Transport- och kommunikationsverkets promemoria om åtskillnad mellan stark autentisering och icke-registrerad elektronisk identifieringstjänst

1 Syftet och innehållet i tolkningspromemorian

1.1 Bakgrund och uppdateringen 2020–2021 av den tidigare tolkningspromemorian från 2017

Den 3 oktober 2017 offentliggjorde Kommunikationsverket en tolkningspromemoria om tillhandahållande av identifieringstjänster för stark och svag autentisering (dnr 657/620/2017). Syftet med promemorian var att ge förhandsanvisningar om tolkning av lagen om stark autentisering och betrodda elektroniska tjänster (617/2009, nedan benämnd autentiseringslagen) i situationer där en leverantör av tjänster för stark autentisering också tillhandahåller tjänster för svag autentisering.

År 2017 gällde aktörernas tolkningsfrågor främst huruvida bankerna, när de tillhandahåller identifieringstjänster, i vissa situationer kan låta bli att följa kraven på stark autentisering i gränssnitten för ärendehanteringstjänster.

År 2020 utarbetade Transport- och kommunikationsverket denna nya preciserade tolkningspromemoria om frågan. Till följd av utvecklingen av de elektroniska identifieringstjänsterna har det uppstått behov att precisera tolkningen av vilken åtskillnad mellan stark autentisering och icke-registrerad elektronisk identifiering som är tillräcklig med avseende på autentiseringslagen. De aktuella frågorna gäller framför allt mobilappar och en ändring av en icke-registrerad identifieringsmetod till en stark autentisering.

I denna promemoria har den tidigare termen *svag autentisering* ersätts med termen *icke-registrerad identifiering*. Denna beskriver läget bättre, eftersom metoden inte har anmälts i ett sådant register som avses i autentiseringslagen så att den ska omfattas av myndighetstillsynen.

Den 27 mars 2020 begärde Transport- och kommunikationsverket utlåtanden om utkastet till promemoria. Bifogat till promemorian finns en sammanfattning av utlåtandena och de ändringar som har gjorts utifrån utlåtandena.

1.2 Förhandsanvisningar om de fastställda kraven

Promemorians rättsliga karaktär är anvisning. Det innebär att skyldigheter tolkas vid tillsynen utifrån de fakta som är tillgängliga i enskilda fall och bestämmelserna i lagen och föreskriften. I promemorian anges det på ett tydligt sätt när det är fråga om Transport- och kommunikationsverkets syn på tolkningen av kraven och när det är fråga om en rekommendation.

Kraven i lagstiftningen om stark autentisering gäller alla leverantörer av identifieringstjänster som har anmält sig till Transport- och kommunikationsverket, och leverantörernas tjänster för stark autentisering. Tolkningen av lagstiftningen ska kunna vara tillämplig på likadant sätt på alla nuvarande och kommande finländska eller utländska leverantörer av identifieringstjänster som gör en anmälan i Finland.

Syftet med promemorian är att ge leverantörerna förhandsanvisningar om hur Transport- och kommunikationsverket tolkar de skyldigheter som fastställs i autentiseringslagen, när en leverantör av identifieringstjänster tillhandahåller tjänster för icke-registrerad elektronisk identifiering vid sidan av tjänster för stark autentisering. Promemorian innehåller en granskning av vilken åtskillnad mellan en stark respektive en svag elektronisk identifieringsmetod och system för

tillhandahållande av metoderna som är tillräcklig med avseende på kraven i lagen, så att

- användare av identifieringsmetoder och parter som förlitar sig på en identifiering på ett tydligt sätt kan skilja på en stark autentisering och en icke-registrerad identifiering
- utbudet av tjänster för icke-registrerad identifiering tekniskt sett inte gör att genomförandet av system för stark autentisering försvagas.

I anvisningspromemorian ges exempel, men det är varken möjligt eller ändamålsenligt att försöka förutse alla situationer som rör ett tekniskt genomförande i nuläget eller i framtiden, eller ge anvisningar i sådana situationer.

Den mest typiska exempelsituationen där Transport- och kommunikationsverket har ombetts ge anvisningar är då en identifieringsmetod som används med en mobilapp för identifiering har tillhandahållits genom förfaranden för inledande identifiering på olika tillitsnivåer. Därför handlar exemplen om en sådan situation och framför allt om höjning av tillitsnivån i mobilappen från en icke-registrerad identifieringsmetod till en stark autentisering. Samma principer kan också tillämpas på andra identifieringsmetoder.

1.3 Tillsyn och registrering garanterar tillförlitlighet hos tjänster för stark autentisering

De krav på tillförlitlighet som fastställs i autentiseringslagen gäller identifieringstjänster som i enlighet med autentiseringslagen har anmälts och registrerats i Transport- och kommunikationsverkets register. Tillförlitligheten hos tjänster för stark autentisering bygger i sin tur på myndighetstillsyn. Alla krav i autentiseringslagen gäller som helhet för de identifieringstjänster som har anmälts.

Tjänsteleverantörerna kan tillhandahålla både stark autentisering och icke-registrerad identifiering. Trots autentiseringslagen kan företag eller sammanslutningar i sig tillhandahålla både tjänster för stark autentisering, när de har anmält sig, och icke-registrerade identifieringstjänster som inte omfattas av bestämmelserna i autentiseringslagen.

Enligt autentiseringslagen är det inte möjligt att tillhandahålla en identifieringsmetod med två olika status, både som stark metod och som icke-registrerad metod, utan metoderna ska skiljas från varandra.

Användare av identifieringsverktyg och parter som förlitar sig på en stark autentisering ska kunna lita på att de identifieringstjänster som tillhandahålls av leverantörer av identifieringstjänster och som är införda i Transport- och kommunikationsverkets register uppfyller kraven på identifieringstjänster i alla avseenden. Användarna och parterna ska kunna skilja på starka respektive icke-registrerade identifieringsverktyg och identifieringsmetoder.

Tillförlitligheten hos identifieringstjänster som enligt anmälan tillhandahålls allmänheten får inte försämras av undantag som leverantören av identifieringsverktyg i sina egna tjänster gjort från kraven i autentiseringslagen med stöd av 1 § i lagen.

Bedömningen av avtalsvillkorens tydlighet och skälighet omfattas av de allmänna bestämmelserna om konsumentskydd och av konsumentombudsmannens behörighet.

Behandlingen av personuppgifter övervakas av dataombudsmannen i egenskap av behörig myndighet.

Banktjänsterna och betaltjänsterna övervakas av Finansinspektionen.

1.4 Det lagstiftningspolitiska målet att öka användningen av stark autentisering

Lagstiftningspolitiska omständigheter är inte juridiska tolkningsargument vid bedömningen av om en tjänst uppfyller de krav som har ställts på tjänsten. I denna fråga vill Transport- och kommunikationsverket lyfta fram syften med lagstiftningen.

Regeringens proposition (RP 36/2009, s. 7–11) innehåller en hänvisning till de nationella riktlinjerna för elektronisk identifiering, som utvecklingsgruppen för elektronisk identifiering drog upp 2008. Målet för riktlinjerna är bland annat att främja användning av stark autentisering även i tjänster som inte nödvändigtvis behöver stark autentisering:

> *Därför bör det slutliga målet vara att användarna kan använda en bekant och lättanvänd metod för stark autentisering även i samband med sådana tjänster som i sig inte nödvändigtvis kräver stark autentisering. För att uppnå detta mål måste kostnadsnivån för stark autentisering vara tillräckligt låg för alla aktörer. Ett av målen för en fungerande marknad är också en skälig prisnivå, som kan nås om det finns tillräckligt med alternativ på marknaden. Även om målet är att alla användare ska kunna använda det verktyg för stark autentisering som de valt i samband med så många tjänster som möjligt, kan tjänsteleverantörerna dock inte tvingas godkänna ett visst verktyg eller en viss leverantör av tjänster för stark autentisering.*

Enligt Transport- och kommunikationsverkets uppfattning är målet fortfarande aktuellt. År 2020 framkom ett allvarligt dataintrång i en psykoterapitjänst vilket skakade samhället. Incidenten ledde till en omfattande offentlig debatt i Finland, bland annat om behovet att öka användningen av stark autentisering i privata ärendehanteringstjänster. Dessutom har kommissionen vid bedömningen av behovet att ändra EU:s eIDAS-förordning betonat behovet att öka användningen av stark autentisering inom den privata sektorn.

2 Termer

Med **stark autentisering eller autentiseringsmetod** avses i denna promemoria en autentisering där tillhandahållandet av autentiseringen har anmälts och registrerats i ett sådant register över identifieringstjänster som avses i autentiseringslagen. Överensstämmelsen hos tjänsten för stark autentisering har bedömts och övervakas i enlighet med lagstiftningen. Tillitsnivån i tjänsten kan vara väsentlig eller hög.

Med **icke-registrerad eller svag identifieringstjänst eller identifieringsmetod** avses i denna promemoria en elektronisk identifieringstjänst som inte har anmälts till ett sådant register som avses i autentiseringslagen. Det innebär att tillförlitligheten hos tjänsten inte har bedömts och tjänsten inte övervakas i enlighet med lagstiftningen.

Leverantör av identifieringsverktyg tillhandahåller identifieringsverktyg till allmänheten, dvs. användare, och tillhandahåller sitt identifieringsverktyg till leverantörer av tjänster för identifieringsförmedling för förmedling i förtroendenätet.

Leverantör av tjänster för identifieringsförmedling förmedlar identifieringstransaktioner till förlitande parter, dvs. leverantörer av elektroniska ärendehanteringstjänster.

Innehavare av identifieringsverktyg är en fysisk eller juridisk person som enligt avtal har fått ett identifieringsverktyg av en leverantör av identifieringstjänster. I denna promemoria benämns innehavare i regel användare.

Förlitande part är en fysisk eller juridisk person som förlitar sig på en elektronisk identifiering. Förlitande parter är ärendehanteringstjänster som av tjänster för identifieringsförmedling skaffar tjänster för elektronisk identifiering av sina kunder.

Med **identifieringsverktyg och identifieringsmetod** avses i lagstiftningen en och samma sak: en materiell och/eller immateriell enhet som innehåller personidentifieringsuppgifter och som används för autentisering för nättjänster. En identifieringsmetod bygger på **autentiseringsfaktorer**, nämligen användarens kunskap, egenskap eller innehav, och **en dynamisk autentiseringsfaktor** som garanterar att varje identifiering är unik.

Med **identifieringssystem** avses ett system där medel för elektronisk identifiering beviljas och tillhandahålls användare. Ett identifieringssystem omfattar identifieringstjänstleverantörens tekniska system, ledning avseende informationssäkerhet och övriga fastställda krav på tillförlitlighet. Systemet omfattar även alla delar och funktioner som har köpts från entreprenörer och som används för att tillhandahålla identifieringstjänster.

Vid den tidpunkt då promemorian utarbetades var leverantörer av identifieringsverktyg banker, mobilteleföretag och Myndigheten för digitalisering och befolkningsdata. En del av dessa är också leverantörer av tjänster för identifieringsförmedling. I registret finns även två leverantörer som enbart tillhandahåller tjänster för identifieringsförmedling.

3 Bestämmelser och tolkningar

3.1 Tillförlitlighet och tillämpningsområde för tillhandahållande av tjänster för stark autentisering baserade på lagen

3.1.1 Bestämmelser

Enligt 1 § i autentiseringslagen (617/2009 och ändringarna) innehåller lagen bestämmelser om stark autentisering och om tillhandahållande av identifieringstjänster till tjänsteleverantörer, till allmänheten och till andra leverantörer av identifieringstjänster. Lagen tillämpas inte på tillhandahållande av tjänster avsedda för identifiering internt inom en sammanslutning. Lagen tillämpas inte heller på en sammanslutning som använder en egen metod för identifiering av egna kunder i samband med egna tjänster.

