

**MOTIVERING TILL OCH TILLÄMPNING AV  
FÖRESKRIFT 8**

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

**INNEHÅLLSFÖRTECKNING**

<b>INNEHÅLLSFÖRTECKNING .....</b>	<b>1</b>
<b>1 LAGSTIFTNING .....</b>	<b>2</b>
1.1 RÄTTSGRUND .....	2
1.2 ANDRA RELATERADE BESTÄMMELSER .....	2
<b>2 SYFTET MED FÖRESKRIFTEN OCH ÄNDRINGSHISTORIA.....</b>	<b>2</b>
2.1 SYFTET MED FÖRESKRIFTEN .....	2
2.2 CENTRALA ÄNDRINGAR OCH ÄNDRINGSHISTORIA .....	3
2.3 DEFINITIONER .....	3
<b>3 MOTIVERING TILL ENSKILDA PARAGRAFER OCH ANVISNINGAR FÖR TILLÄMPNING .....</b>	<b>6</b>
3.1 1 § TILLÄMPNINGSOMRÅDE.....	7
3.2 2 § HANTERING AV INFORMATIONSSÄKERHET .....	7
3.3 3 § INLEDANDE IDENTIFIERING OCH REGISTRERING AV SÖKANDE .....	18
3.4 4 § SKAPANDE AV IDENTIFIERINGSVERKTYG OCH KVALIFICERADE CERTIFIKAT .....	22
3.5 5 § DISTRIBUTION AV CERTIFIKAT .....	23
3.6 6 § TILLHANDAHÅLLANDE AV TJÄNSTEN .....	23
3.7 7 § UPPHÖRANDE AV VERKSAMHET.....	26
<b>4 REFERENSLISTA.....</b>	<b>27</b>

## **1 LAGSTIFTNING**

Syftet med detta kapitel är att ge föreskriftens användare en helhetsbild av de författningar som utgör grunden för föreskriften. Här uppräknas också andra väsentliga författningar som har samband med ämnet.

### **1.1 Rättsgrund**

Kommunikationsverkets föreskrift baserar sig på 8 § 3 mom. och 42 § 2 mom. i lagen om stark autentisering och elektroniska signaturer (617/2009, nedan lagen om stark autentisering ) [1].

### **1.2 Andra relaterade bestämmelser**

I detta avsnitt beskrivs Kommunikationsverkets andra föreskrifter som har samband med denna föreskrift.

Kommunikationsverket har på basis av 10 § 4 mom. och 32 § 1 mom. i lagen om stark autentisering meddelat föreskrift 7 B/2009 M om skyldighet för leverantörer av identifieringstjänster och certifikatutfärdare som tillhandahåller allmänheten kvalificerade certifikat att göra en anmälan om sin verksamhet till Kommunikationsverket. Krav på innehållet i anmälningarna behandlas närmare i föreskriftens 2–7 §.

## **2 SYFTET MED FÖRESKRIFTEN OCH ÄNDRINGSHISTORIA**

Syftet med detta kapitel är att informera användaren om föreskriftens mål och syften. I kapitlet behandlas också de mest betydande ändringarna av tidigare skyldigheter och rekommendationer.

### **2.1 Syftet med föreskriften**

Hanteringen av informationssäkerheten har beskrivits på ett heltäckande sätt bland annat i standarden ISO 27001 (Information Security Management – Specification With Guidance for Use) [2]. Ett heltäckande iakttagande av denna standard kan vara alltför tungt i synnerhet för små tjänsteleverantörer i Finland.

I föreskriften beskrivs de minimikrav för administrationen av informationssäkerheten som varje tjänsteleverantör bör uppfylla i sin verksamhet. Syftet med kraven är att trygga tjänsteleverantörernas grundläggande informationssäkerhetsnivå när de utfärdar kvalificerade certifikat och tillhandahåller identifieringstjänster. Den grundläggande informationssäkerhetsnivån utgör grunden för informationssäkerheten hos de tjänster som erbjuds. Kraven fokuserar i synnerhet på inledande identifiering och att informationssäkerhet hanteras med hjälp av kontinuerlig utveckling, planering, genomförande och bedömning. Syftet med föreskriften är också att minska informationssäkerhetsriskernas skadliga verkningar på tjänsten.

## 2.2 Centrala ändringar och ändringshistoria

Föreskriftens tillämpningsområde har utvidgats så att alla paragrafer gäller både leverantörer av identifieringstjänster och utfärdare av kvalificerade certifikat. Innehållsmässigt har föreskriftens krav ändrats så att de i princip lämpar sig på både identifieringstjänster och utfärdande av kvalificerade certifikat. I föreskriften anges särskilt, om ett krav endast kan tillämpas på utfärdande av kvalificerade certifikat eller på en identifieringstjänst som tillhandahålls med hjälp av ett certifikat.

Bestämmelser om hantering av informationssäkerhet har samlats ihop i föreskriftens 2 §. Också paragrafen som tidigare endast gällde återkallande av kvalificerade certifikat och kontroll av certifikatens giltighetstid (f.d. 7 §, nu 6 §) har utvidgats till att gälla tillhandahållandet av tjänsten i allmänhet.

## 2.3 Definitioner

Här behandlas de definitioner som används i föreskriften.

### 2.3.1 Tjänsteleverantör

Med tjänsteleverantör avses i föreskriften både utfärdare av kvalificerade certifikat och leverantörer av stark autentisering.

### 2.3.2 Informationssäkerhet

Med informationssäkerhet avses administrativa och tekniska åtgärder genom vilka säkerställs att uppgifter är tillgängliga endast för behöriga personer, att uppgifterna inte kan ändras av andra än behöriga personer och att uppgifterna och datasystemen kan utnyttjas av behöriga personer.

### 2.3.3 Informationssäkerhetsrisk

Med informationssäkerhetsrisker avses i denna föreskrift en sådan oavsiktlig eller avsiktlig faktor som äventyrar den tillhandahållna tjänstens konfidentialitet, integritet eller tillgänglighet. Skillnaden mellan informationssäkerhetsrisker och informationssäkerhetshot är att informationssäkerhetsriskernas sannolikhet och verkningar har bedömts.

Informationssäkerhetsrisker kan orsakas av:

- mänskliga misstag
- brister i eller underlåtenhet att iaktta instruktioner till personalen
- stölder

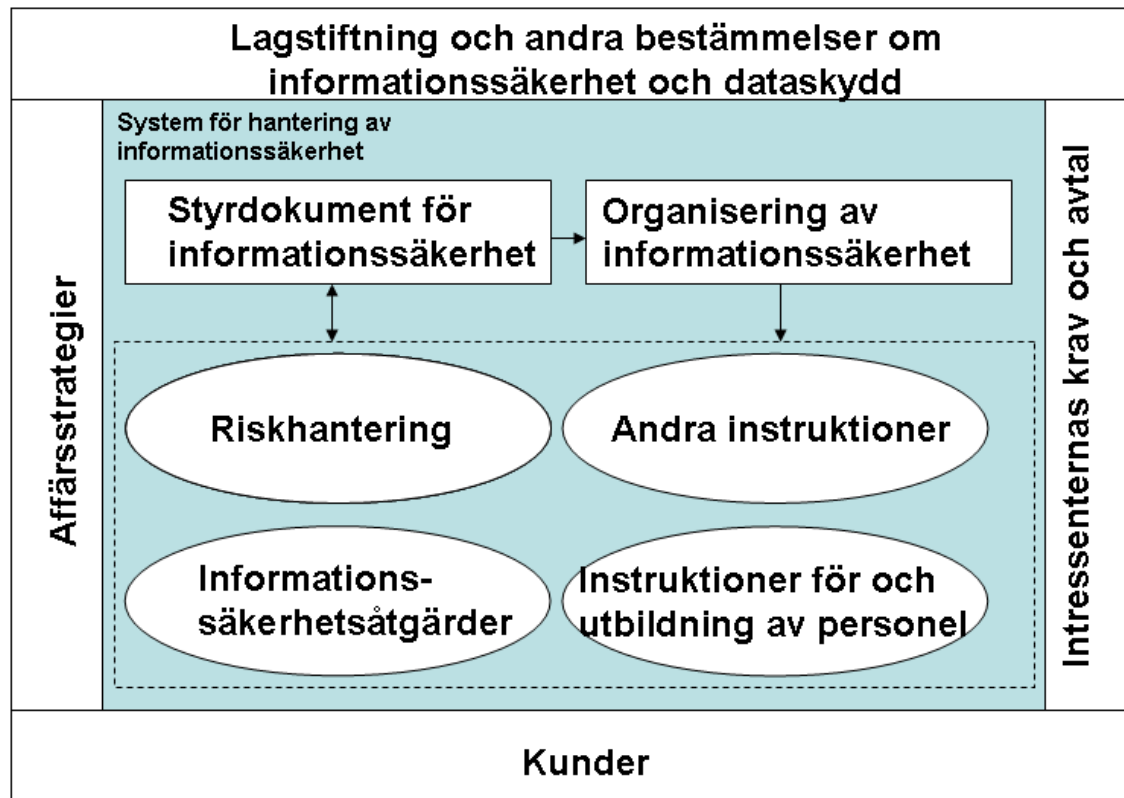
- kapacitetsbrister
- fel i apparater
- fel i applikationer
- spridning av skadliga program
- telekommunikationsstörningar
- vandalism
- eldsvåda
- fel och försummelser begångna av en underleverantör eller en aktör som ingår i partnerskapsnätverket.

