eller avbrottsläget.

Tjänsteleverantören ska kunna återkalla alla identifierings- och signaturverktyg. Tjänsteleverantören ska underrätta innehavaren av identifierings- och signaturverktyget om återkallandet.

Den som förlitar sig på ett certifikat ska ha möjlighet att kontrollera certifikatets status med hjälp av en spärmliststjänst. Spärmliststjänsten kan uppdateras i realtid eller med jämna mellanrum. Tjänsteleverantören ska signera alla spärmlistor och svar på förfrågningar om certifikatens spärstatus. Den signerade spärmlistan eller det signerade svaret ska innehålla uppgift om den tidpunkt då listan offentliggjorts eller svaret givits.

Certifikatutfärdarens signaturnycklar

Tjänsteleverantören ska se till att de privata nycklar som använts vid skapandet av certifikaten inte kan tas i bruk igen när nycklarnas livscykel tar slut.

Tjänsteleverantören ska försäkra sig om att alla privata och hemliga nycklar vilka använts för skapande och signatur av certifikat förvaras på ett tryggt sätt och lagras och säkerhetskopieras endast av behöriga personer i trygg miljö.

Avsevärda händelser vid tillhandahållandet av tjänsten

Tjänsteleverantören ska lagra uppgifter om alla händelser som är avsevärda med tanke på tillhandahållandet av tjänsten.

Hindrande av obehörig användning

Tjänsteleverantören ska skydda identifieringsverktyget och det kvalificerade certifikatet mot obehörig användning.

Tjänsteleverantören ska säkerställa att hemliga uppgifter som hänför sig till det kvalificerade certifikatet eller identifieringsverktyget inte under några omständigheter avslöjas till personalen.

7 §

Upphörande av verksamhet

En leverantör av identifieringstjänster ska underrätta Kommunikationsverket, de personer som den anlitat i identifieringsverksamheten, innehavare av identifieringsverktyg, tjänsteleverantörer som använder identifieringstjänster samt övriga samarbetsparter inom identifieringsverksamheten om att verksamheten upphör. Leverantören av identifieringstjänster ska också se till att den olägenhet som upphörandet av verksamheten vållar innehavare av identifieringsverktyg och tjänsteleverantörer som använder identifieringstjänster är så liten som möjligt.

En certifikatutfärdare som tillhandahåller kvalificerade certifikat ska underrätta Kommunikationsverket, de personer som den anlitat i certifikatverksamheten, innehavare av kvalificerade certifikat och alla samarbetsorganisationer i anslutning till certifikatverksamheten om att verksamheten upphör. Certifikatutfärdaren ska också se till att den olägenhet som upphörandet vållar innehavare av kvalificerade certifikat och parter som förlitar sig på de kvalificerade certifikaten är så liten som möjligt.

8 §

Ikraftträdande och övergångsbestämmelser

Denna föreskrift träder i kraft den 20 oktober 2010 och gäller tills vidare. Genom föreskriften upphävs föreskrift 8 B/2009 M av den 27 augusti 2009 om krav på tillförlitlighet och informationssäkerhet i verksamhet hos leverantörer av identifieringstjänster och certifikatutfärdare som tillhandahåller allmänheten kvalificerade certifikat.

9 §

Erhållande av upplysningar och publicering

Föreskriften har publicerats i Kommunikationsverkets föreskriftssamling och kan erhållas vid Kommunikationsverkets kundtjänst:

Besöksadress	Östersjögatan 3 A, HELSINGFORS
Postadress	PB 313, 00181 HELSINGFORS
Telefon	09 69661
från utlandet	+358 9 69661
Telefax	09 6966 410
från utlandet	+358 9 6966 410
Webbplats	http://www.ficora.fi/
FO-nummer	0709019-2

Helsingfors den 20 oktober 2010

Ställföreträdande generaldirektör Jorma Koivunmaa

Direktör Timo Lehtimäki