Enligt 10 § i lagen ska en leverantör av identifieringstjänster innan verksamheten inleds göra en skriftlig anmälan till Transport- och kommunikationsverket och lämna de uppgifter som fastställs i paragrafen. Enligt 11 § kan en leverantör av identifieringstjänster som är etablerad i Europeiska ekonomiska samarbetsområdet också göra en anmälan.

Enligt 12 § ska Transport- och kommunikationsverket föra ett offentligt register över de leverantörer av identifieringstjänster som har gjort en anmälan enligt 10 § och om de tjänster som de tillhandahåller.

Enligt 14 § ska leverantörer av identifieringstjänster ha principer för identifiering som närmare anger hur tjänsteleverantören uppfyller de skyldigheter som anges i denna lag. Leverantören av identifieringstjänster ska hålla principerna för identifiering allmänt tillgängliga och uppdaterade.

I regeringens proposition 36/2009 konstateras följande:

> *Registret är en av hörnstenarna för det planerade arrangemanget. Både den som skaffar ett identifieringsverktyg, som ofta agerar i egenskap av konsument, och en tjänsteleverantör som skaffar en identifieringstjänst blir tvungna att avgöra vilken leverantör av identifieringstjänster de kan lita på. Ett offentligt register på Kommunikationsverkets webbsidor ger på ett enkelt sätt information om de tjänsteleverantörer som i princip kan förväntas iaktta bestämmelserna i denna lag och som övervakas av myndigheten.*
>
> *…*
>
> *I största delen av de elektroniska tjänsterna behövs varken elektronisk identifiering eller elektroniska signaturer. I en del elektroniska tjänster kan man ändå bl.a. företa olika rättshandlingar. Sådana elektroniska tjänster förutsätter att parterna har förtroende för varandra på ett helt annat sätt än när ärenden sköts genom fysisk närvaro. Den som använder tjänsterna ska bl.a. kunna lita på att tjänsteleverantören har byggt upp sin service så att kraven på informationssäkerhet och integritetsskydd har beaktats. Tjänsteleverantören ska å sin sida bl.a. kunna lita på att den som använder tjänsterna via en fjärranslutning är den som han eller hon ger sig ut för att vara. För att de elektroniska tjänsterna och den elektroniska kommunikationen ska kunna utvecklas förutsätts att det framöver finns välfungerande tjänster för elektronisk identifiering.*

I regeringens proposition 272/2014 konstateras följande i motiveringen till 12 a §:

> *Identifieringstjänster kan tillhandahållas också utan att det görs en anmälan till Kommunikationsverket, men i detta fall anses leverantören av identifieringstjänster inte vara en leverantör av tjänster för stark autentisering. En leverantör av identifieringstjänster som hör till förtroendenätet är skyldig att iaktta bestämmelserna i lagen om stark autentisering och elektroniska signaturer, såsom de allmänna skyldigheterna för leverantörer av identifieringstjänster.*

3.1.2 Riktlinjer

Utifrån autentiseringslagen och motiveringen till lagen anser Transport- och kommunikationsverket att tillförlitlighetskraven gäller de identifieringstjänster som har anmälts till Transport- och kommunikationsverket och som har publicerats i registret som helhet och att tillförlitligheten i stark autentisering i sin tur bygger på myndighetstillsyn.

En situation där man påstår att ett identifieringsverktyg faktiskt tillhandahålls med två olika status kan juridiskt sett inte skiljas från en situation där de fastställda kraven inte följs, till exempel när en tjänst för stark autentisering av kunder tillhandahålls en ärendehanteringstjänst utan nödvändig kryptering. Kraven på stark autentisering är i alla fall tillämpliga när det är fråga om tillhandahållande av tjänster för stark autentisering.

Det är en annan sak att autentiseringslagen enligt undantagsbestämmelsen i 1 § inte tillämpas på användning av en sammanslutnings egen metod för identifiering av egna kunder i samband med egna tjänster. Därför behöver autentiseringslagens krav på identifieringstjänster som anmälts i ett sådant register som avses i

autentiseringslagen inte heller följas i identifieringstjänstleverantörernas egna tjänster. Sådana undantag får inte försämra tillförlitligheten hos identifieringstjänster som enligt anmälan tillhandahålls allmänheten.

Webbankskoder kan till exempel tillhandahållas allmänheten som identifieringsverktyg för stark autentisering. Utifrån undantagsbestämmelsen i lagen kan en identifieringsmetod och ett identifieringsverktyg användas som begränsade webbankskoder vid identifiering av bankens egna kunder i bankens egna tjänster utan att banken i sådana ärendehanteringssituationer följer alla krav i autentiseringslagen.

Banktjänsterna och betaltjänsterna övervakas av Finansinspektionen.

3.2 Inledande identifiering och ändring av ett icke-registrerat identifieringsverktyg till ett starkt identifieringsverktyg

3.2.1 Allmänt

Med inledande identifiering avses förfaranden för att verifiera identiteten hos den som ansöker om ett identifieringsverktyg, så att identifieringsverktyget för stark autentisering säkert beviljas och överlämnas till rätt person.

Tillförlitliga källor och inledande identifiering. I 17 § i autentiseringslagen finns bestämmelser om alternativa förfaranden och om tillförlitliga källor som bevisande av identitet kan grunda sig på och som godtas i Finland. Tillförlitliga källor är sådana som fastställs på nationell nivå. De förfaranden för inledande identifiering som fastställs i autentiseringslagen är förenliga med förfarandena i EU:s förordning om tillitsnivåer. Tillförlitliga källor är pass och identitetskort som har utfärdats av en myndighet.

I stället för pass eller identitetskort kan en inledande identifiering även grunda sig på en annan metod för stark autentisering, en inledande identifiering som polisen gör för att kunna bevilja ett identifieringsverktyg eller ett annat lagstadgat förfarande som Transport- och kommunikationsverket godkänner separat.

Dessutom ska identiteten kontrolleras i befolkningsdatasystemet. På så sätt grundar sig ett identifieringsverktyg för stark autentisering alltid på en identitet som har garanterats av staten.

Fjärridentifiering (*remote identification)* I nuläget handlar tolkningsfrågorna inom Europa framför allt om hur identiteten hos personer som ansöker om identifieringsverktyg på ett tillförlitligt sätt kan bevisas och verifieras (på engelska: *identity proofing and verification*) på sökandens identitetsbevis genom en elektronisk metod. I punkt 3.10 i anvisning 211/2019 O om bedömning av elektroniska identifieringstjänster har Transport- och kommunikationsverket samlat de faktorer som ska kontrolleras. Transport- och kommunikationsverket kommer att följa den internationella debatten och precisera tolkningen.

Höjning av tillitsnivån för en identifieringsmetod. Tolkningsfrågor kan även orsakas av hur en icke-registrerad elektronisk identifieringsmetod kan ändras till en stark autentiseringsmetod. Framför allt vid tillhandahållande av mobilappar planerar flera leverantörer att införa appen som icke-registrerad identifieringsmetod utan en lagenlig inledande identifiering och att sedan ändra appen till en stark autentiseringsmetod när en tillförlitlig inledande identifiering görs.

I exemplet är mobilappen tillgänglig för användare genom två olika metoder för beviljande.

- Den förenklade metoden uppfyller inte kraven på inledande identifiering i autentiseringslagen, och tillhandahållandet som grundar sig på denna metod anmäls inte till registret över identifieringstjänster.
- Genom en inledande identifiering som uppfyller kraven i lagstiftningen kan användaren höja tillitsnivån för identifieringsappen till en stark nivå, och denna metod för beviljande och tillhandahållandet av identifieringstjänster anmäls till registret över identifieringstjänster.

3.2.2 Riktlinjer

Beviljande av identifieringsverktyg för stark autentisering ska alltid grunda sig på ett lagenligt förfarande för inledande identifiering och lagenliga källor.

Inledande identifiering kan grunda sig på verifiering av identitet genom stark autentisering eller uppvisande av pass eller identitetskort vid besök på plats eller genom en tillförlitlig distansuppkoppling. Vid uppvisande av pass eller identitetskort ska det kunna kontrolleras att handlingen är äkta och tillhör den som visar upp den.

En icke-registrerad identifieringsmetod kan vara en del av beviljandet av en stark autentiseringsmetod och den inledande identifieringen, dvs. verifieringen av sökandens identitet.

En stark inledande autentisering kan inte enbart grunda sig på en icke-registrerad identifieringsmetod och verifiering av identitet i anslutning till beviljande av en icke-registrerad identifieringsmetod. En icke-registrerad identifieringsmetod kan vara en del av processen för beviljande av en stark autentiseringsmetod och den inledande identifieringen, dvs. verifieringen av sökandens identitet.

Redan på tillitsnivån väsentlig ska förfarandet beakta risken att ett icke-registrerat identifieringsverktyg och ett pass eller identitetskort kan ha hamnat i orätta händer eller att passet eller identitetskortet kan vara förfalskade.

Appen kan till exempel ursprungligen ha tagits i bruk med falska personuppgifter, mobilappen kan ha hamnat i orätta händer eller man kan obehörigt ha skapat en instans baserad på appen för utomstående.

För att en icke-registrerad identifieringsmetod och dess autentiseringsfaktorer, såsom bankkoder eller en mobilapp, ska kunna ändras till en stark autentiseringsmetod, krävs ytterligare kontroller som gör att kraven på verifiering av identiteten hos den som ansöker om en stark autentiseringsmetod som helhet ska uppfyllas.

Ytterligare kontroller ska kunna garantera att rätt sökande innehar och kommer att inneha det icke-registrerade identifieringsverktyg som ska ändras till ett starkt identifieringsverktyg.

Följande kan beaktas vid **helhetsbedömningen**:

- tillförlitligheten i kontrollen av att pass eller identitetskort är äkta
- kontroll av giltigheten för pass eller identitetskort
- jämförelse av sökandens egenskaper med det identitetsbevis som sökanden har visat upp

- olika ytterligare kontroller, såsom frågor om omständigheter som rätt sökande enbart känner till
- information som ska lämnas till innehavaren via olika kanaler efter beviljande
- uppföljning, observation om avvikelser och åtgärder på grund av avvikelser
- kontroller i anslutning till beviljande av icke-registrerade identifieringsverktyg, leveransförfarande och användning
- kontroller av leveransförfarande i anslutning till höjning av tillitsnivå.