#### **2.3.4 Certifikat**

Med ett certifikat avses i denna föreskrift kvalificerade certifikat som uppfyller kraven i EU:s direktiv om elektroniska signaturer samt certifikat som baserar sig på stark autentisering och används i identifieringsverktyg.

#### **2.3.5 System för hantering av informationssäkerhet**

Med system för hantering av informationssäkerhet avses i detta sammanhang en del av tjänsteleverantörens ledningssystem som baserar sig på bedömning och hantering av risker. Av tjänsteleverantören förutsätts kännedom om dess verksamhetsmiljö och beaktande av verksamhetsmiljöns särdrag i utvecklingen av systemet för hantering av informationssäkerhet. Krav på systemet baserar sig förutom på affärsstrategin i allmänhet även på informationssäkerhets- och dataskyddslagstiftningen, Kommunikationsverkets föreskrifter, andra bestämmelser samt kundernas och intressenternas krav och avtal.



**Krav på tjänsteleverantörens informationssäkerhet baserar sig på informationssäkerhets- och dataskyddslagstiftningen samt andra bestämmelser, till exempel:**

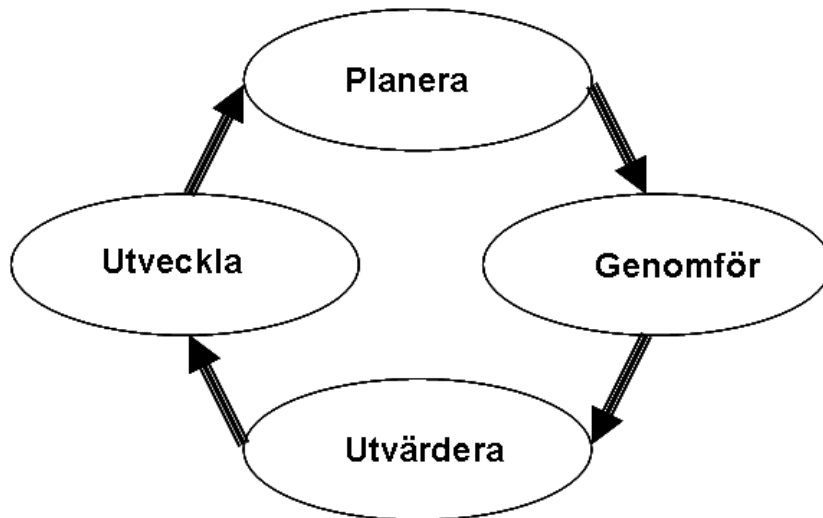
- lagen om stark autentisering och elektroniska signaturer
- Kommunikationsverkets föreskrift 8/2010 M
- personuppgiftslagen.

**Även andra krav gällande informationssäkerheten kan ställas på tjänsteleverantörens verksamhet, till exempel:**

- kundernas krav
- andra föreskrifter, författningar och standarder som gäller identifieringsverktyg och kvalificerade certifikat
- branschspecifika krav.

Syftet med hanteringssystemet är att stödja utvecklingen, planeringen, genomförandet och utvärderingen av informationssäkerheten.

Systemet för hantering av informationssäkerhet beskrivs i allmänhet som en process i fyra steg:

**Planering:**

Vid planeringen skapas policyn, definieras målsättningarna och objekten samt nödvändiga funktioner för informationssäkerheten.

**Genomförande:**

Vid genomförandet tillämpas informationssäkerhetspolicyn, -kontroller och -funktioner.

**Utvärdering:**

Vid utvärderingen mäts åtgärdernas inverkan på de målsättningar, policyn och praktiska erfarenheter som fastställts vid planeringen.

**Utveckling:**

I utvecklingsfasen utvecklas systemet för hantering av informationssäkerhet utifrån resultaten av utvärderingen. Utvecklingsmål kan bland annat vara informationssäkerhetspolicyn och informationssäkerhetsfunktioner.

### 3 MOTIVERING TILL ENSKILDA PARAGRAFER OCH ANVISNINGAR FÖR TILLÄMPNING

I detta kapitel behandlas motiveringen till enskilda paragrafer samt rekommendationer för tillämpningen av dem.

Syftet med detta dokument är att beskriva bästa praxis och bidra till deras genomförande. Leverantörer av identifieringstjänster eller utfärdare av kvalificerade certifikat är i och för sig inte bundna till dokumentet som inte heller används som måttstock för bedömning eller auditering av informationssäkerhetsarrangemang hos leverantörerna eller utfärdarna. Rekommendationsartade ärenden skrivs i form av rekommendation.

Detta dokument omfattar även skyldigheter som föranleds av föreskriften och därför anges i form av bindande förpliktelse.

### **3.1 1 § Tillämpningsområde**

Denna föreskrift tillämpas på leverantörer som tillhandahåller tjänster för stark autentisering och på certifikatutfärdare som tillhandahåller kvalificerade certifikat. Då det i föreskriften hänvisas till både leverantörer av identifieringstjänster och certifikatutfärdare som utfärdar kvalificerade certifikat, kallas båda tjänsteleverantör.

Leverantör av identifieringstjänster och certifikatutfärdare som tillhandahåller kvalificerade certifikat är i överensstämmelse med termerna i lagen om stark autentisering och därför är det inte nödvändigt att upprepa definitionerna i föreskriften. Med leverantör av identifieringstjänster avses i 2 § 4 punkten i lagen en tjänsteleverantör som tillhandahåller tjänster för stark autentisering till tjänsteleverantörer som använder sådana tjänster eller som ger ut identifieringsverktyg till allmänheten eller bådadera.

Med certifikatutfärdare avses enligt 2 § 8 punkten i lagen en fysisk eller juridisk person som tillhandahåller allmänheten certifikat. En certifikatutfärdare som tillhandahåller kvalificerade certifikat är en certifikatutfärdare som tillhandahåller kvalificerade certifikat enligt lagens 30 §. Då definitionen av en certifikatutfärdare i lagen om stark autentisering redan omfattar tillhandahållandet av certifikat till allmänheten, är det inte nödvändigt att upprepa definitionen här.

### **3.2 2 § Hantering av informationssäkerhet**

Säkerställandet av data, datasystem och verksamhetsförutsättningar förutsätter att informationssäkerhetsfunktionerna är effektivt organiserade i företaget. Den grundläggande förutsättningen är att ansvarsområdena och skyldigheterna för informationssäkerhetsfunktionerna har definierats.

#### **3.2.1 Organisering av informationssäkerheten**

Systemet för hantering av informationssäkerhet ska omfatta den högsta ledningens uppfattning om hur ansvaret för informationssäkerheten är fördelat inom organisationen. Ansvaret och skyldigheterna för informationssäkerheten kan vara både administrativa och operativa. Det finns skäl att granska ansvaret för informationssäkerheten i synnerhet då det sker ändringar i organisationen. Det kan till exempel handla om en ändring i personalen eller en ändring av verksamhetsomgivningen på grund av företagsarrangemang.

Ansvaret för informationssäkerheten kan fördelas mellan olika grupper. Vad gäller det administrativa ansvaret kan man som exempel nämna informationssäkerhetsgruppen. Exempel på operativa grupper är cert/csirt-grupperna.

Exempel på administrativt ansvar för informationssäkerheten är utveckling av system för hantering av informationssäkerhet och styrdokument, upprätthållande av företagets informationssäkerhetsläge, beaktande av informationssäkerhetsfrågor i riskhanteringen och kontinuitetsplaneringen, upprätthållande och utveckling av ändamålsenliga datasystem samt korrekt allokering av resurser till informationssäkerhetsfunktioner och -investeringar samt beaktande av informationssäkerhetsfrågor i synnerhet i utbildningen av nyckelpersonal.

Eftersom dessa ansvarsförhållanden gäller flera delområden inom företagets ledningssystem är det motiverat att styra och övervaka genomförandet av informationssäkerhetsansvaret på ett koordinerat sätt. Betydelsen av en fungerande samordning är desto viktigare ju mer utspritt ansvaret för informationssäkerheten är i företagets organisation. Beroende på företagets storlek ska ansvaret för utvecklingen och uppföljningen av informationssäkerhetsärenden fördelas mellan en eller flera informationssäkerhetsansvariga. Informationssäkerhetsärenden ska hanteras som en del av ledningens normala rapportering.

För de primära samordnade åtgärderna vid hanteringen av kränkningar av informationssäkerheten och upprätthållandet av kontaktpunkten används i vissa sammanhang benämningen CERT (Computer Emergency Response Team) eller CSIRT (Computer Security Incident Response Team).