3.2.3 Bestämmelser

Autentiseringslag: 8 § (29.6.2016/533) Krav på system för elektronisk identifiering

Ett system för elektronisk identifiering ska uppfylla följande krav:

1) identifieringsmetoden grundar sig på en identifiering enligt 17 och 17 a § så att uppgifterna om den kan kontrolleras i efterskott i enlighet med 24 §,

2) identifieringsmetoden medger entydig identifiering av innehavaren av identifieringsverktyget så att åtminstone de villkor uppfylls som gäller för tillitsnivån väsentlig enligt avsnitten 2.1.2, 2.1.3 och 2.1.4 i bilagan till kommissionens genomförandeförordning (EU) 2015/1502 om fastställande av tekniska minimispecifikationer och förfaranden för tillitsnivåer för medel för elektronisk identifiering i enlighet med artikel 8.3 i Europaparlamentets och rådets förordning (EU) nr 910/2014 om elektronisk identifiering och betrodda tjänster för elektroniska transaktioner på den inre marknaden, nedan förordningen om tillitsnivåer vid elektronisk identifiering

[…]

17 § (23.11.2018/1009) Identifiering av en fysisk person som ansöker om ett identifieringsverktyg

Vid inledande identifiering ska identifieringen av en fysisk person göras personligen eller elektroniskt på ett sådant sätt att de krav uppfylls som gäller för tillitsnivån väsentlig eller hög enligt avsnitt 2.1.2 i bilagan till förordningen om tillitsnivåer vid elektronisk identifiering. Kontrollen av en persons identitet kan grunda sig på en identitetshandling som utfärdats av en myndighet eller ett sådant identifieringsverktyg för stark autentisering som avses i denna lag. Kontrollen av identiteten kan dessutom grunda sig på ett förfarande som en offentlig eller privat aktör tidigare och i annat syfte än för beviljande av ett identifieringsverktyg för stark autentisering har använt sig av och som Transport- och kommunikationsverket godkänner utifrån de bestämmelser som gäller förfarandet och utifrån myndighetstillsynen eller utifrån en bekräftelse av ett i 28 § 1 punkten avsett organ för bedömning av överensstämmelse.

Dokument som godkänns vid inledande identifiering, när identifieringen endast sker utifrån en identitetshandling som utfärdats av en myndighet, är ett giltigt pass eller identitetskort som har utfärdats av en myndighet i en medlemsstat inom Europeiska ekonomiska samarbetsområdet. En leverantör av identifieringsverktyg som så önskar kan också vid kontrollen av identiteten använda ett giltigt pass som har utfärdats av en myndighet i någon annan stat.

Om identiteten hos den som ansöker om ett identifieringsverktyg inte kan verifieras på ett tillförlitligt sätt, ska polisen utföra den inledande identifiering som gäller ansökan. De kostnader som polisens inledande identifiering orsakar den som ansöker om ett identifieringsverktyg är en offentligrättslig prestation. Bestämmelser om avgiften för en sådan prestation finns i lagen om grunderna för avgifter till staten.

[…]

Autentiseringslag: 7 § (20.2.2015/139) Användning av uppgifter i befolkningsdatasystemet

Leverantörer av identifieringsverktyg och certifikatutfärdare som tillhandahåller betrodda tjänster ska hämta och uppdatera de uppgifter som de behöver för tillhandahållandet av identifieringstjänster för fysiska personer med användning av befolkningsdatasystemet. Leverantörer av identifieringstjänster ska dessutom säkerställa att de uppgifter som de behöver för tillhandahållandet av identifieringstjänster är uppdaterade enligt uppgifterna i befolkningsdatasystemet. (29.6.2016/533)

[…]

3.3 Åtskillnad mellan en stark autentiseringsmetod och en icke-registrerad identifieringsmetod i användarens identifieringsverktyg

3.3.1 Allmänt

Användarens autentiseringsfaktorer. Användning av ett identifieringsverktyg samt en identifieringsmetod är förknippade med sådana autentiseringsfaktorer som användaren kan se och en sådan autentiseringsmekanism för ett tekniskt genomförande av identifieringstransaktioner som användaren inte kan se.

I detta avsnitt behandlas de egenskaper som användaren kan se för att kunna skilja en identifieringsmetod från andra identifieringsmetoder och på så sätt även en stark autentiseringsmetod från en icke-registrerad identifieringsmetod. Det är med andra ord fråga om skillnader som gör att användaren på ett tydligt sätt kan förstå att denne vid elektronisk kommunikation använder olika identifieringsmetoder som omfattas av olika skydd i lagstiftningen.

Kommersialisering. Transport- och kommunikationsverket konstaterar att autentiseringslagen naturligtvis inte innehåller uttryckliga bestämmelser om kommersialisering eller varumärkesregistrering. Därför ska tolkningen utgå från en så objektiv generell bedömning och genomförbarhet som möjligt. Hänsyn bör tas till kraven på en specifik driftsmiljö för elektroniska identifieringsmetoder, eftersom det till exempel finns skillnader i användningen av kodkalkylatorer, webbläsare, mobilappar och chipkort.

Gemensam praxis för identifieringstjänster. Transport- och kommunikationsverket konstaterar även att det är önskvärt att kommersialiseringen, exempelvis i samarbete för förtroendenätet för identifieringstjänster, syftar till att hitta gemensam god praxis som alla leverantörer av identifieringstjänster ska kunna tillämpa på samma sätt för att kunna skilja en stark autentisering från en icke-registrerad identifiering. Detta kan förbättra användarnas möjligheter att förstå skillnaderna mellan olika identifieringstjänster och förtroendet för en stark autentisering.

3.3.2 Riktlinjer

Transport- och kommunikationsverket anser att följande egenskaper som användaren kan se ska beaktas när en stark autentiseringsmetod ska skiljas från en icke-registrerad identifieringsmetod:

1) **Identifieringsmetodernas namn ska skiljas åt i tillräckligt många avseenden.**
2) **De visuella layouterna för identifieringsmetoderna ska vara tillräckligt olika.**
3) **Det är möjligt att överväga att använda autentiseringsfaktorer i olika kategorier för en stark autentiseringsmetod respektive en icke-registrerad identifieringsmetod, om det är tekniskt genomförbart.**
4) **Användarens möjligheter att ansvara för det starka autentiseringsverktyget ska tryggas.**
5) **Tillgängligheten ska beaktas**

Transport- och kommunikationsverket anser att följande egenskaper som användaren kan se ska beaktas när en stark autentiseringsmetod ska skiljas från en svag identifieringsmetod:

1) Identifieringsmetodernas namn ska skiljas åt i tillräckligt många avseenden. En stark metod kan skiljas åt i tillräcklig mån genom en identifieringsprodukt med ett helt annat namn. Om man emellertid i huvudsak vill behålla ett och samma produktnamn på den starka metoden och den icke-registrerade metoden, ska den starka metoden skiljas åt genom namndelar eller namntillägg som är klart begripliga och särskiljande. Dessutom bör förhindrade personer beaktas när namnen ska skiljas från varandra.

2) De visuella layouterna för identifieringsmetoderna ska vara tillräckligt olika. Olika logotyper, färger, särskiljande ordförråd och andra visuellt särskiljande drag kan användas för att skilja på metoderna. Förhindrade personer bör beaktas, eftersom skillnader som enbart kan upptäckas med synen inte kan anses vara tillräcklig.

3) Det är möjligt att överväga att använda autentiseringsfaktorer i olika kategorier för en stark autentiseringsmetod respektive en svag identifieringsmetod, om det är tekniskt genomförbart.

Driftsmiljön och användbarheten kan beaktas i genomförbarheten.

I lagstiftningen delas autentiseringsfaktorerna in i följande kategorier:
- en innehavsbaserad autentiseringsfaktor
- en kunskapsbaserad autentiseringsfaktor
- en egenskapsbaserad autentiseringsfaktor utgår från en kroppslig egenskap hos en fysisk person.

Enligt Transport- och kommunikationsverkets bedömning är det alltid möjligt att använda en kunskapsbaserad autentiseringsfaktor för en stark autentiseringsmetod respektive en icke-registrerad identifieringsmetod, till exempel pinkoder eller andra lösenord. Det är med andra ord godtagbart att använda autentiseringsfaktorer i en och samma kategori. När en leverantör av identifieringsverktyg tillhandahåller en svag identifiering och en stark autentisering, till exempel i en mobilapp, kan de överväga definition av olika pinkoder eller lösenord. Utifrån en utredning från leverantörerna av identifieringstjänster är det dock motiverat att beakta observationerna om huruvida användare kan hantera olika lösenord eller pinkoder i ett sådant användarsammanhang.

En innehavsbaserad autentiseringsfaktor, till exempel lösenordsdosa, lösenordslista, mobilapp eller simkort, kan urskiljas, men det kan uppstå tekniska problem med att genomföra åtskillnaden. Dessutom kan metodens användbarhet få en negativ effekt.

En egenskapsbaserad autentiseringsfaktor (fingeravtryck, ansiktsbild osv.) kan urskiljas exempelvis så att en biometrisk faktor inte alls används för någondera metoden eller så att olika egenskaper används för olika metoder, eller så bör en kombination av flera biometriska egenskaper användas för den starka metoden. Även i detta avseende är det motiverat att beakta observationerna om användarnas typiska verksamhet.

4) Användarens möjligheter att ansvara för det starka autentiseringsverktyget ska tryggas.

I 23 § i autentiseringslagen finns bestämmelser om skyldigheten för innehavare av identifieringsverktyg att förvara identifieringsverktyget och om förbudet att överlåta verktyget för att användas av någon annan.

Transport- och kommunikationsverket anser att specifikationen av funktionerna för en stark autentiseringsmetod respektive en icke-registrerad identifieringsmetod ska ta hänsyn till användarens möjligheter att omsorgsfullt förvara identifieringsverktyget i enlighet med sin lagstadgade skyldighet så att användningen av den icke-registrerade identifieringsmetoden inte utgör en risk för användaren att inneha och använda faktorerna för den starka autentiseringen.

5) Tillgänglighet

Vissa krav i lagen om tillhandahållande av digitala tjänster (306/2019) gäller leverantörer av tjänster för stark autentisering. Enligt 2 § 4 punkten i lagen avses med *tillgänglighet principer och tekniska hänsyn som ska respekteras när digitala tjänster planeras, utvecklas, underhålls och uppdateras, i syfte att göra tjänsterna mer tillgängliga för användarna, särskilt personer med funktionsnedsättning*.

Kraven i lagen har samband med internationella standarder för webbläsare och mobilappar.

Transport- och kommunikationsverket övervakar inte efterlevnaden av lagen om tillhandahållande av digitala tjänster, men rekommenderar i detta sammanhang att leverantörerna beaktar en eventuell inverkan av lagens krav på åtskillnaden. Enligt Transport- och kommunikationsverkets bedömning ska förhindrade personer också kunna särskilja om de använder en stark autentiseringsmetod eller en icke-registrerad identifieringsmetod.

3.3.3 Bestämmelser

Autentiseringslag: 8 a § (29.6.2016/533) Autentiseringsfaktorer som ska användas i identifieringsmetoden

I en identifieringsmetod ska minst två av följande autentiseringsfaktorer användas:

1) en kunskapsbaserad autentiseringsfaktor som personen måste kunna visa att den har kunskap om,

2) en innehavsbaserad autentiseringsfaktor som personen måste kunna visa att den innehar,

3) en egenskapsbaserad autentiseringsfaktor som utgår från en kroppslig egenskap hos en fysisk person.

[…]

Autentiseringslag: 8 § (29.6.2016/533) Krav på system för elektronisk identifiering

Ett system för elektronisk identifiering ska uppfylla följande krav:

[…]

3) med hjälp av identifieringsmetoden går det att säkerställa att endast innehavaren av identifieringsverktyget kan använda verktyget på ett sådant sätt att åtminstone de villkor uppfylls som gäller för tillitsnivån väsentlig enligt avsnitten 2.2.1 och 2.3 i bilagan till förordningen om tillitsnivåer vid elektronisk identifiering,

[…]

[…]

3.4 Tekniska krav på autentiseringsmekanismer och identifieringssystem

3.4.1 Allmänt

I 8 § och 8 a § i autentiseringslagen och i punkt 2.3 i bilagan till EU:s förordning om tillitsnivåer finns bestämmelser om att endast innehavaren av identifieringsverktyget får använda identifieringsmetoden och om att autentiseringsmekanismen ska tåla en sådan angreppspotential som fastställts enligt tillitsnivå. I 23 § i autentiseringslagen finns bestämmelser om skyldigheten för innehavare av identifieringsverktyg att ansvara för verktyget.

Kraven på autentiseringsmekanismer gäller framför allt hemligheter på olika nivåer i identifieringsmetoder. Detta är också förknippat med preciseringarna i 6 § i Transport- och kommunikationsverkets föreskrift 72.

I övrigt fastställs krav på identifieringssystem i 13 § i autentiseringslagen och i punkterna 2.4.4 Registerföring, 2.4.5 Anläggningar och personal och 2.4.6 Tekniska kontroller i EU:s förordning om tillitsnivåer. Kraven preciseras i 5 § Tekniska informationssäkerhetsåtgärder i identifieringssystem och 7 § Krypteringskrav för identifieringssystem och gränssnitt i Transport- och kommunikationsverkets föreskrift 72.

Syftet med denna promemoria är inte att beskriva alla krav, men under punkten Bestämmelser finns en hänvisning till relevanta bestämmelser om tillförlitlighet.

3.4.2 Riktlinjer

Skydd av hemligheter i identifieringsmetoder för stark autentisering omfattar hemligheter som användaren har kännedom om och hemligheter om metodens egenskaper.

När autentiseringsfaktorerna i en stark autentiseringsmetod kopplas till en person som har identifierats genom en stark inledande identifiering, ska hänsyn framför allt tas till säkerheten i autentiseringsfaktorerna och i identifieringsmekanismens hemlighet (den privata nyckeln).

Vanligen är hemligheten i anslutning till en metod exempelvis en privat signaturnyckel som har koppling till PKI-implementeringen av mobilcertifikat och som inte visas för användaren och är lagrad på simkortet, eller en privat nyckel för en mobilapp så att nyckeln är lagrad i en skyddad SE- eller TEE-komponent i den mobila enheten.

När en identifieringsmetod och en autentiseringsmekanism genomförs, gäller det att i alla faser av identifieringsmetodens livscykel säkerställa skyddet av de hemligheter som ska användas i identifieringsmetodens autentiseringsmekanism.

Även om en icke-registrerad identifieringsmetod tillhandahålls parallellt med en stark autentiseringsmetod, får det inte till några delar underminera skyddet av hemligheterna för den starka autentiseringen mot angreppspotential enligt tillitsnivå.

Transport- och kommunikationsverket anser att, om en identifieringsmetod som har beviljats genom en svag inledande identifiering ändras till en stark autentiseringsmetod genom en lagenlig inledande identifiering, ska uppmärksamhet framför allt ägnas åt att hemligheter för identifieringsmetoden och

hemligheter som ska användas i autentiseringsmekanismen har skapats och att hemligheterna tryggas enligt kraven på stark autentisering.

Transport- och kommunikationsverket anser att en ny privat nyckel/hemlighet i princip ska skapas för en stark autentiseringsmetod, om behandlingen av uppgifterna om nyckeln/hemligheterna i en mobilapp som används för en icke-registrerad identifieringsmetod inte uppfyller kraven på stark autentiseringsmetod.

Enligt Transport- och kommunikationsverkets bedömning är åtminstone hemligheter som är lagrade i SE-komponenten eller i TEE-komponenten skyddade på så tillförlitliga sätt att användning av en och samma hemlighet i både en icke-registrerad identifieringsmetod och en stark autentiseringsmetod kan övervägas. Säkerheten i hemligheterna ska dock utvärderas som helhet med hänsyn till de säkerhetskontroller som används.

Transport- och kommunikationsverket anser att skyddet av en autentiseringsmekanism och hemligheter ska säkerställas i hela identifieringssystemet, dvs. även i de bakgrundssystem som påverkar tillförlitligheten i identifieringen och motståndskraften mot angrepp, så att tillhandahållandet av en icke-registrerad identifiering inte underminerar skyddet av den starka autentiseringsmetoden. Bland annat följande ska beaktas i identifieringssystem:

- koppling mellan autentiseringsfaktorer och användare i bakgrundssystemet
- tekniskt genomförande av autentiseringsfaktorer
- lagring av information
- hantering av åtkomst till systemet och informationen
- kryptering av gränssnitt samt protokoll.

3.4.3 Bestämmelser

Autentiseringslag: 8 § (29.6.2016/533) Krav på system för elektronisk identifiering

Ett system för elektronisk identifiering ska uppfylla följande krav:

[…]

4) identifieringssystemet är säkert och tillförlitligt på ett sådant sätt att åtminstone de villkor uppfylls som gäller för tillitsnivån väsentlig enligt avsnitten 2.2.1, 2.3.1 och 2.4.6 i bilagan till förordningen om tillitsnivåer vid elektronisk identifiering, med hänsyn till de informationssäkerhetsrisker som är förknippade med den teknik som används vid tidpunkten, och de lokaler som används för tillhandahållandet av identifieringstjänsten är säkra på det sätt som anges i avsnitt 2.4.5 i bilagan till den förordningen,

5) ledningen avseende informationssäkerheten sköts på ett sådant sätt att de villkor uppfylls som anges i det inledande stycket i avsnitt 2.4 i bilagan till förordningen om tillitsnivåer vid elektronisk identifiering och åtminstone de villkor uppfylls som gäller för tillitsnivån väsentlig enligt avsnitten 2.4.3 och 2.4.7 i bilagan till den förordningen.

[…]

Autentiseringslag: 8 a § (29.6.2016/533) Autentiseringsfaktorer som ska användas i identifieringsmetoden

I en identifieringsmetod ska minst två av följande autentiseringsfaktorer användas:

[…]

I varje identifieringsmetod ska det i enlighet med avsnitt 2.3.1 i bilagan till förordningen om tillitsnivåer vid elektronisk identifiering användas en sådan dynamisk autentisering som

ändras vid varje ny autentisering mellan en person och det system som kontrollerar personens identitet.

Bilagan till EU:s förordning om tillitsnivåer: 1. Tillämpliga definitioner

*3. **dynamisk autentisering**: en elektronisk process som använder kryptering eller andra metoder för att på begäran skapa ett elektroniskt bevis för att en person har kontroll över eller är i besittning av identifieringsinformationen, och som ändras vid varje autentisering mellan personen och det system som kontrollerar personens identitet.*

Autentiseringslag: 13 § Allmänna skyldigheter för leverantörer av identifieringstjänster

Hos leverantörer av identifieringstjänster ska lagringen av uppgifter som sammanhänger med identifieringen, personalen och de tjänster som köps av underleverantörer uppfylla åtminstone kraven för tillitsnivån väsentlig enligt avsnitten 2.4.4 och 2.4.5 i bilagan till förordningen om tillitsnivåer vid elektronisk identifiering. Leverantörer av identifieringstjänster ska dessutom ha en omfattande plan för identifieringstjänstens upphörande. (29.6.2016/533)

[…]

Autentiseringslag: 23 § Skyldigheter för innehavare av identifieringsverktyg

Innehavaren av ett identifieringsverktyg ska använda verktyget i enlighet med villkoren i avtalet. Innehavaren ska förvara identifieringsverktyget omsorgsfullt. Innehavaren är skyldig att ansvara för verktyget efter att ha tagit emot det.

Innehavaren av ett identifieringsverktyg får inte överlåta verktyget för att användas av någon annan.

Bilagan till EU:s förordning om tillitsnivåer: 2.3.1 Autentiseringsmekanism

LÅG

[…]

2. Om personidentifieringsuppgifter lagras som en del av autentiseringsmekanismen är dessa uppgifter säkrade för att skydda mot förlust och från att den äventyras, inklusive offline-analys.

[…]

VÄSENTLIG

Nivå låg, samt

1. innan personidentifieringsuppgifter lämnas ut sker en tillförlitlig kontroll av medlet för elektronisk identifiering och dess giltighet med hjälp av en dynamisk autentisering.

2. autentiseringsmekanismen genomför säkerhetskontroller för att verifiera medlet för elektronisk identifiering, varför det är högst osannolikt att exempelvis gissningar, tjuvlyssning, omspelning eller manipulation av kommunikation som görs av en angripare med måttlig angreppspotential kan underminera autentiseringsmekanismerna.

HÖG

Nivå väsentlig, samt

autentiseringsmekanismen genomför säkerhetskontroller för att verifiera medlet för elektronisk identifiering, varför det är högst osannolikt att exempelvis gissningar, tjuvlyssning, omspelning eller manipulation av kommunikation som görs av en angripare med stor angreppspotential kan underminera autentiseringsmekanismerna.

M72: 6 § Krav på informationssäkerhet i identifieringsmetoder

Identifieringsverktyg får inte kombineras med den sökande förrän en inledande identifiering av den sökande har gjorts, eller så ska det vid processen för beviljande av identifieringsverktyg annars säkerställas att identifieringsverktyget inte kan användas innan den sökande har gjort en inledande identifiering enligt 17 § i autentiseringslagen.

Tjänsteleverantören ska säkerställa att hemliga uppgifter om identifieringsverktyget inte i någon situation röjs för dess personal.

Tjänsteleverantören får inte kopiera hemliga uppgifter om identifieringsverktyget.

Autentiseringslag: 13 § Allmänna skyldigheter för leverantörer av identifieringstjänster

Hos leverantörer av identifieringstjänster ska lagringen av uppgifter som sammanhänger med identifieringen, personalen och de tjänster som köps av underleverantörer uppfylla åtminstone kraven för tillitsnivån väsentlig enligt avsnitten 2.4.4 och 2.4.5 i bilagan till förordningen om tillitsnivåer vid elektronisk identifiering. Leverantörer av identifieringstjänster ska dessutom ha en omfattande plan för identifieringstjänstens upphörande. (29.6.2016/533)

[…]

LoA: 2.4.4 Registerföring

LÅG

1. Registrera och lagra relevant information med hjälp av ett effektivt registerhanteringssystem, med beaktande av tillämplig lagstiftning och god praxis i fråga om skydd och lagring av personuppgifter.

2. Lagra – i den mån det är tillåtet enligt nationell lag eller andra nationella administrativa bestämmelser – och skydda register så länge som de behövs för granskning och undersökning av säkerhetsöverträdelser och för lagring, varefter registren ska förstöras på ett säkert sätt.

VÄSENTLIG/HÖG

Samma som nivån låg, samt

känsligt kryptografiskt material, om sådant används för utfärdande av medel för elektronisk identifiering och autentisering, ska skyddas från manipulation.

LoA: 2.4.5 Anläggningar och personal

LÅG/VÄSENTLIG

1. Förfaranden ska finnas som ser till att personal och underleverantörer är tillräckligt utbildade, kvalificerade och erfarna i de färdigheter som krävs för att sköta sina roller.

2. Tillräcklig personal och underleverantörer ska finnas för att korrekt driva och bemanna tjänsten i enlighet med policyer och förfaranden som gäller för den.

3. Anläggningar som används för att tillhandahålla tjänsten ska kontinuerligt övervakas och skyddas mot skador orsakade av miljöhändelser, obehörig åtkomst och andra faktorer som kan inverka på tjänstens säkerhet.

4. Anläggningar som används för att tillhandahålla tjänsten ska säkerställa att tillträde till utrymmen där personliga, kryptografiska eller andra känsliga uppgifter finns eller behandlas, är begränsat till auktoriserad personal eller underleverantörer.