Tjänsteleverantören ska dock alltid ha en grundläggande beredskap för att hantera informationssäkerhetsbrott och -risker som har en betydande inverkan på företagets verksamhet och dess kunder.

Med administrativt ansvar kan man till exempel avse ansvar för:

- planering av informationssäkerhetspolicy
- planering av personalens informationssäkerhetsutbildning
- uppföljning av tjänsteleverantörens interna informationssäkerhetsnivå
- planering och organisering av riskhanteringen
- hantering och planering av projekt som förbättrar informationssäkerheten.

### **3.2.2 Styrdokument för informationssäkerhet**

Informationssäkerhet utgör en del av kvaliteten på den tjänst som tillhandahålls. Styrdokumentet för informationssäkerhet är grundläggande dokument om informationssäkerhet genom vilka organisationens ledning visar de övergripande målen och de allmänna principerna för informationssäkerheten. Dokumentet skapar en grund för en systematisk utveckling och hantering av informationssäkerheten och hjälper att rikta investeringarna i informationssäkerhet.

Tjänsteleverantören ska planera styrdokumenterna om informationssäkerhet enligt sina egna risker och behov. Till exempel en informationssäkerhetsgrupp eller en annan tillräckligt omfattande enhet inom organisationen bereder dokumenten som ledningen godkänner. Den aktör som berett dokumenten kan också ansvara för deras publicering och en ändamålsenlig informering om dem till alla medarbetare inom organisationen. Styrdokumenterna ska vara lättillgängliga för alla medarbetare till exempel via organisationens intranätsidor. Dessutom ska dokumenterna ingå i inskolningsprogrammet för nya medarbetare. Tjänsteleverantören ska se till att iakttagandet av huvudprinciperna för informationssäkerheten i dokumenterna övervakas.

Av styrdokumenterna för informationssäkerhet bör följande ärenden framgå vad gäller företagets verksamhet inom identifieringstjänster och utfärdandet av kvalificerade certifikat:

- informationssäkerhetsmål
- ansvar för informationssäkerheten
- informationssäkerhetsorganisation
- metoder för upprätthållande och utveckling av organisationens egen informationssäkerhet till exempel vad gäller interna revisioner.

Tjänsteleverantören ska skriftligt dokumentera hur följande specialområden har beaktats i praktiken och genomförts i den mån som de är lämpliga på identifieringstjänster och utfärdande av kvalificerade certifikat:

- Personalsäkerhet
  - Ansvar och skyldigheter i anslutning till personalens informationssäkerhet.
  - Personalens informationssäkerhetskompetens och utveckling av den.
  - Kartläggning av nyckelpersonsrisiker genom eventuella bakgrundskontroller.
  - Förebyggande av ansvars- och uppgiftshelheter som är farliga för tillhandahållandet av tjänsten.
  - Anvisningar för förfarandet när arbetsförhållandet slutar.
- Fysisk säkerhet
  - Förhindrande av obehörigas tillträde till lokaliteterna.
  - Övervakning av tillträde till utrymmen.
  - Strävan efter förebyggande av brand-, vatten-, el- och ventilationsskadorna i systemen.
- Maskinvaru- och programvarusäkerhet
  - Tillräcklig dokumentation för att korrigera upptäckta sårbarheter.
  - Tillgång till reservdelar.
  - Allmän hanteringsprocess för ändringar av systemen.
- Telekommunikationssäkerhet
  - Ombesörjning av tillräcklig informationssäkerhetsnivå i nätet med t.ex. krypteringsmetoder vid koppling till öppna och otillförlitliga nät
  - Säkerställande av konfidentialitet och integritet hos meddelanden som förmedlas
  - Ombesörjning av tillräcklig accesskontroll av nätet till exempel med brandväggar.

- Datamaterialsäkerhet
  - Säkerställande av informationens konfidentialitet, integritet och användbarhet: hur klassificeras informationen och hur instrueras personalen i hanteringen av informationen.
- Driftssäkerhet
  - Ansvar för registret för användarrättigheter: delning, ändring, och radering av användarrättigheter.
  - Förebyggande av att användarrättigheter samlas på hög.
  - Förhindrande av att utomstående kommer åt den hanterings- och konfigurationsinformation som anknyter till tillhandahållandet av tjänsterna.
- Ingripande i kränkningar och missbruk av informationssäkerheten
  - Verksamhetsansvar för att upptäcka betydande händelser i informationssäkerheten och ingripande i dem.
  - Verksamhetsanvisningar och processer för återhämtning från informationssäkerhetsproblem.
  - Bedömning av hotets allvar.
  - Anmälan till myndigheter.
  - Meddelanden om avvikelser.
  - Verksamhet efter avvikelser.
  - Missbruk och underlåtenhet att iaktta instruktioner från personalens sida.

Tjänsteleverantören ska därtill fastställa tillräckligt detaljerade anvisningar för enskilda rutiner som är väsentliga för informationssäkerheten. I praktiken innebär detta fastställande av detaljerade anvisningar bland annat för hanteringen av personuppgifter.

I avtal om anlitan­de av underleverantörer/underleverantörsfunktioner ska man se till att gränserna för informationssäkerhetsansvaret har fördelats tillräckligt noggrant mellan tjänsteleverantören och underleverantören. Det totala ansvaret för tjänsternas informationssäkerhet innehas dock alltid av tjänsteleverantören oberoende av om funktioner har lagts ut eller inte.

I underleverantörsavtal finns det skäl att införa hänvisningar till förpliktande bestämmelser gällande tillhandahållande av tjänsten och sanktioner för brott mot bestämmelserna.

Försörjningsberedskapscentralen har publicerat rekommendationer [3], som man kan hänvisa till vad gäller hanteringen av verksamhetens kontinuitet. Dessa rekommendationer handlar om:

- ledning
- styrning av verksamheten
- personal och hantering av personalresurser
- partnerskap
- utvärdering av hanteringen av verksamhetens kontinuitet.

### 3.2.3 Riskhantering

En av de viktigaste komponenterna i hanteringssystemet för informationssäkerhet är en effektiv riskhantering. Med detta avses i allmänhet identifiering av betydande risker i anslutning till företagets affärsverksamhet, bedömning och åtgärdande av riskerna efter att de identifierats samt övervakning av genomförandet av åtgärderna. Den viktigaste uppgiften för hanteringssystemet är att skydda organisationen och dess förmåga att utföra sina fastställda uppgifter under normala förhållanden, störningar under normala förhållanden och undantagsförhållanden med beaktande av ekonomiska faktorer. Riskhantering kan utgöra en del av företagets förberedelse- eller kontinuitetsplanering.

Målsättningen för riskhanteringen är bland annat att:

- snabba upp återhämtningen från informationssäkerhetsproblem
- minska kostnader och skador som informationssäkerhetsproblemen förorsakar
- rikta investeringar som förbättrar informationssäkerheten
- förbättra tjänstens kvalitet och produktivitet
- ekonomiskt optimera de risker som hänför sig till tjänsten
- förebygga riskerna mot tjänsten.

Genom kraven på riskhanteringen strävar man efter att säkerställa att tjänsteleverantören är medveten om följderna om riskerna realiserar och huruvida de riskminskande åtgärderna är tillräckliga.

Bland annat följande standarder och publikationer har utarbetats om riskhanteringen:

- ISO/IEC TR 13335-3, Information technology - Guidelines for the management of IT Security - Techniques for the management of IT Security. [4],
- ISO/IEC 27005:2008 Information technology - Security techniques - Information security risk management [5],
- NIST Special Publication 800-30, Risk Management Guide for Information Technology Systems, Recommendations of the National Institute of Standards and Technology [6],
- Enisa: Risk Management: Implementation principles and Inventories for Risk Management/Risk Assessment methods and tools [7],
- COSO ERM (Enterprise Risk Management - Integrated Framework (2004)) [8],
- BS 31100:2008, Risk management. Code of practice [9],
- ISO 31000 Risk management -- Principles and guidelines [10],
- The Institute of Risk Management (IRM), Risk Management Standard [11]
- PK-RH: riskhantering i små och medelstora företag [12].