Bilagan till EU:s förordning om tillitsnivåer: 2.4.6 Tekniska kontroller

LÅG/VÄSENTLIG

1. Proportionella tekniska kontroller ska finnas för att hantera riskerna för tjänsternas säkerhet, och för att skydda de behandlade uppgifternas sekretess, integritet och tillgänglighet.

2. Elektroniska kommunikationskanaler som används för att utbyta personuppgifter eller känslig information skyddas mot avlyssning, manipulation och omspelning.

3. Tillgång till känsligt kryptografiskt material, om sådant används för utfärdande av medel för elektronisk identifiering och autentisering, ska strikt begränsas till de befattningar och applikationer som kräver tillgång. Det ska säkerställas att sådant material aldrig ständigt lagras i klartext.

4. Förfaranden finns för att se till att säkerheten upprätthålls över tiden och att förmåga finns att agera om risknivån förändras eller vid incidenter och säkerhetsöverträdelser.

5. Alla medel som innehåller personuppgifter eller kryptografiska eller andra känsliga uppgifter ska lagras, transporteras och bortskaffas på ett säkert sätt.

M72: 5 § Tekniska informationssäkerhetsåtgärder i identifieringssystem

Ett identifieringssystem ska planeras, genomföras och administreras med beaktande av följande faktorer:

1) datakommunikationssäkerhet
- *a) säkerhet i nätstrukturen*
- *b) indelning av datakommunikationsnätet i zoner*
- *c) filtreringsregler enligt principen om behovsenlig behörighet*
- *d) administration av filtrering och kontrollsystem under hela livscykeln*
- *e) administrationsförbindelser*

2) säkerhet i informationssystem
- *a) administration av åtkomsträttigheter*
- *b) identifiering av användare av system*
- *c) härdande av system*
- *d) skydd mot skadliga program*
- *e) spårning av säkerhetshändelser*
- *f) förmåga att observera avvikelser samt återhämtning*
- *g) internationellt eller nationellt rekommenderade krypteringslösningar till andra delar än vad som föreskrivs i 7 §*

3) säkerhet i användning
- *a) hantering av förändringar*
- *b) behandlingsmiljön för sekretessbelagt material*
- *c) distansanvändning och -administration*
- *d) hantering av programsårbarheter*
- *e) säkerhetskopiering.*

Ett produktionsnät och administrationsförbindelser i 1) e) samt distansanvändning och -administration i 3) c) ovan ska genomföras så att informationssäkerhetshot som orsakas av organisationens övriga tjänster, som e-post eller webbsurfning, samt informationssäkerhetshot som orsakas av organisationens terminalenhet vid hantering av andra funktioner än de som är nödvändiga för hanteringen är

- *a) speciellt bedömda och minimerade på tillitsnivån väsentlig och*
- *b) förhindrade som helhet på tillitsnivån hög.*

M72: 7 § Krypteringskrav för identifieringssystem och gränssnitt

Trafiken i gränssnitten mellan leverantörer av identifieringstjänster och mellan leverantörer av identifieringstjänster och tjänster för ärendehantering ska krypteras. Följande metoder ska användas vid kryptering, nyckelutbyte och i underskrifter i anslutning till kryptering:

1) ***Nyckelutbyte:*** *DHE-metoder, eller ECDHE-metoder som använder elliptiska kurvor, ska användas vid nyckelutbyte. Den ändliga kroppen (finite field) som används i räkneoperationer ska utgöra minst 2 048 bitar i DHE-metoden och minst 224 bitar i ECDHE-metoden.*

2) ***Underskrifter:*** *Vid användning av RSA för elektronisk underskrift ska nyckeln utgöra minst 2 048 bitar. Vid användning av ECDSA-metoden för elliptisk kurva ska den ändliga kroppen nedan utgöra minst 224 bitar.*

3) ***Symmetrisk kryptering:*** *Krypteringsalgoritmen ska vara AES eller Serpent. Nyckeln ska utgöra minst 128 bitar. Krypteringsmoden ska vara CBC, GCM, XTS eller CTR.*

4) ***Hashfunktioner****: Hashfunktionen ska vara SHA-2, SHA-3 eller Whirlpool. Med SHA-2 avses funktionerna SHA224, SHA256, SHA384 och SHA512.*

Krypteringsinställningarna ska tekniskt tvingas till miniminivåerna ovan för att handskakningen inte ska resultera i inställningar som är sämre än miniminivåerna.

Vid användning av protokollet TLS ska TLS-version 1.2 eller nyare användas. TLS-version 1.1 kan användas endast om användarens terminalutrustning inte stöder nyare versioner.

Integriteten och sekretessen för meddelanden med personuppgifter ska skyddas förutom med kryptering som avses i 1 mom. också på meddelandenivå enligt 1 mom.

Man ska sörja för integriteten och sekretessen för uppgifter som lagras i identifieringssystem. Om skyddet av uppgifterna endast baserar sig på kryptering, tillämpas kraven på underskrift, symmetrisk kryptering och hashfunktioner i 1 mom. ovan.

3.5 Avtalsvillkor och ansvar för användare

3.5.1 Allmänt

I 20 § i lagen konstateras att utgivningen av identifieringsverktyg grundar sig på ett avtal mellan den som ansöker om verktyget och leverantören av identifieringstjänster. Avtalet ska ingås skriftligen. Avtalet kan även ingås elektroniskt om dess innehåll inte kan ändras ensidigt och det hålls tillgängligt för parterna.

I 15 § i autentiseringslagen finns bestämmelser om de uppgifter (avtalsvillkor) som en leverantör av identifieringsverktyg ska lämna till användaren innan ett avtal ingås.

I 23 § i lagen finns bestämmelser om skyldighet för användare att omsorgsfullt förvara identifieringsverktyget, och i 21–27 § finns också i övrigt bestämmelser om rättigheter, skyldigheter och ansvar för leverantörer av identifieringsverktyg och innehavare av identifieringsverktyg.

Transport- och kommunikationsverket övervakar kravet i 15 § i autentiseringslagen på att en leverantör av tjänster för stark autentisering innan ett avtal ingås ska informera den som ansöker om ett identifieringsverktyg (användaren) om de faktorer som fastställs i paragrafen. Bedömningen av avtalsvillkorens tydlighet och skälighet omfattas av de allmänna bestämmelserna om konsumentskydd.

Frågor om tillhandahållande kan också bedömas utifrån den allmänna lagstiftningen om konsumentskydd eller den allmänna konkurrenslagstiftningen. Dessa uppdrag tillhör Konkurrens- och konsumentverket eller konsumentombudsmannen som arbetar vid Konkurrens- och konsumentverket.

3.5.2 Riktlinjer

Med tanke på användarens rättigheter kan en identifieringsmetod inte tillhandahållas som både en stark metod och en icke-registrerad metod baserat på att de rättigheter som fastställs i autentiseringslagen genomförs genom avtalsvillkor.

Tillförlitligheten hos tjänster för stark autentisering bygger i sin tur på myndighetstillsyn. De tvingande bestämmelserna om rättigheter för användare i autentiseringslagen gäller inte icke-registrerade identifieringstjänster, och Transport- och kommunikationsverket har inte behörighet att övervaka genomförandet av icke-registrerad elektronisk identifiering och inte heller avtalsvillkoren för en sådan identifiering. Om de rättigheter som fastställs i autentiseringslagen ska genomföras genom avtalsvillkor, räcker det inte till för att ersätta det skydd av användare och ärendehanteringstjänster som fastställs i autentiseringslagen och som inte gäller icke-registrerade identifieringsmetoder.

Transport- och kommunikationsverket anser *inte* att det med stöd av autentiseringslagen är nödvändigt att tillhandahålla helt separata avtal och avtalsvillkor för en svag identifieringsmetod respektive en stark autentiseringsmetod.

I alla fall ska villkoren för stark autentisering i enlighet med 15 § i lagen framgå tydligt av avtalsvillkoren, och villkoren för icke-registrerad identifiering får inte förväxlas med de villkoren.

Om en leverantör av identifieringsverktyg utarbetar avtalsvillkor för både en icke-registrerad identifiering och en stark autentisering, krävs en särskild omsorgsfullhet för att skyldigheten för leverantörer av identifieringsverktyg att lämna uppgifter ska kunna uppfyllas.

- Tjänsteleverantören ska i detalj lyfta fram skillnaderna mellan tjänsten för icke-registrerad identifiering och tjänsten för stark autentisering vad gäller de uppgifter som räknas upp i 15 § i autentiseringslagen och eventuella andra relevanta uppgifter. Till Transport- och kommunikationsverkets behörighet hör tillsyn över att uppgifterna i 15 § om verktyg för stark autentisering lämnas till användaren på det sätt som avses i lagen.

- En högre skyldighet att lämna uppgifter följer av att användaren till exempel bör uppfatta skillnaderna mellan en stark autentiseringsmetod och en annan identifiering som avses i samma avtal (skyldighet att lämna uppgifter om de tjänster som tillhandahålls och om att tjänsterna och tjänsteleverantören endast till den del det gäller stark autentisering omfattas av offentlig tillsyn) och skillnaderna i användarens rättsliga ställning beroende på vilket av identifieringsverktyget användaren använder (uppgifter om parternas rättigheter och skyldigheter). En skillnad i den rättsliga ställningen följer till exempel oundvikligen av att användarens ansvar för obehörig användning regleras med stöd av autentiseringslagen enbart i fråga om stark autentisering[1].

- Med stöd av konsumentskyddslagen ska dessutom de villkor som tillhandahålls konsumenter vara tydliga och begripliga, vilket övervakas av konsumentombudsmannen. Transport- och kommunikationsverket har inte

[1] Dessa skillnader kan förmodligen inte helt undanröjas genom avtal, eftersom exempelvis användarens ansvar för obehörig användning i förhållande till tredje man inte på ett giltigt sätt kan begränsas genom avtal mellan användaren och leverantören av identifieringstjänster.

heller behörighet att utgående från konsumentskyddslagen ta ställning till marknadsföringen av identifieringstjänster.

Hanteringen av ett icke-registrerat identifieringsverktygs livscykel ska skiljas från hanteringen av ett starkt autentiseringsverktygs livscykel på ett tydligt sätt, om olika förfaranden tillämpas på hanteringen.

Exempelvis ett starkt autentiseringsverktyg eller dess autentiseringsfaktor kan enbart förnyas på den tillitsnivå som krävs enligt lagen, och eventuella förenklade förnyelseförfaranden för en icke-registrerad identifieringsmetod får inte underminera den starka autentiseringsmetoden. Det är möjligt att samtidigt bevilja ett starkt verktyg och ett icke-registrerat verktyg, om det sker på det sätt som det krävs för att öppna ett starkt verktyg. På samma sätt är det möjligt att samtidigt spärra dem.

Transport- och kommunikationsverket anser att användaren alltid ska ha vetskap om vilket identifieringsverktyg användaren ska använda och använder.

Användaren ska kunna lita på att alla skyldigheter i lagstiftningen alltid iakttas vid användning av det identifieringsverktyg som har tillhandahållits som identifieringsverktyg för stark autentisering till användaren genom ett avtal.

3.5.3 Bestämmelser

Autentiseringslag: 3 § Bestämmelsernas tvingande natur

Ett avtalsvillkor som avviker från bestämmelserna i denna lag till konsumentens nackdel är utan verkan, om inte något annat föreskrivs nedan.