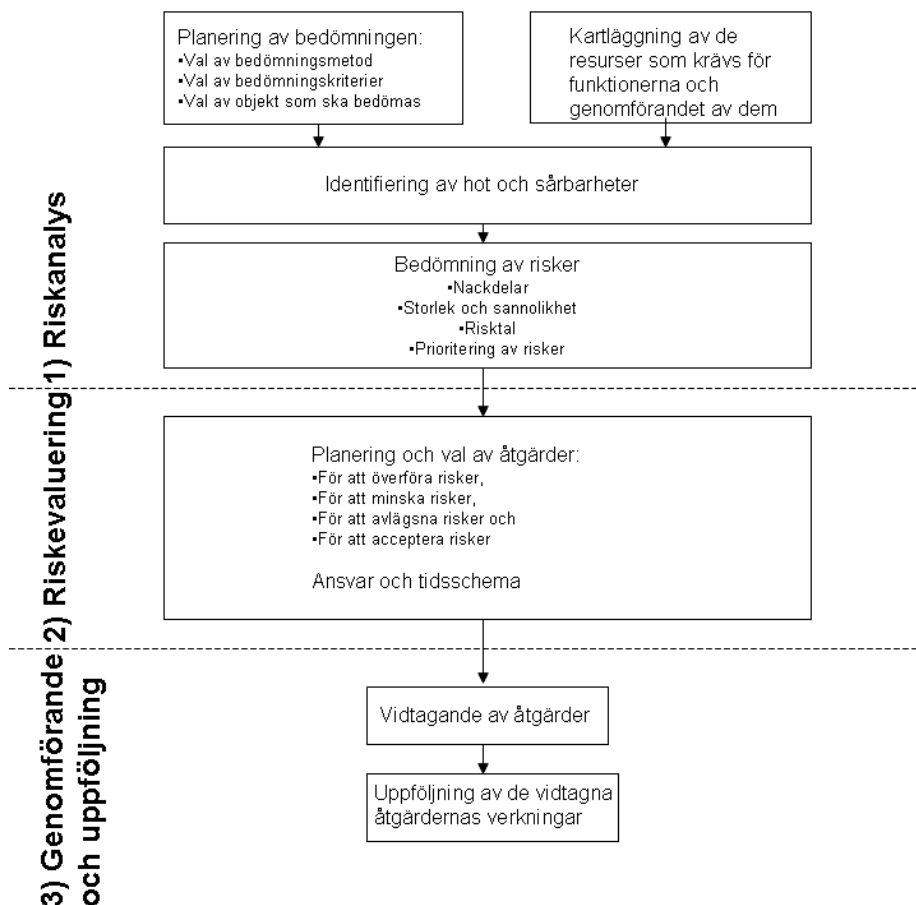
I denna föreskrift ställs inga skyldigheter på iakttagandet av en viss standard. Riskhanteringsmodellerna varierar mellan företagen, och det finns inte en enda modell som skulle passa varje företag. Det viktiga är att sammankoppla målen för företagets riskhanteringssystem med målen för dess verksamhet och se till att de stöds av företagets ledning.

Minimikraven för riskhanteringen kan anses vara att:

- Tjänsteleverantören har klassificerat de med tanke på den tillhandahållna tjänsten viktigaste och mest kritiska funktionerna, processerna och systemen.
- Informationssäkerhetsriskerna i anslutning till tillhandahållandet av tjänsten har kartlagts.
- Tjänsteleverantören regelbundet följer upp informationssäkerhetsnivån i anslutning till den tillhandahållna tjänsten. Informationssäkerhetsnivån kan följas upp till exempel med stickprov, informationssäkerhetsinspektioner och informationssäkerhetsrevisioner.

Informationssäkerhetsriskerna i anslutning till tillhandahållandet av tjänsten ska kartläggas vad gäller de för den tillhandahållna tjänsten viktigaste och mest kritiska funktionerna, processerna och systemen, och åtgärderna för att minimera, avlägsna och överföra riskerna ska dokumenteras.

Riskhanteringen kan grovt indelas i tre olika faser:



### 3.2.3.1 Riskanalys

Med riskanalys avses de systematiska åtgärder genom vilka man strävar efter att identifiera hot och sårbarheter för informationssäkerheten som äventyrar genomförandet av tjänsten, samt att bedöma följderna av de hot som eventuellt realiseras. Riskanalysen ska planeras, genomföras och dokumenteras omsorgsfullt. Riskanalysen borde göras upp i relation till en på förhand fastställd

målnivå. Med detta avses till exempel krav på tjänstens tillgänglighet enligt Kommunikationsverkets föreskrift eller ett kundavtal. Genom riskanalysen strävar man i synnerhet efter att identifiera de hot som äventyrar uppnåendet av de mål som ställts på föremålet.

Riskanalysen består av fem delområden:

- planering av utvärderingen
- identifiering av informationssäkerhetshot som äventyrar tjänsten
- identifiering av utsatta system och funktioner
- bedömning av riskernas storlek och sannolikhet
- prioritering av risker.

De viktigaste målsättningarna för riskanalysen är att:

- stödja informationssäkerhetsledningen och styra investeringarna
- förbättra informationssäkerheten
- identifiera de informationssäkerhetsrisker som inverkar på tjänstens funktion och deras storlek.

På grund av målsättningarna för riskanalysen borde de som utför analysen ha god kännedom om den verksamhet som objektet för riskanalysen bedriver, om målen för dess verksamhet samt om de krav som ställs på verksamheten.

### **Planering av riskbedömningen**

Planeringen av riskbedömningen ska omfatta de använda metoderna för riskbedömningen, kriterierna för riskbedömningen och objekten för bedömningen samt de ämnesområden som bedömningen riktar sig till.

Vid planeringen av bedömningen är det motiverat att beakta den erbjudna tjänstens omfattning och organisationens möjligheter. Minimikravet på planeringen av riskbedömningen är dock att även de förenklade bedömningsmetoderna är dokumenterade.

Vid riskbedömningen lönar det sig att utnyttja till exempel tidigare informationssäkerhetsgranskningar, "nära ögat"-situationer och annat informationssäkerhetsmaterial.

Tjänsteleverantören ska säkerställa att de personer som deltar i bedömningen är tillräckligt förtrodda med den använda riskbedömningsmetoden.

I planeringsskedet ska man också komma överens om registreringen, lagringen och hanteringen av bedömningens resultat.

### **Kartläggning av funktionerna och de resurser som behövs för genomförandet av dem**

Grundförutsättningen för identifieringen av systemen och funktionerna är att kartläggningen av de för den tillhandahållna tjänsten centrala systemen och funktionerna har gjorts åtminstone vad gäller följande delområden:

- utrustningsutrymmen
- maskinvara och programvara
- telekommunikationsförbindelser
- datamaterial
- systemens underhålls- och stödpersoner.

Kartläggningen förbättrar tjänsteleverantörens möjligheter att bedöma hur kritiska och känsliga datasystemen och de hanterade uppgifterna är och vilka resurser som behövs. Dessutom gör kartläggningen det lättare att rikta de informationssäkerhetsfrämjande åtgärderna.

### **Identifiering av hot**

Med hot avses i detta sammanhang en situation som äventyrar tjänstens funktion och vars sannolikhet eller storlek inte har bedömts. Definitionen av hot beror på det valda riskanalysobjektet och avgränsningen. Vid definitionen av hot ska man utnyttja resultaten av de informationssäkerhetsrevisioner som gjorts på riskanalysobjektet samt tidigare realiserade risker eller informationssäkerhetsavvikelser. Informationssäkerhetsrevisionerna kan genomföras antingen som interna revisioner eller köpas av utomstående tjänsteleverantörer. Vi rekommenderar att revisioner görs, beroende på objektets kritiskhet, med 6 till 24 månaders mellanrum och alltid då betydande förändringar inträffar i det bedömda objektet.

Realiseringen av hotet anknyter alltid till en sårbarhet, dvs. utsatthet för en faktor som hotar tjänsten. Sårbarheterna kan antingen vara tekniska eller icke-tekniska, och de kan till exempel anknyta till:

- maskinvara och programvara
- processer
- personal.

Med hot som anknyter till maskinvara och programvara avses till exempel att ett skadeprogram förhindrar apparatens eller programvarans funktion.

Med hot som anknyter till processer kan man till exempel avse dröjsmål i återhämtningen från ovan nämnda skadeprogram. Sårbarheten kan till exempel bero på avsaknaden av överenskomna rutiner.

Hot som anknyter till personalen kan vara att en viss tjänst saknar ansvarig person. Exempel på den här sårbarheten är att den ansvariga insjuknar eller säger upp sig.

## **Riskbedömning**

Med riskbedömning avses bedömning av storleken på en identifierad risk och sannolikheten för att den realiserar.

De analyserade riskerna kan prioriteras till exempel enligt risktalet som kan vara hotets storlek multiplicerat med hotets sannolikhet. Prioriteringen av risker enligt deras inverkan på affärsverksamheten är en allmänt använd metod, i synnerhet i större företag. Det som är viktigt är emellertid att de upptäckta riskerna har klassificerats på något sätt så att de tillgängliga resurserna kan inriktas på de mest allvarliga riskerna.

Klassificeringen av riskerna fungerar som en rekommendation, som stödjer beslutsfattandet när man planerar och riktar korrigerande åtgärder.

### **Dokumentation:**

Dokumentationen ska innehålla sådana uppgifter utifrån vilka man i efterhand kan bedöma genomförandet av riskhanteringen samt riskkartläggningens och åtgärdernas tillräcklighet.

Dokumentationen ska omfatta åtminstone följande områden:

- riskanalys
  - målsättningar för riskanalysen
  - avgränsningar av riskanalysen
  - resultat av riskanalysen
  - slutrapport om riskanalysen.
  
- riskevaluering
  - lista över de största riskerna
  - lista över de mest kritiska bristerna.

### **3.2.3.2 Riskevaluering**

Vid riskevaluering lyfter man fram de viktigaste utvecklingsbehoven utifrån riskbedömningens resultat. Av detta sammandrag av riskbedömningen framgår bland annat:

- de största riskerna
- de mest kritiska bristerna
- föremålen för tilläggsutredningar.

### **Planering och val av åtgärder**

Vid valet av informationssäkerhetsåtgärder utifrån riskanalysen finns det skäl att beakta kostnaderna för lösningarna, personalresurserna, företagets risktagningens vilja och de förluster som uppkommer genom att risken realiserar.

Om en betydande risk inte kan avlägsnas helt och hållet ska tjänsteleverantören göra upp en återhämtningsplan för den eventualitet att risken realiserar.

Kostnaderna för en realiserad risk kan också överföras till en tredje part till exempel genom försäkringar eller avtal. Tjänsteföretaget bär dock det totala ansvaret för tjänstens informationssäkerhet om risken realiserar.

Risker med liten inverkan kan ofta accepteras om riskerna inte strider mot lagstiftning och bestämmelser. Om flera obetydliga risker realiserar samtidigt kan situationen dock förändras väsentligt till exempel vad gäller den tillhandahållna tjänstens kvalitet. När beslut om att acceptera risker fattas ska man från fall till fall beakta ur vilket perspektiv och under vilka förhållanden risken kan accepteras samt de följder och kostnader som uppkommer genom att risken realiserar.

Ägaren till en verksamhet eller tjänst ska se till att riskerna accepteras. Beslut om att acceptera risker fattas i enlighet med företagets beslutsfullmakter.

### **3.2.3.3 Genomförande och uppföljning**

En plan ska uppgöras för de valda informationssäkerhetsfrämjande åtgärderna, och i den ska man bland annat fastställa de ansvariga personerna för de åtgärder som man beslutat vidta samt för genomförandet av och tidsschemat för uppföljningen av dem.

Exempel på informationssäkerhetsfrämjande åtgärder vad gäller avlägsnande av risker är:

- undvikande av vissa produkter, protokoll eller metoder
- undvikande av diffusa avtalspartner
- nedläggande av verksamhet med alltför stora risker.

Exempel på informationssäkerhetsfrämjande åtgärder vad gäller minskning av risker är:

- personalutbildning i informationssäkerhet
- verksamhetsdirektiv
- införande av informationssäkerhetsfrämjande produkter
- reservsystem
- uppdaterade säkerhetskopior
- säkerhetsklassificering av dokumentationen
- passagekontroll.

Upptäckt av risker kan förbättras till exempel genom regelbundna revisioner av objekten, införande av riskhantering i produktutvecklingen i ett så tidigt skede som möjligt, främjande av personalens medvetenhet om informationssäkerhet och anvisningar för rapportering i problemsituationer.

Till exempel personalrisker kan förebyggas med hjälp av ersättare och datasystemrisker med hjälp av reservsystem.

Tjänsteleverantören ska definiera detaljerade och tillräckliga anvisningar för enskilda rutiner som är väsentliga för informationssäkerheten. Dessa anvisningar kan gälla till exempel följande delområden:

- förfarande vid besök
- hantering av passagerättigheter
- distansanvändning av system för tillhandahållandet av tjänsten
- hantering av känsligt datamaterial (t.ex. kunduppgifter).

Tjänsteleverantören ska använda anvisningar för hantering av datamaterial som är viktigt för den tillhandahållna tjänsten. Anvisningen ska omfatta bland annat följande frågor:

- allmänna principer för bedömning av datamaterialets säkerhetsklass och konfidentialitet samt hemlighållandet av datamaterial
- hanterings- och ändringsrättigheter vad gäller fördelningen av läsrättigheter till datamaterialet, ändringsrättigheter och fördelningen av dessa rättigheter,
- fastställande av konfidentialitetsklass
- offentlighet av uppgifter eller dokument: till exempel rätten att tala om ett ärende offentligt
- dokumentets egenskaper: papper, stämpel och andra märkningar
- förvaring och kryptering
- utskrifter och kopiering
- mottagning, distribution, sändning och transport
- dokumentering av hanteringen av uppgifter och dokument
- arkivering och hantering av dokument eller upphörande av hanteringsrätten samt förstörande av uppgifter och dokument.

Separata användar- eller användargruppspecifika behörigheter att hantera material ska fastställas för allt säkerhetsklassificerat datamaterial. Samtidigt ska man se till att utomstående inte kommer åt säkerhetsklassificerat datamaterial. Säkerhetsklassificerat datamaterial ska dock vara tillgängligt för dem som har rätt att hantera det.

Anvisningen för hantering av tjänsteleverantörens datamaterial kan i tillämpliga delar basera sig på till exempel finansministeriets informationssäkerhetsanvisning för hantering av datamaterial inom statsförvaltningen [13].

Tjänsteleverantören ska se till att datamaterial som är väsentligt för den tillhandahållna tjänstens tillgänglighet har uppdaterade säkerhetskopior, som förvaras i låsta utrymmen och separat från ifrågavarande apparater. Säkerhetskopior ska kunna tas i användning om det ursprungliga datamaterialet skadas till exempel på grund av fel i programvara, apparater eller en olycka i utrustningsutrymmet. Sådant datamaterial består till exempel av användaruppgifter och konfigurationsuppgifter.

### 3.2.4 Upptäckt av och ingripande i missbruk och informationssäkerhetsproblem

Tjänsteleverantören ska kunna reagera på brott och hot mot informationssäkerheten, som å ena sidan inverkar på företagets förmåga att producera tjänster och som å andra sidan väsentligt äventyrar informationssäkerheten för tjänsteleverantörens kunder.

Ingripandet i missbruk av tillhandahållna tjänster samt informationssäkerhetsproblem ska vara organiserat och åtminstone omfatta följande funktioner:

- beredning av anvisningar och processer för ingripande i missbruk och informationssäkerhetsproblem
- uppföljning av respons från kunderna
- rapportering om missbruk och informationssäkerhetsproblem
- ansvar och funktioner för undersökningar och förundersökningar av missbruk och informationssäkerhetsproblem och bedömning av deras storlek
- ansvar och funktioner för begränsning av skador, åtgärdande av missbruk och informationssäkerhetsproblem samt information till den högsta ledningen
- anmälningar till myndigheter till exempel enligt Kommunikationsverkets föreskrift 7 B/2009 M
- ansvar och funktioner för återhämtning från missbruk eller informationssäkerhetsproblem
- funktioner för förebyggande av att händelsen upprepas.

### 3.2.5 Uppföljning av hanteringen av informationssäkerheten

Hanteringen av informationssäkerheten ska vara fortlöpande, reagera på förändringar och utgöra en del av företagets normala verksamhet från planering av tjänster till underhåll.

Organisationens ledning ska se till att det finns tillräckligt med resurser för planering, genomförande, bedömning och upprätthållande av systemet för hantering av informationssäkerheten.

Systemet för hantering av informationssäkerheten ska underhållas regelbundet och uppdateras vid behov. Ändringsbehoven ska granskas en gång om året och alltid vid behov. Behovet av ändringar av hanteringssystemet kan uppstå på grund av till exempel organisationsreformer eller ändringar av företagets strategi. Också ändringar i personalen kan medföra behov av uppdatering av hanteringssystemet. I samband med ändringarna måste man alltid försäkra sig om att informationssäkerhetsrutiner och avtal överensstämmer med varandra.

## 3.3 3 § Inledande identifiering och registrering av sökande

## **Inledande identifiering**

En leverantör av identifieringstjänster och en certifikatutfärdare som tillhandahåller kvalificerade certifikat ska omsorgsfullt verifiera identiteten hos den som ansöker om ett identifieringsverktyg eller kvalificerat certifikat i enlighet med de förutsättningar som ges i lag. Om inledande identifiering av den som ansöker om ett identifieringsverktyg bestäms i 17 § i lagen om stark autentisering och om identifiering av den som ansöker om ett kvalificerat certifikat bestäms i lagens 35 §.

Den inledande identifieringen ska göras i samband med att en sökande vill skaffa ett identifieringsverktyg eller ett kvalificerat certifikat. Inledande identifiering kan alltså inte göras i förväg, ifall kunden en gång vill börja använda identifieringsverktyget. Den inledande identifieringen behöver inte göras på nytt om sökanden har ett identifieringsverktyg som har getts ut av samma tjänsteleverantör och verktyget förnyas eller byts ut mot ett annat. Då kan kunden identifieras elektroniskt med hjälp av det existerande identifieringsverktyget. Med förnyande avses i detta fall inte bara sändning av en ny lista med nyckeltal utan exempelvis utbyte av ett identifieringsverktyg mot ett annat eller förnyande av ett tidsbundet avtal. En ansökan om ett kvalificerat certifikat som utfärdats av Befolkningsregistercentralen kan göras elektroniskt med ett giltigt kvalificerat certifikat med stöd av 68 § i lagen om befolkningsdatasystemet och Befolkningsregistercentralens certifikattjänster.