[…]

Autentiseringslag: 15 § Skyldighet för leverantörer av identifieringsverktyg att lämna uppgifter innan avtal ingås (29.6.2016/533)

En leverantör av identifieringsverktyg ska innan ett avtal ingås informera den som ansöker om ett identifieringsverktyg om (29.6.2016/533)
1) tjänsteleverantören,
2) de tjänster som tillhandahålls och priserna på dem,
3) principerna för identifiering enligt 14 §,
4) parternas rättigheter och skyldigheter,
5) eventuella ansvarsbegränsningar,
6) förfarandena för klagomål och avgörande av tvister,
7) eventuella hinder för och begränsningar av användningen som avses i 18 §, och
8) övriga eventuella villkor för användning av identifieringsverktyget.

De uppgifter som avses i 1 mom. ska lämnas skriftligen eller elektroniskt så att den som ansöker om ett identifieringsverktyg kan spara och återge dem i oförändrad form. Om ett avtal på begäran av den som ansöker om ett identifieringsverktyg ingås genom distanskommunikation så att uppgifter och avtalsvillkor inte kan lämnas på det sätt som avses ovan innan avtalet ingås, ska uppgifterna utan dröjsmål lämnas på det nämnda sättet efter det att avtalet har ingåtts.

Bestämmelser om skyldigheten att lämna uppgifter vid behandlingen av personuppgifter finns i personuppgiftslagen.

Autentiseringslag: 20 § Beviljande av identifieringsverktyg (29.6.2016/533)

Utgivningen av identifieringsverktyg grundar sig på ett avtal mellan den som ansöker om verktyget och leverantören av identifieringstjänster. Avtalet ska ingås skriftligen. Avtalet kan även ingås elektroniskt om dess innehåll inte kan ändras ensidigt och det hålls

tillgängligt för parterna. Leverantören av identifieringstjänster ska bemöta sina kunder på ett icke-diskriminerande sätt och dem som ansöker om identifieringsverktyg jämlikt när avtalet ingås.

Avtalet kan gälla tills vidare eller för viss tid. Ett identifieringsverktyg kan ha en giltighetstid som är kortare än avtalets giltighetstid.

Identifieringsverktyg beviljas endast fysiska och juridiska personer. Bindningen mellan en fysisk persons och en juridisk persons identifieringsverktyg ska genomföras i enlighet med avsnitt 2.1.4 i bilagan till förordningen om tillitsnivåer vid elektronisk identifiering. Ett identifieringsverktyg ska vara personligt. Till ett identifieringsverktyg kan det vid behov fogas en uppgift om att innehavaren av identifieringsverktyget i enskilda fall även får företräda en annan fysisk person eller en juridisk person. (29.6.2016/533)

Autentiseringslag: 21 § (29.6.2016/533) Överlåtelse av identifieringsverktyg till sökande

Leverantören av ett identifieringsverktyg ska överlåta identifieringsverktyget till sökanden på det sätt som anges i avtalet. Leverantören ska säkerställa att verktyget inte obehörigt kommer i någon annans besittning vid överlåtelsen, på ett sådant sätt att åtminstone de krav uppfylls som gäller för tillitsnivån väsentlig enligt avsnitt 2.2.2 i bilagan till förordningen om tillitsnivåer vid elektronisk identifiering.

EU:s förordning om tillitsnivåer: 2.2.2 Utfärdande, leverans och aktivering

VÄSENTLIG

Efter utfärdandet levereras medlet för elektronisk identifiering via en mekanism genom vilken det kan antas att medlet levereras endast till ägaren.

Autentiseringslag: 22 § (29.6.2016/533) Förnyande av identifieringsverktyg

En leverantör av identifieringsverktyg får leverera ett nytt verktyg till en innehavare av identifieringsverktyg utan en uttrycklig begäran endast om ett verktyg som tidigare har tillhandahållits ska ersättas med ett nytt. När identifieringsverktyg förnyas ska de krav uppfyllas som gäller för tillitsnivån väsentlig enligt avsnitt 2.2.4 i bilagan till förordningen om tillitsnivåer vid elektronisk identifiering.

EU:s förordning om tillitsnivåer: 2.2.4 Förnyelse och ersättning

LÅG/VÄSENTLIG

Med beaktande av riskerna för ändring i personidentifieringsuppgifterna måste förnyelse eller ersättning uppfylla samma tillitskrav som det ursprungliga styrkandet och kontrollen av identiteten eller grundas på ett giltigt medel för elektronisk identifiering med samma eller högre tillitsnivå.

Autentiseringslag: 25 § Anmälan om återkallande eller förhindrande av användning av identifieringsverktyg

Innehavaren av ett identifieringsverktyg ska göra en anmälan till leverantören av identifieringsverktyget, eller någon annan aktör som denne har utsett, om verktyget har förkommit, obehörigen har kommit i någon annans besittning eller obehörigen har använts. (29.6.2016/533)

Leverantören av identifieringsverktyg ska se till att det är möjligt att när som helst göra en anmälan enligt 1 mom. Leverantören ska utan dröjsmål återkalla identifieringsverktyget eller förhindra dess användning efter det att anmälan har mottagits. (29.6.2016/533)

Leverantören av ett identifieringsverktyg ska på lämpligt sätt och utan dröjsmål i systemet registrera uppgifter om tidpunkten för återkallandet eller förhindrandet av användningen. Innehavaren av identifieringsverktyget har rätt att på begäran få ett intyg över att

innehavaren har gjort den anmälan som avses i 1 mom. Intyget ska begäras inom 18 månader från anmälan. (29.6.2016/533)

Systemet ska vara sådant att en tjänsteleverantör som använder identifieringstjänster lätt kan kontrollera uppgifterna i systemet vilken tid på dygnet som helst. Skyldighet att ordna möjlighet att kontrollera uppgifterna föreligger dock inte, om användning av identifieringsverktyget kan förhindras med hjälp av tekniska medel eller om verktyget kan spärras.

En tjänsteleverantör som använder identifieringstjänster ska i samband med användningen av ett identifieringsverktyg kontrollera uppgifterna om eventuella återkallanden och hinder i de system och register som leverantören av identifieringstjänster har. Detta behöver dock inte göras om användning av identifieringsverktyget kan förhindras med hjälp av tekniska medel eller om verktyget kan spärras.

Om en identifieringstjänst grundar sig på certifikat och uppgifter om återkallade certifikat ges med hjälp av en spärrlista, får den som tillhandahåller certifikattjänster registrera uppgifter om sådan kontroll av certifikatens giltighet som gjorts på spärrlistan. Certifikatutfärdaren kan alternativt lagra spärrlistan.

Autentiseringslag: 26 § (29.6.2016/533)Rätten för leverantörer av identifieringsverktyg att återkalla eller förhindra användning av identifieringsverktyg

Utöver vad som föreskrivs i 25 § får leverantören av ett identifieringsverktyg återkalla eller förhindra användningen av identifieringsverktyget, om

1) leverantören har skäl att misstänka att identifieringsverktyget används av någon annan än den som det har beviljats till,

2) identifieringsverktyget innehåller ett uppenbart fel,

3) leverantören har skäl att misstänka att säkerheten vid användningen av identifieringsverktyget har äventyrats,

4) innehavaren av identifieringsverktyget använder det på ett sätt som väsentligt strider mot avtalsvillkoren,

5) innehavaren av identifieringsverktyget har avlidit.

Leverantören av identifieringsverktyget ska så snart som möjligt underrätta innehavaren av identifieringsverktyget om att identifieringsverktyget har återkallats eller användningen av det förhindrats samt om tidpunkten för och orsakerna till detta.

Leverantören av identifieringsverktyget ska erbjuda en ny möjlighet att använda identifieringsverktyget eller tillhandahålla innehavaren ett nytt verktyg omedelbart efter det att en sådan orsak som avses 1 mom. 2 eller 3 punkten inte längre föreligger.

Autentiseringslag: 27 § Begränsningar av ansvaret för innehavaren vid obehörig användning av ett identifieringsverktyg

Innehavaren av ett identifieringsverktyg ansvarar för obehörig användning av verktyget endast om

1) innehavaren har överlåtit identifieringsverktyget till någon annan,

2) identifieringsverktyget har försvunnit, kommit i någon annans besittning obehörigt eller använts obehörigt på grund av innehavarens vårdslöshet, som inte är lindrig, eller

3) innehavaren har försummat att utan obefogat dröjsmål efter det att saken har upptäckts anmäla till leverantören av identifieringstjänster eller någon annan aktör som denne har angett att identifieringsverktyget har försvunnit, kommit i någon annans besittning obehörigt eller använts obehörigt.

Innehavaren av ett identifieringsverktyg ansvarar dock inte för obehörig användning av verktyget

1) till den del identifieringsverktyget har använts efter det att innehavaren har anmält till leverantören av identifieringstjänster att identifieringsverktyget har försvunnit, kommit i någon annans besittning obehörigt eller använts obehörigt,

2) om innehavaren av identifieringsverktyget inte har kunnat göra en anmälan utan obefogat dröjsmål efter det att saken har upptäckts om att verktyget har försvunnit, kommit i någon annans besittning obehörigt eller använts obehörigt på grund av att leverantören av identifieringstjänster har åsidosatt skyldigheten enligt 25 § 2 mom. att se till att innehavaren av ett identifieringsverktyg har möjlighet att när som helst göra en sådan anmälan, eller

3) om en tjänsteleverantör som använder identifieringstjänster har åsidosatt sin skyldighet enligt 18 § 4 mom. och 25 § 5 mom. att kontrollera om det finns begränsningar för användningen av identifieringsverktyget eller uppgift om hinder för användningen av eller spärrning av verktyget.

3.6 Behandling av personuppgifter, identifieringstransaktioner och loggdata

3.6.1 Allmänt

I 6 § och 7 § i autentiseringslagen finns bestämmelser om behandling av personuppgifter vid stark autentisering. RP 237/2020 föreslår att 6 § ska ändras. Enligt lagstiftningen är befolkningsdatasystemet den betrodda källan till uppgifter.

Bestämmelser om behandling av personuppgifter finns främst i EU:s allmänna dataskyddsförordning och bestämmelser om användning av personbeteckningar i 29 § i dataskyddslagen.

Behandling av personuppgifter med stöd av autentiseringslagen, den allmänna dataskyddsförordningen och dataskyddslagen övervakas av dataombudsmannen.

I 24 § i autentiseringslagen finns bestämmelser om registrering av uppgifter om identifieringstransaktioner och tillåtna grunder för användning av registrerade uppgifter. Dessutom innehåller paragrafen bestämmelser om skyldighet att föra behandlingsloggar.

I 12 § i Transport- och kommunikationsverkets föreskrift 72 fastställs de obligatoriska personuppgifter (*obligatoriska attribut*) som en identifieringstjänst ska kunna tillhandahålla i förtroendenätet och de valfria personuppgifter (*optionella attribut*) som tjänsten ska ha en planerad beredskap att tillhandahålla. Syftet med föreskriften är att garantera interoperabiliteten i identifieringen. Uppgifterna är helt förenliga med eIDAS-förordningen (kommissionens genomförandeförordning (EU) 2015/1501), och syftet med förordningen är att vid behov även garantera gränsöverskridande interoperabilitet.

Hänsyn bör tas till att bestämmelserna om stark autentisering inte kräver att obligatoriska eller valfria attribut ska levereras eller bekräftas för en förlitande part. Tjänster för stark autentisering kan även kommersialiseras så att en förlitande part endast får pseudonymer eller exempelvis uppgifter om att de som har identifierat sig är myndiga.