Den inledande identifieringen av sökanden ska göras personligen. Enligt 17 § 2 mom. i lagen behöver den inledande identifieringen inte göras personligen, om leverantörer av identifieringstjänster sinsemellan har avtalat om möjligheten att lita på varandras inledande identifieringar. Ansökan om identifieringsverktyg kan i så fall också göras elektroniskt, förutsatt att leverantören av identifieringstjänster, som gjort den ursprungliga inledande identifieringen personligen, alltid är den andra parten i avtalet.

En leverantör av identifieringstjänster kan använda ombud vid inledande identifiering. Leverantören av identifieringstjänster bör dock säkerställa ombudets tillförlitlighet, informationssäkerhetsnivå och säkerhet i arbetssättet. Leverantören av identifieringstjänster svarar även till denna del för verksamheten hos de personer som tjänsteleverantören anlitar på det sätt som konstateras i 13 § 4 mom. i lagen om stark autentisering.

I lagen om stark autentisering förutsätts inte att ett identifieringsverktyg eller ett kvalificerat certifikat överlåts till den sökande personligen utan överlåtelsen kan ske på det sätt som anges i avtalet. Identitet hos och övriga uppgifter om den som ansöker om ett identifieringsverktyg eller ett kvalificerat certifikat ska dock granskas omsorgsfullt innan verktyget eller certifikatet första gången överlåts till sökanden. Med övriga uppgifter om sökanden avses här i synnerhet sådana uppgifter som lagrats i identifieringsverktyget eller det kvalificerade certifikatet och som tjänsteleverantören garanterar.

Den som ansöker om ett identifieringsverktyg eller ett kvalificerat certifikat ska också identifieras om sökanden är minderårig eller på något annat sätt omyndig. I så fall måste sökanden vara personligen närvarande. Överlåtelse av verktyget kan dock förutsätta intressebevakarens samtycke eller närvaro. Denna föreskrift förutsätter inte att identifieringsverktygets eller det kvalificerade certifikatets giltighetstid upphör efter det att intressebevakarens uppdrag har avslutats (t.ex. när ett barn har blivit myndigt), men det är skäl att ha en sådan praxis i synnerhet om det är möjligt att definiera en giltighetstid för verktyget.

Enligt 17 § i lagen om stark autentisering ska den som ansöker om ett identifieringsverktyg identifieras med hjälp av ett giltigt pass eller identitetskort som har utfärdats av en myndighet i en medlemsstat inom Europeiska ekonomiska samarbetsområdet, i Schweiz eller i San Marino. Vid den inledande identifieringen får leverantören, om denne så önskar, även använda ett giltigt körkort som har utfärdats efter den 1 oktober 1990 av en myndighet i en medlemsstat i Europeiska ekonomiska samarbetsområdet eller ett giltigt pass som har utfärdats av en myndighet i någon annan stat. Dokument som godkänns vid den inledande identifieringen ska nämnas i tjänsteleverantörens principer för identifiering.

Med identitetskort som har utfärdats av en myndighet i någon annan stat än i Finland avses i lagen endast identitetskort som kan användas som resehandling.

Pass som avses i lagen om stark autentisering är alla vanliga pass och diplomatpass. Det är närmast främlingspass och resedokument för flykting som kan vara problematiska vid identifieringen. Både främlingspass och resedokument för flykting är handlingar som utfärdats av finska myndigheter, men de används primärt inte för att verifiera identitet hos en person utan de används som ett resedokument. Båda typer av handlingar kan utfärdas utgående från att den sökandes identitet kan verifieras på ett tillförlitligt sätt eller att identiteten inte har kunnat säkerställas. Om identiteten hos en innehavare av ett främlingspass eller resedokument för flykting har säkerställts, kan leverantören av identifieringstjänsten, om denne så önskar, också använda handlingen för inledande identifiering. Om identiteten inte har kunnat säkerställas på ett tillförlitligt sätt, förses främlingspasset eller resedokumentet för flykting med en anteckning om detta (identitet inte fastställd). Om främlingspasset eller resedokumentet för flykting har en anteckning om att innehavarens identitet inte har kunnat fastställas, ska dokumentet inte heller användas för inledande identifiering i enlighet med lagen om stark autentisering.

Körkort används för tillfället ganska allmänt för att påvisa identitet, men det finns problem i att godkänna körkortet som en handling för att verifiera identitet. Processen för beviljande av körkort är inte på samma nivå som pass och personkort, och körkortens säkerhetsfaktorer är ringa. Att körkort som utfärdats utomlands och körkort som byts ut för utlänningarna i Finland godkänns som identitetsbevis kan anses vara synnerligen problematiska. En utländsk person får, enligt internationella vägtrafikavtal, byta ut sitt körkort till ett finskt körkort efter ett års vistelse i Finland. En person, vars identitet inte har kunnat fastställas även om en anteckning om detta finns

i hans eller hennes resedokument, kan byta ut sitt körkort till ett finskt körkort utan att uppgift om att personens identitet är osäker antecknas i körkortet. Det nya körkortet kan sedan användas för att verifiera identitet. Kommunikationsverket uppmanar tjänsteleverantörerna att bedöma risker som godkännande av körkort orsakar och vara kritiska mot sådana körkort vars fält för specialvillkor visar att kortet har bytts ut (fält nr 12, kod 70 och landskod från senaste land).

Om tjänsteleverantören på ett tillförlitligt sätt inte kan identifiera den som ansöker om ett identifieringsverktyg eller ett kvalificerat certifikat eller ett dokument, kan tjänsteleverantören begära att polisen identifierar sökanden. Polisen identifierar sökanden och skickar ett intyg av sökandens identitet till leverantören av identifieringstjänster som rekommenderat brev. Sökanden måste ha med sig två foton, dokument som eventuellt bidrar till identifieringen samt kontaktuppgifter om tjänsteleverantören till vilken intyget om identifieringen skickas. Alternativt kan den som ansöker om ett identifieringsverktyg skaffa sig ett temporärt identitetskort hos polisen.

I lagens 35 § uppges inte några dokument genom vilka identiteten hos den som ansöker om ett kvalificerat certifikat kan kontrolleras på ett tillförlitligt sätt. Dokument som nämns i lagens 17 § kan anses vara tillförlitliga dokument.

### **Lagring av uppgifter**

En leverantör av identifieringstjänster ska lagra uppgift om den inledande identifieringen av sökanden och om den handling som använts samt om eventuella hinder och begränsningar för användningen av identifieringsverktyget. Det är nödvändigt att lagra uppgifter till exempel om identifieringsverktyget har getts ut till fel person. Uppgifter som lagras kan vara passnummer eller identitetskortsnummer. Ibland kan det vara nödvändigt att bevara en kopia på den handling som använts. Företag som omfattas av penningtvättslagen måste vid lagringen av uppgifterna beakta de krav som ställs i 10 § i lagen.

Om identifieringsmetoden baserar sig på ett certifikat eller om det är fråga om ett kvalificerat certifikat, ska tjänsteleverantören samla in alla uppgifter som hänför sig till certifikatets datainnehåll. Om ett certifikats minimiinnehåll för leverantörer av identifieringstjänster bestäms i 19 § i lagen om stark autentisering. Om innehållet i ett kvalificerat certifikat bestäms i lagens 30 § 2 mom. Sådana uppgifter kan vara eventuella specialuppgifter som har samband med ett visst användningssyfte för certifikatet, såsom det företag eller den organisation som sökanden representerar samt sökandens befattningsbeskrivning eller position. 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.

Enligt 37 § i lagen om stark autentisering ska en certifikatutfärdare som tillhandahåller kvalificerade certifikat föra register över utfärdade kvalificerade certifikat. Uppgifter som registreras

måste samlas in i samband med registrering av den som ansöker om ett kvalificerat certifikat. I registret införs förutom uppgifter om det kvalificerade certifikatet också uppgifter om sökandens person som är relevanta för utgivningen och upprätthållandet av det kvalificerade certifikatet.

Sådana uppgifter är

- hela namnet (efternamn och förnamn)
- födelsetid och -ort
- personbeteckning eller annan beteckning som identifierar en person
- andra uppgifter som är behövliga t.ex. för att kunna identifiera olika personer med samma namn
- adress och/eller andra kontaktuppgifter.

I certifikatutfärdarens certifikatregister införs också uppgift om datumet när det kvalificerade certifikatet ansöktes om, den inledande identifieringen och anlitade dokument samt övriga uppgifter som är väsentliga för beviljande av det kvalificerade certifikatet. Sådana uppgifter är till exempel begränsningar som gäller användningen av det kvalificerade certifikatet.

### **3.4 4 § Skapande av identifieringsverktyg och kvalificerade certifikat**

Kundens elektroniska identitet och certifikatets datainnehåll baserar sig på de uppgifter man fått i samband med ansökan om ett kvalificerat certifikat eller identifieringsverktyg. En tjänsteleverantör bör säkerställa ansökans ursprung, tillförlitlighet och riktighet.

Identifieringsverktyget och det kvalificerade certifikatet kan skapas bara om ansökan om dem uppfyller villkoren för beviljande av kvalificerat certifikat eller identifieringsverktyg. Det betyder bland annat att identifieringsverktyget eller det kvalificerade certifikatet kan skapas först efter att sökanden har blivit identifierad i enlighet med föreskriftens 3 § och givit de uppgifter som krävs i ansökan.

Med skapande av certifikat avses en process där certifikatutfärdaren kopplar ihop den öppna nyckeln med sökanden och signerar certifikatet med en avancerad elektronisk signatur som framställts av certifikatutfärdarens privata nyckel. Med skapande av identifieringsverktyg som baserar sig på någonting annat än certifikat avses att identifieringsverktyget kopplas ihop med sökanden.

Tjänsteleverantören ska lagra uppgifter om att ett identifieringsverktyg och ett kvalificerat certifikat har skapats. Om tjänsteleverantören själv skapar nycklarna ska uppgifter om detta också lagras. På basis av dessa uppgifter ska det efteråt vara möjligt att kunna utreda tidpunkten för när identifieringsverktyget eller det kvalificerade certifikatet skapades och hur sökanden i detta fall har blivit identifierad.

Tjänsteleverantören ska på ett tillräckligt sätt säkerställa att endast innehavaren av ett identifieringsverktyg eller kvalificerat certifikat kan använda det. Sådana sätt är till exempel någonting som endast innehavaren av verktyget vet (t.ex. en PIN-kod) eller är (biometriska kännetecken).

Algoritmer och nycklar som använts vid identifieringsmetoden, det kvalificerade certifikatet och skapandet av nycklarna ska vara trygga och överensstämna med allmänt godkända standarder eller rekommendationer. Sådana standarder utfärdas bland annat av NIST [14], ANSI [15], ISO [16] och VAHTI-gruppen [17].

### **3.5 5 § Distribution av certifikat**

Föreskriftens 5 § tillämpas på certifikatutfärdare som utfärdar kvalificerade certifikat samt på de leverantörer av identifieringstjänster vars identifieringsmetod baserar sig på ett certifikat.

Tjänsteleverantören ger ut uppgifter som behövs för identifiering och signering, dvs. den privata nyckeln och de koder som används för att skydda nyckeln endast till innehavaren av verktyget. Utdelningen av de data som används vid verifiering av signatur och identitet, dvs. certifikatet och med det anslutna öppna nyckeln, ska arrangeras så att de är tillgängliga för alla som förlitar sig på certifikatet och med det framställda elektroniska signaturen eller identifieringen. Tjänsteleverantören kan använda t.ex. en offentlig katalogtjänst som utdelningskanal för certifikaten. En sådan katalogtjänst ska vara tillgänglig dygnet runt. Tjänsteleverantören och innehavaren av certifikatet kan komma överens om att innehavaren av certifikatet ställer datainnehållet i certifikatet tillgängligt för alla som förlitar sig på certifikatet.

Tjänsteleverantören får inte kopiera hemliga uppgifter som hänför sig till verktyget, eftersom endast den sökande bör veta om eller ha tillgång till dem. Sådana uppgifter är till exempel privata nycklar som hör samman med certifikat och finns lagrade på kort.

Distribution av uppgifter som hänför sig till skapande av certifikat och signaturer eller till identifieringshändelsen bör genomföras så att:

- privata och hemliga nycklar inte utdelas i läsbar form
- öppna men fortfarande overifierade nycklar förvaras på ett tryggt sätt t.ex. för att hindra manipulering
- certifikatutfärdaren och certifikatinnehavaren kommer överens om hur certifikatets datainnehåll hålls tillgängligt för tredje parter som förlitar sig på certifikatet och detta avtal sätts in i förvar.

### **3.6 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. I certifikatpolicyn beskrivs bland annat certifikatutfärdarens förfaringsätt, begränsningar för användning av certifikatet samt certifikatutfärdarens och undertecknarens skyldigheter. I policyn beskrivs även de uppgifter som den som förlitar sig på certifikatet ska kontrollera vid bedömning av certifikatets tillförlitlighet. I certifieringsstandard (CPS) beskrivs närmare hur kraven på certifikatpolicy genomförs i certifikatutfärdarens verksamhet. I principerna för identifiering anges hur leverantören av identifieringstjänster uppfyller de skyldigheter som avses i lag. Allmänt tillgänglig betyder exempelvis publicering av handlingarna på tjänsteleverantörens webbplats.

Parternas informationssäkerhets- och certifikatpolicy, principer för identifiering samt informationssäkerhetsrutiner och certifieringsstandard ska motsvara varandra vid krosscertifieringen. Det betyder bland annat att en certifikatutfärdare som utfärdar starka identifieringsverktyg inte kan krosscertifiera en certifikatutfärdare som utfärdar identifieringsverktyg som inte är starka. Med krosscertifiering avses att två certifikatutfärdare kan certifiera varandras öppna nycklar.

### **Återkallande av identifieringsverktyg och kvalificerade certifikat och kontroll av deras giltighet**

Parter som förlitar sig på ett certifikat och en signatur som framställts med hjälp av det eller på identifiering ska kunna kontrollera det kvalificerade certifikatets eller identifieringsverktygets giltighet med hjälp av en spärmlisttjänst. Tjänsten kan ske i realtid eller den kan uppdateras med jämna mellanrum.

Återkallande av ett identifieringsverktyg och ett kvalificerat certifikat bör genomföras så att:

- Identifieringsverktyget spärras och certifikatet ställs på spärmlista antingen på begäran av innehavaren eller om det finns andra särskilda skäl för det. Grunderna för spärrning av ett identifieringsverktyg av en annan orsak än på begäran av innehavaren ges i 26 § i lagen som gäller stark autentisering och kvalificerade certifikat.
- Ursprung och riktighet av begäran om återkallande, avbrott och återkallande av avbrott kontrolleras på ett tillräckligt tillförlitligt och omsorgsfullt sätt. Tjänsteleverantören kan spärra verktyget också om den har skäl att misstänka att verktyget har använts obehörigt eller säkerheten vid användningen av verktyget har äventyrats.
- Återtagning av ett återkallat identifieringsverktyg och kvalificerat certifikat hindras.
- Återkallande av signaturnycklar för certifikat och systemnycklar är möjligt bara under tillsyn av två personer.
- Återkallande av identifieringsverktyg och kvalificerade certifikat uppdateras i certifikatutfärdarens databas utan dröjsmål efter att ansökan om återkallande har behandlats.

- Om uppgifterna om återkallade certifikat offentliggörs på en spärrlista, ska uppgift om återkallande av ett certifikat publiceras på listan antingen genast eller i enlighet med en bestämt regelbunden uppdatering – dock senast inom 24 timmar efter att certifikatutfärdaren fått begäran om återkallande eller avbrott.
- Uppdaterad spärrlista publiceras regelbundet oberoende av om den innehåller ändringar eller inte.
- De av certifikatutfärdaren använda tillförlitliga system kan återkalla alla kvalificerade certifikat som certifikatutfärdaren har utfärdat.
- Tjänsteleverantören underrättar innehavaren av identifieringsverktyget eller det kvalificerade certifikatet om återkallandet av verktyget eller certifikatet.  
Tjänsteleverantören ska alltid underrätta innehavaren av identifieringsverktyget eller det kvalificerade certifikatet om att identifieringsverktyget har återkallats eller användningen av det förhindrats i enlighet med lagens 26 § samt om att det kvalificerade certifikatet har återkallats. Detta kan göras till exempel genom ett SMS-meddelande, ett meddelande som ges när man loggar in i identifieringstjänsten och per brev. Det lönar sig att använda flera kommunikationskanaler. Om innehavaren av identifieringsverktyget eller det kvalificerade certifikatet själv anhåller om återkallande, är ett separat meddelande inte nödvändigt.
- Certifikatutfärdaren undertecknar alla spärrlistor eller svar på förfrågningar om certifikatens spärrstatus med sin avancerade elektroniska signatur och svaret innehåller tidpunkten för signaturen (tidpunkten kan vara tidpunkten för signaturen i den uppbyggda spärrlistan eller tidpunkten för ett realtidssvar på förfrågningar om spärrlistan).
- Alla följande händelser registreras i logguppgifterna:
  - anhållan om ändringar av statusen hos identifieringsverktyg och kvalificerade certifikat samt huruvida anhållan blev godkänd eller inte
  - till spärrtjänsten inkommande och från tjänsten utgående meddelanden som inte hänför sig till upprätthållandet
  - eventuella anhållan om kontroll av spärrlistan och svar på förfrågningar om spärrstatus.

### **Certifikatutfärdarens signaturnycklar**

Certifikatutfärdarens signaturnyckel används enbart för signatur av certifikat och möjligen för signatur av spärrlistor och/eller svar på förfrågningar om certifikatens spärrstatus.