3.6.2 Riktlinjer

Transport- och kommunikationsverket anser att bestämmelserna om stark autentisering utgör en med dataskyddsförordningen förenlig grund för behandling av de personuppgifter som fastställs i 12 b § 2 punkten i autentiseringslagen och i

Transport- och kommunikationsverkets föreskrift som utfärdats med stöd av autentiseringslagen. Bestämmelserna i autentiseringslagen gäller inte enbart uppgifter som identifierar och beskriver en person utan även registrering av identifieringstransaktioner, och de förpliktelser som gäller informationssäkerhet kräver olika tekniska loggningar.

Autentiseringslagen gäller inte icke-registrerad identifiering och fastställer ingen grund för behandling av personuppgifter i icke-registrerade identifieringstjänster. Det innebär att personuppgiftsansvariga separat i enlighet med dataskyddsförordningen och dataskyddslagen ska motivera och utvärdera grunderna för behandling av personuppgifter, överlåtelsen till tjänster för ärendehantering och hanteringen av loggdata vid icke-registrerad identifiering. Hänsyn bör tas till att grunden för behandling av personuppgifter även kan påverka de registrerades rättigheter. Dessutom ska hanteringen av loggdata vid icke-registrerad identifiering utvärderas på någon annan grund än baserat på 24 § i autentiseringslagen.

Om andra personuppgifter än dem som avses i bestämmelserna om identifiering (s.k. berikade data) tillhandahålls i anslutning till en stark autentisering, ska grunden för behandling av sådana personuppgifter utvärderas separat utifrån dataskyddsförordningen.

3.6.3 Bestämmelser

Det har föreslagits att 6 § i autentiseringslagen skulle ändras (RP 237/2020). Enligt förslaget ska skyldigheten gällande behandling av personbeteckningar fortfarande föreskrivas. Syftet med lagändringen är inte att ändra rättsläget. Enligt bedömningar följer de skyldigheter som fastställs i lag 533/2016 däremot redan av dataskyddsförordningen och dataskyddslagen.

Föreslagna 6 § Behandling av personbeteckningar i autentiseringslagen

När leverantörer av identifieringstjänster och certifikatutfärdare som tillhandahåller betrodda tjänster kontrollerar sökandens identitet ska de kräva att sökanden uppger sin personbeteckning.

Se även dataskyddslagen 1050/2018 och (EU) 2016/679 (allmän dataskyddsförordning).

Autentiseringslag: 7 § (20.2.2015/139) Användning av uppgifter i befolkningsdatasystemet

Leverantörer av identifieringsverktyg och certifikatutfärdare som tillhandahåller betrodda tjänster ska hämta och uppdatera de uppgifter som de behöver för tillhandahållandet av identifieringstjänster för fysiska personer med användning av befolkningsdatasystemet. Leverantörer av identifieringstjänster ska dessutom säkerställa att de uppgifter som de behöver för tillhandahållandet av identifieringstjänster är uppdaterade enligt uppgifterna i befolkningsdatasystemet. (29.6.2016/533)

[…]

Autentiseringslag: 8 § (29.6.2016/533) Krav på system för elektronisk identifiering

[…]

Bestämmelserna i 1 mom. hindrar inte att specifika tjänster tillhandahålls så att leverantören av identifieringstjänster meddelar den tjänsteleverantör som använder en identifieringstjänst den pseudonym som innehavaren av identifieringsverktyget använder eller endast ett begränsat antal personuppgifter.

Autentiseringslag: 24 § (29.6.2016/533) Registrering och användning av uppgifter om identifieringstransaktioner och identifieringsverktyg

Leverantörer av identifieringstjänster ska registrera

1) de uppgifter som behövs för att verifiera en enskild identifieringstransaktion eller elektronisk underskrift,

2) uppgifter om i 18 § avsedda hinder och begränsningar som gäller användningen av identifieringsverktyg,

3) i fråga om certifikat, uppgifter om innehållet i certifikat enligt 19 §.

Leverantörer av identifieringsverktyg ska registrera behövliga uppgifter om den inledande identifiering av sökande som avses i 17 och 17 a § och om de handlingar eller den elektroniska identifiering som använts i den inledande identifieringen.

De uppgifter som avses i 1 mom. 1 punkten ska lagras i fem år från identifieringstransaktionen. De övriga uppgifter som avses i 1 och 2 mom. ska lagras i fem år från det att ett fast kundförhållande har upphört.

Personuppgifter som har uppkommit i samband med en identifieringstransaktion ska förstöras efter transaktionen, om det inte är nödvändigt att registrera dem för att verifiera en enskild identifieringstransaktion.

Leverantören av identifieringstjänster får behandla registrerade uppgifter endast för att tillhandahålla och upprätthålla tjänsterna, fakturera, trygga sina rättigheter vid tvister och utreda missbruk samt på begäran av en tjänsteleverantör som använder identifieringstjänster eller en innehavare av ett identifieringsverktyg. Leverantören av identifieringstjänster ska registrera uppgifter om när och varför uppgifterna behandlats och vem som gjort det.

Om en tjänsteleverantör endast ger ut identifieringsverktyg

1) tillämpas inte 1 mom. 1 punkten och 4 mom. på tjänsteleveratören,

2) räknas den registreringstid på fem år som avses i 3 mom. från det att identifieringsverktyget upphörde att gälla.

M72: 12 § Minimiuppsättning uppgifter som ska förmedlas i förtroendenätet

Följande uppgifter ska förmedlas via gränssnitten mellan leverantörer av identifieringsverktyg och leverantörer av tjänster för identifieringsförmedling:

1) vid identifiering av en fysisk person, åtminstone den identifieringsuppgift som identifierar personen, personens förnamn, efternamn och födelsedatum,

2) vid identifiering av en juridisk person, åtminstone den identifieringsuppgift som identifierar den fysiska personen som företräder den juridiska personen, personens efternamn och förnamn och den identifieringsuppgift som identifierar organisationen,

3) om identifieringsverktyget ligger på tillitsnivån väsentlig eller hög.

Gränssnitten mellan leverantörer av identifieringsverktyg och leverantörer av tjänster för identifieringsförmedling ska ha beredskap att förmedla följande uppgifter:

1) om en identifieringstransaktion gäller en offentlig eller en privat tjänst för ärendehantering,

2) vid identifiering av en fysisk person; förnamn och efternamn vid födseln, födelseort, nuvarande adress och kön

3.7 Bestämmelser om förtroendenätets avtalsskyldigheter och samarbete

3.7.1 Allmänt

I 12 a § i autentiseringslagen finns bestämmelser om förtroendenätet för leverantörer av tjänster för stark autentisering. Förtroendenätet består av de identifieringstjänster som har gjort en anmälan enligt autentiseringslagen och som Transport- och kommunikationsverket har godkänt för registret. Termen förtroendenätet används i stor utsträckning som synonym till stark autentisering. I strikt bemärkelse innebär förtroendenätet emellertid skyldighet för leverantörer av identifieringsverktyg att till tjänster för identifieringsförmedling överlåta tillträdesrätt till identifieringstjänster samt därtill hörande bestämmelser om avtalsvillkor. Dessutom är identifieringstjänsterna skyldiga att samarbeta för att säkerställa en teknisk interoperabilitet.

I 16 § i lagen finns bestämmelser om bland annat anmälan om betydande hot och störningar som riktas mot tjänsternas funktion, informationssäkerheten eller användningen av en elektronisk identitet till avtalsparterna i förtroendenätet.

I 12 a § 5 punkten finns bestämmelser om begränsningar av behandlingen av sådan information om en annan leverantör av identifieringstjänster som erhållits i samband med överlåtelse av tillträdesrätt eller med stöd av 16 § och om skyldighet att ersätta en skada som orsakats av en användning som har stridit mot bestämmelsen.

3.7.2 Riktlinjer

Bestämmelserna om förtroendenätet i autentiseringslagen, dvs. bestämmelserna om överlåtelse av tillträdesrätt till identifieringstjänster, avtalsvillkor, hantering av störningar och därtill hörande särskilda sekretesskyldigheter, gäller endast stark autentisering.

Förmedling av icke-registrerad elektronisk identifiering omfattas inte av bestämmelserna om tillträdesrätt för förtroendenätet, men autentiseringslagen utgör inget hinder för förmedling på någon annan grund.

3.7.3 Bestämmelser

12 a § (29.3.2019/412) Förtroendenätet för leverantörer av identifieringstjänster

En leverantör av identifieringstjänster ansluter sig till förtroendenätet när leverantören gör en anmälan enligt 10 § till Transport- och kommunikationsverket.

En leverantör av identifieringsverktyg ska erbjuda leverantörer av tjänster för identifieringsförmedling tillträdesrätt till sina identifieringstjänster så att leverantörerna kan förmedla identifieringstransaktioner till en part som förlitar sig på en elektronisk identifiering. En leverantör av identifieringsverktyg ska upprätta leveransvillkor för tillträdesrätt till sin identifieringstjänst och tillämpa dem vid ingående av avtal med leverantörer av tjänster för identifieringsförmedling. Villkoren för tillträdesrätten ska vara förenliga med denna lag samt rimliga och icke-diskriminerande. Leverantören av identifieringsverktyg ska godkänna en begäran av en leverantör av tjänster för identifieringsförmedling om att ingå ett avtal enligt leveransvillkoren samt bevilja tillträdesrätt till identifieringstjänsten utan dröjsmål och senast inom en månad efter att begäran har gjorts. Leverantören av identifieringsverktyg kan vägra ingå avtal endast om leverantören av tjänster för identifieringsförmedling handlar i strid med denna lag eller de bestämmelser som utfärdats eller de föreskrifter som meddelats med stöd av den eller om det finns andra vägande skäl för vägran.

Leverantörer av identifieringstjänster ska samarbeta för att säkerställa att de tekniska gränssnitten mellan medlemmarna i förtroendenätet är kompatibla och att de gör det möjligt att tillhandahålla gränssnitt som följer allmänt kända standarder för de förlitande parterna.

Leverantörer av identifieringstjänster ska genomföra underhålls-, ändrings- och informationssäkerhetsåtgärder på ett sådant sätt att åtgärderna innebär minsta möjliga olägenhet för identifieringstjänsternas övriga leverantörer, användare och förlitande parter. Utöver det som föreskrivs i 25 och 26 § får en leverantör av identifieringstjänster tillfälligt utan en annan leverantörs samtycke avbryta tillhandahållandet av en identifieringstjänst eller begränsa dess användning, om det är nödvändigt för att de åtgärder som avses ovan ska kunna genomföras framgångsrikt. Övriga leverantörer av identifieringstjänster vilkas tjänster kan påverkas av avbrott och ändringar ska effektivt informeras om dessa.

En leverantör av identifieringstjänster får använda sådan information om en annan leverantör av identifieringstjänster som den erhållit i samband med överlåtelse av tillträdesrätt eller med stöd av 16 § endast för det ändamål för vilket informationen har lämnats till leverantören av identifieringstjänster. Uppgifterna får behandlas endast av den som arbetar hos eller för en leverantör av identifieringstjänster och som nödvändigt behöver uppgifterna i sitt arbete. Uppgifterna ska också annars behandlas så att affärshemligheter som tillhör en annan leverantör av identifieringstjänster inte röjs. En leverantör av identifieringstjänster som genom att handla i strid med detta moment vållar en annan leverantör av identifieringstjänster skada är skyldig att ersätta skadan.

Närmare bestämmelser om förtroendenätets administrativa praxis, tekniska gränssnitt och administrativa ansvar utfärdas genom förordning av statsrådet.