Tjänsteleverantören ska se till att certifikatutfärdarens nycklar inte kan tas i bruk igen när nycklarnas livscykel tar slut. Tjänsteleverantörens nycklar används bara under deras tillåtna livstid och giltighetstiden för certifikat med osymmetriska nycklar kontrolleras. Tjänsteleverantörens infrastruktur- och administrationsnycklar byts ut med jämna mellanrum (t.ex. årligen) och utbyte av nycklarna sker på ett tillförlitligt sätt. Tjänsteleverantörens certifikat bör förnyas innan giltighetstiden går ut.

Vid skapande av signaturnycklarna för certifikat bör man använda en kryptografisk modul som för de kvalificerade certifikaten måste uppfylla kraven av nivå 3 i FIPS 140-2 [18] eller kraven enligt Common Criteria i CWA 14167-3 [19]. Nycklarna skapas under tillsyn av två personer.

### **Avsevärda händelser vid tillhandahållandet av tjänsten**

Tjänsteleverantören ska lagra uppgifter om alla händelser som är avsevärda med tanke på tillhandahållandet av tjänsten. Tjänsteleverantören bör säkerställa att i logguppgifterna registreras:

- alla händelser som hänför sig till skapande, avbrott och återkallande av certifikaten och identifieringsverktygen, även sådana certifikat som certifikatutfärdaren utnyttjar i sin verksamhet
- alla händelser som hänför sig till administration av certifikatutfärdarens signaturnycklar
- alla meddelanden som gäller registreringstjänst, certifikatens distribution och tillvalstjänster även om de inte hänför sig till administration av systemet
- igångsättning och avställning av loggsystemet
- ändring av inställningarna i loggsystemet.

### **Hindrande av obehörig användning**

Tjänsteleverantören ska säkerställa att hemliga uppgifter som hänför sig till verktyget inte under några omständigheter avslöjas förrän de har överlåtit till innehavaren. Ett exempel på sådana uppgifter är PIN-kod som skyddar användningen av verktyget. Ifall man behöver öppna ett låst verktyg ska tjänsteleverantören med tillräckliga åtgärder säkerställa att uppgifterna inte avslöjas för andra. Exempel på sådana åtgärder är säkerhetskuvert, skrapytor eller separata bakgrundssystem. Ett sådant bakgrundssystem kan vara ett system där kunden vid tjänsteleverantörens betjäningsspunkt loggar sig in i självbetjäningssportalen med ett engångslösenord som är giltigt för en viss tid och ställer in de nya PIN-koderna i identifieringsverktyget eller det kvalificerade certifikatet.

### **3.7 7 § Upphörande av verksamhet**

En leverantör av identifieringstjänster ska utan onödigt dröjsmål underrätta Kommunikationsverket, alla de samarbetsparter och personer som den anlitar i identifieringsverksamheten (t.ex. underleverantörer), innehavare av identifieringsverktyg och tjänsteleverantörer som använder identifieringstjänster om att verksamheten upphör. Kommunikationsverket ska underrättas skriftligen i enlighet med 10 § i lagen om stark autentisering.

Leverantören av identifieringstjänster måste också minimera den olägenhet som upphörandet av verksamheten vållar innehavare av identifieringsverktyg och tjänsteleverantörer som använder

identifieringstjänster. Leverantören av identifieringstjänster ska, i mån av möjlighet, se till att uppgifterna till exempel om identifieringshändelser och identifieringsverktyg förvaras på ett behörigt sätt vid upphörandet av verksamheten.

En certifikatutfärdare som tillhandahåller kvalificerade certifikat ska utan onödigt dröjsmål underrätta Kommunikationsverket, alla samarbetsorganisationer (t.ex. andra certifikatutfärdare) och personer som anlitas (t.ex. underleverantörer) samt innehavare av kvalificerade certifikat om att certifikatverksamheten upphör. Certifikatutfärdaren ska också minimera den olägenhet som upphörandet vållar innehavare av kvalificerade certifikat och dem som förlitar sig på de kvalificerade certifikaten. Till Kommunikationsverket ska anmälan göras skriftligen.

Certifikatutfärdaren som tillhandahåller kvalificerade certifikat måste också avsluta sina underleverantörers verksamhet så att nya certifikat inte utfärdas och nya ansökningar inte tas emot efter att certifikatutfärdarens verksamhet har upphört. Certifikatutfärdaren som tillhandahåller kvalificerade certifikat ska, i mån av möjlighet, se till att uppgifterna som lagrats i certifikatregistret också förvaras vid upphörandet av verksamheten. Certifikatutfärdaren måste ha tillräckliga ekonomiska resurser eller försäkringar för att täcka kostnaderna föranledda av förvaringen av uppgifterna.

Informationssäkerhetsrutiner eller certifieringsstandard hos certifikatutfärdaren som tillhandahåller kvalificerade certifikat måste innehålla uppgifter om de åtgärder som tillämpas vid upphörandet av verksamheten. Av handlingarna måste framgå åtminstone följande åtgärder:

- hur undertecknare och certifikatutfärdarens samarbetspartner och de som förlitar sig på certifikaten informeras om upphörandet av verksamheten
- hur certifikatutfärdarens ansvar överförs till andra instanser
- hur gällande kvalificerade certifikat och i synnerhet uppgifterna på spärllistan hanteras.

#### **4 REFERENSLISTA**

[1] Lag om stark elektronisk autentisering och elektroniska signaturer (617/2009), uppdaterad version

<http://www.finlex.fi/sv/laki/ajantasa/2009/20090617>

[2] Information Security Management - Specification With Guidance for Use

<http://www.iso.org/iso/home.htm>

[3] Försörjningsberedskapscentralen: Avtalsbaserad beredskap inom informationssamhällssektorn

[http://www.huoltovarmuus.fi/documents/3/SOPIVA\\_julkaisu.pdf](http://www.huoltovarmuus.fi/documents/3/SOPIVA_julkaisu.pdf) (på finska)

[4] ISO/IEC TR 13335-3, Information technology - Guidelines for the management of IT Security - Techniques for the management of IT Security

<http://www.iso.org/iso/home.htm>

[5] ISO/IEC 27005:2009 Information technology - Security techniques - Information security risk management

<http://www.iso.org/iso/home.htm>

[6] NIST Special Publication 800-30, Risk Management guide for Information Technology Systems, Recommendation of the National Institute of Standards and Technology

<http://csrc.nist.gov/publications/nistpubs/800-30/sp800-30.pdf>

[7] Enisa: Risk Management: Implementation principles and Inventories for Risk Management/Risk Assessment methods and tools

[http://www.enisa.europa.eu/rmra/files/D1\\_Inventory\\_of\\_Methods\\_Risk\\_Management\\_Final.pdf](http://www.enisa.europa.eu/rmra/files/D1_Inventory_of_Methods_Risk_Management_Final.pdf)

[8] COSO ERM (Enterprise Risk Management - Integrated Framework (2004))

<http://www.coso.org/-ERM.htm>

[9] BS 31100:2008, Risk management. Code of practice.

<http://www.bsi-global.com/en/Shop/Publication-Detail/?pid=00000000030191339>

[10] ISO 31000 Risk management -- Principles and guidelines

[http://www.iso.org/iso/iso\\_catalogue/catalogue\\_tc/catalogue\\_detail.htm?csnumber=43170](http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=43170)

[11] The Institute of Risk Management (IRM), Risk Management Standard

<http://www.theirm.org/publications/PUstandard.html>

[12] PK-RH: riskhantering för små och medelstora företag

[www.pk-rh.fi/riskilajit/tietoriskit/tietoriskit](http://www.pk-rh.fi/riskilajit/tietoriskit/tietoriskit) (på finska)

[13] Finansministeriet: finansministeriets informationssäkerhetsanvisning för statsförvaltningens informationsmaterial

[http://www.vm.fi/vm/fi/04\\_julkaisut\\_ja\\_asiakirjat/01\\_julkaisut/05\\_valtionhallinnon\\_tietoturvallisuus/3386/3388\\_fi.pdf](http://www.vm.fi/vm/fi/04_julkaisut_ja_asiakirjat/01_julkaisut/05_valtionhallinnon_tietoturvallisuus/3386/3388_fi.pdf) (på finska)

[14] National Institute of Standards and Technology

<http://www.nist.gov/index.html>

[15] American National Standards Institute

<http://www.ansi.org/>

[16] International Organization for Standardization

<http://www.iso.org/iso/home.html>

[17] Ledningsgruppen för datasäkerheten inom statsförvaltningen

[http://www.vm.fi/vm/sv/13\\_forvaltningsutveckling/09\\_datasakerhet/index.jsp](http://www.vm.fi/vm/sv/13_forvaltningsutveckling/09_datasakerhet/index.jsp)

[18] FIPS 140 Security Requirements for Cryptographic Modules

<http://csrc.nist.gov/groups/STM/cmvp/standards.html#03>

[19] CWA 14167-3 Cryptographic module for CSP key generation services protection profile  
CMSKGPP

<http://www.cen.eu/esearch/>