16 § (29.3.2019/412) Anmälningar av leverantörer av identifieringstjänster om hot och störningar som riktas mot verksamheten eller skyddet av uppgifter

En leverantör av identifieringstjänster ska trots sekretessbestämmelserna utan ogrundat dröjsmål anmäla betydande hot och störningar som riktas mot tjänsternas funktion, informationssäkerheten eller användningen av en elektronisk identitet till de tjänsternas förlitande parter, till innehavarna av identifieringsverktyg, till övriga avtalsparter i förtroendenätet och till Transport- och kommunikationsverket. I anmälan ska det redogöras för de åtgärder som olika aktörer har tillgång till för att avvärja hot eller störningar samt de beräknade kostnaderna för åtgärderna.

Leverantören av identifieringstjänster får trots sekretessbestämmelserna underrätta alla medlemmar i förtroendenätet om hot och störningar som avses i 1 mom. samt om tjänsteleverantörer som skäligen kan misstänkas för att eftersträva orättmätig ekonomisk vinning, lämna betydelsefull osann eller vilseledande information eller behandla personuppgifter på ett olagligt sätt.

Transport- och kommunikationsverket får för anmälarens räkning på teknisk väg förmedla uppgifterna mellan parterna i förtroendenätet trots vad som föreskrivs i lagen om offentlighet i myndigheternas verksamhet (621/1999).

Bilaga: Sammanfattning av utlåtandena om promemorian av den 27 mars 2020

Utlåtanden lämnades in av Avaintec Oy, Danske Bank A/S, filial i Finland, Myndigheten för digitalisering och befolkningsdata, Elisa Abp, FiCom rf, Finans Finland, Konkurrens- och konsumentverket, Nets Denmark A/S, Branch Norway, OP Andelslag och S-Banken Ab.

I flera utlåtanden stödde organisationerna (KKV, Nets, Elisa, FiCom, MDB) utgångspunkterna för och preciseringen av promemorian, tryggande av kraven på stark autentisering, en tillräcklig åtskillnad av stark autentisering och icke-registrerad identifiering samt en klar syn på användarens ställning. Promemorian och riktlinjerna ansågs vara motiverade.

Danske Bank och S-Banken begärde preciseringar.

Nedan behandlas utlåtandena efter tema

Främja marknaden och utvecklingen

KKV konstaterade att användning av ett enda identifieringssystem för att tillhandahålla verktyg för både stark autentisering och svag identifiering kan underlätta tillträdet till marknaden för elektronisk identifiering och att det i sin tur främjar konkurrensen och bidrar till en välfungerande marknad.

I utlåtandena från Elisa, bankerna och Finans Finland framförde organisationerna motsatta åsikter om huruvida anvisningarna i tolkningspromemorian skapar förutsättningar för att utveckla identifieringstjänsterna eller huruvida de utgör hinder för att utnyttja teknik.

Elisa ansåg att de riktlinjer som Traficom nu föreslår möjliggör en konkurrens mellan inhemska alternativ med Google, Facebook och Apple som har nått längst i utvecklingen.

Den omständigheten att kraven kan förutses ansågs vara bra för den pågående utvecklingen av tjänsterna. Å andra sidan poängterade organisationerna att stela och detaljerade definitioner inte är ändamålsenliga och att de utvecklingsmöjligheter som till exempel biometriska autentiseringsfaktorer medför ännu inte kan förutsägas.

- Transport- och kommunikationsverket anser att båda synpunkterna är korrekta och motiverade. I myndighetsstyrningen är det viktigt att hitta en god balans mellan förutsebarhet i krav och smidig teknisk utveckling. Därför ges nu anvisningar i form av en tolkningspromemoria, inte till exempel i form av en föreskrift.

- **I promemorian har Transport- och kommunikationsverket lagt till en precisering av den juridiska karaktären i förhållande till bestämmelserna och ändrat vissa riktlinjer så att de till karaktären är mer allmänna.**

Användarnas rättigheter

KKV och banksektorn framförde någorlunda motsatta åsikter om huruvida det är relevant att för användare förtydliga när de använder en stark autentisering respektive en icke-registrerad identifiering.

Enligt KKV är det viktigt att man på det sätt som beskrivs i promemorian ser till att verktygen skiljs åt i tillräcklig utsträckning och att avtalsvillkoren är begripliga. När konsumenter använder identifieringsverktyg, får det inte vara oklart för dem om det är fråga om en svag identifiering eller en lagstadgad stark autentisering. Som det i utkastet till promemoria beskrivs bör hänsyn tas till att identifieringssättet kan urskiljas utifrån de egenskaper som användaren kan upptäcka och till att användarens rättigheter förverkligas, när metoderna för stark autentisering och svag idenfiering genomförs. Skillnaderna mellan tjänster för svag identifiering respektive stark autentisering ska kunna uppfattas utifrån villkoren för tjänsterna. Villkoren för svag identifiering och stark autentisering får inte på något annat sätt skapa oklarhet om vad konsumenterna förbinder sig till när de godkänner villkoren.

Finans Finland och OP ansåg i sin tur att nivån på en identifieringsmetod och den åtskillnad som avses i utkastet till promemoria inte har någon betydelse för användare. Det viktigaste för användare är enkelhet och att användarens förtroende utgår från tjänsteleverantören, inte från identifieringstjänstens status som stark. På denna grund ansåg organisationerna att åtskillnaden av en stark autentiseringsmetod och en icke-registrerad identifieringsmetod inte skulle ha någon betydelse för användare. De ansåg att en stark autentisering låg i den förlitande partens intresse, inte i användarens intresse.

- Transport- och kommunikationsverket konstaterar att bedömningarna av en medelanvändares intresse för en identifieringstjänsts status kan vara relevanta, men att detta egentligen bara betonar behovet att ge information om identifieringstjänster. Användare ska enkelt kunna upptäcka vilken identifiering de använder och vilka villkoren för identifieringen är.

OP och Finans Finland ansåg att det ur användarens synvinkel är bättre att använda processer tillhandahållna av den som beviljat identifieringsverktyg för stark autentisering, och tekniker med färre identifieringselement eller kontroller, än att ta fram olika lösningar och dela ut flera olika koder till användare eller att endast använda allmänt användbara identifieringsverktyg som fungerar på en låg nivå. I sitt utlåtande poängterade OP att åtskillnaden kan medföra oklarhet, till exempel när identifieringsverktyg behöver spärras.

- Syftet med tolkningspromemorian är att förtydliga de ramvillkor enligt vilka det är möjligt att även tillhandahålla identifieringsmetoder på en låg nivå i ett och samma system.

- **Punkten om spärrning av identifieringsverktyget och hantering av livscykler har förtydligats.** Metoderna ska skiljas åt om två olika förfaranden tillämpas vid en stark autentisering och en icke-registrerad identifiering.

Termen svag identifiering

I sitt utlåtande kritiserade Avaintec användningen av termen *svag identifiering*.

- Transport- och kommunikationsverket var av samma åsikt om att ordet innehåller onödiga värdeomdömen. Därför har Transport- och kommunikationsverket i fråga om definitionen i promemorian särskilt understrukit att det är fråga om registrering och tillsyn, inte om identifieringens kvalitet. Transport- och kommunikationsverket anser att utmaningen med ordet *låg* är att denna hänvisar till den lägsta tillitsnivån i eIDAS och att det på samma sätt kan saknas objektiv information om hur den lägsta tillitsnivån har genomförts.

- **I promemorian har uttrycket svag identifiering ersatts med icke-registrerad identifieringsmetod.**

PSD2

I sina utlåtanden lyfte bankernas företrädare fram att den viktigaste lagstiftningen om bankidentifiering bygger på PSD2 och att kraven på stark autentisering vid betaltjänster härrör från kommissionens tekniska standard för tillsyn och EBA:s och Finansinspektionens tolkningar. Man frågade om det är ändamålsenligt att i promemorian lägga till hänvisningar och eventuella nya tolkningar av *förhållandet mellan ansvarsbestämmelserna* i betaltjänstlagen och autentiseringslagen när det gäller icke-registrerad identifiering och svag elektronisk identifiering. Man önskade tolkningssamarbete med Transport- och kommunikationsverket och Finansinspektionen.

I ett utlåtande ansåg organisationen att betaltjänstlagen ska tillämpas i stället för autentiseringslagen, eftersom identifieringsverktyg används för att använda betaltjänster. Man uttalade sig även om att syftet inte kan vara att dedikerade identifieringsverktyg börjar tas fram i Finland enbart för att godkänna betalningar enligt PSD2.

- **Transport- och kommunikationsverket har lagt till ett omnämnande om PSD2-reglerna.**

- Frågor gällande teknisk samordning eller samordning av ansvarsbestämmelser kan dessvärre inte behandlas närmare i denna promemoria, utan det kommer om möjligt att göras i andra sammanhang. I utlåtandena lyfte man fram gränssnittet för kortbetalningar och ansvarsbestämmelserna. I utlåtandena lyfte man inte i övrigt fram krav vars samordning riktlinjerna ska kunna gälla.

- År 2018 granskade Transport- och kommunikationsverket och Finansinspektionen tekniska krav utgående från att lagarna tillämpas parallellt och skillnaderna ska uppfylla kraven i den lag som för tillfället är strängare eller noggrannare. Transport- och kommunikationsverket konstaterar att utvecklingen av båda lagarna och tolkningen på EU-nivå kommer att medföra nya samordningsfrågor som ska avgöras och som kräver samarbete mellan tillsynsmyndigheterna.

- **Syftet med Transport- och kommunikationsverkets styrning och tillsyn är att en och samma identifieringsmetod kan användas som ett allmänt användbart identifieringsverktyg och som ett identifieringsverktyg enligt PSD2-reglerna.**

Autentiseringsfaktorer och hemligheter

Bland de detaljerade riktlinjerna i utkastet till promemoria ansågs det inte vara ändamålsenligt att olika lösenord bör användas för en stark autentiseringsmetod respektive en svag identifieringsmetod. Detta motiverades med erfarenheterna i tillhandahållandet av tjänster om att kravet på att komma ihåg olika lösenord medför nackdelar som är större än eventuella fördelar med åtskillnaden. Som jämförelsepunkt hänvisade man till att ett och samma lösenord används utan problem vid både debit-betalningar och credit-betalningar med betalkort.

- **Utifrån utlåtandena har Transport- och kommunikationsverket ändrat riktlinjen för åtskillnad av autentiseringsfaktorer i tolkningspromemorian.**

- **Dessutom har Transport- och kommunikationsverket utvärderat åtskillnaden av kryptografiska hemligheter och lättat på sin tolkning i utkastet.**

Inledande identifiering

Utöver det egentliga temat i promemorian underströk utlåtandena behovet att fastställa krav på inledande fjärridentifiering.

- Precisering av kraven för bedömning av inledande fjärridentifiering är ett separat uppdrag från denna tolkningspromemoria.

- Tolkningspromemorian innefattar dock riktlinjer för vilka faktorer som ska beaktas när en icke-registrerad identifieringsmetod ändras till en stark metod.

Annat

Utlåtandena innehöll enskilda önskemål och förslag till precisering.

- **Transport- och kommunikationsverket har preciserat en del formuleringar i promemorian.**

Utlåtandena innehöll önskemål om att Transport- och kommunikationsverket ska vidta åtgärder för att öka användarnas förståelse av bland annat skillnaderna mellan identifiering och elektronisk signatur, och även lyfta fram och främja andra e-tjänster än tjänsterna för stark autentisering.

- **Transport- och kommunikationsverket tackar för att dessa frågor har lyfts fram och beaktar om möjligt frågorna i andra sammanhang inom ramen för sin behörighet**