

Transport- och kommunikationsverkets promemoria om tolkning av användning av körkort vid styrkande av en persons identitet när personens identifieringsverktyg är låst eller när personen ska beviljas ett nytt identifieringsverktyg eller en ny autentiseringsfaktor

1 Fråga och syfte med promemorian

Leverantörerna av identifieringstjänster har begärt anvisningar för följande situationer av Transport- och kommunikationsverket (Traficom):

Frågorna gäller situationer där identifieringsverktyget har beviljats före den 1 januari 2019 och kundens identifieringsverktyg öppnas på nytt efter att verktyget har varit låst, eller där kunden beviljas ett nytt identifieringsverktyg eller en ny autentiseringsfaktor efter att kunden exempelvis har tappat sitt identifieringsverktyg eller sin autentiseringsfaktor.

- Handlar dessa olika åtgärder för att identifiera en kund om en sådan inledande identifiering som avses i autentiseringslagen?
- Vilka krav bör uppfyllas vid identifiering av en kund om det inte handlar om ovannämnda inledande identifiering?
- Kan körkortet användas vid identifiering av en kund i ovannämnda situationer, trots att körkortet inte längre efter den 1 januari 2019 är en giltig handling vid inledande identifiering?

Enligt Transport- och kommunikationsverkets uppfattning har branschen varierande praxis om huruvida det i ovannämnda situationer krävs identitetskort eller pass.

Med tanke på autentiseringslagen påverkas bedömningen av kraven i förordningen om tillitsnivåer (EU) 2015/1502 (LOA) och av de lagbestämmelser som har samlats till denna promemoria.

Syftet med denna promemoria är att ge aktörerna förhandsanvisningar om Traficoms tolkning utifrån autentiseringslagen. I promemorian har hänsyn inte tagits till på vilket sätt regleringen av finanssektorn eventuellt påverkar frågan.

2 Sammanfattning

Traficom anser att ovannämnda rådgivningstillfälle inte handlar om inledande identifiering.

Traficom anser att kontroll av en persons körkort inte kan vara den enda åtgärden för att säkerställa att identifieringsverktyget inte obehörigt kommer i någon annans

besittning vid förnyelse/ersättning eller återaktivering. Om en person ges (alla) delfaktorer som behövs för att använda ett identifieringsverktyg, är ett pass eller körkort de enda godtagbara handlingarna för kontroll av personens identitet.

Förfarandet för förnyelse/ersättning eller återaktivering kan även omfatta uppvisande av körkortet. Överlåtelse och andra åtgärder bör dock omfatta andra kontroller som säkerställer att identifieringsverktyget och de delfaktorer som behövs för att använda verktyget kan antas bli levererade enbart till ägaren av identifieringsverktyget, även om körkortet är förfalskat eller stulet. Även i sådana situationer rekommenderas, att man hellre använder pass eller identitetskort.

3 Bedömning utifrån lagbestämmelser: Handlar det om inledande identifiering?

3.1 Kraven på inledande identifiering i autentiseringslagen

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, Schweiz eller i San Marino. 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.

RP 74/2016:

Paragrafens 2 mom. ändras så att leverantören av identifieringsverktyg i inledande identifiering, när identifieringen endast grundar sig på en identitetshandling som beviljats av en myndighet, vid kontrollen av identiteten inte längre får använda endast ett körkort som beviljats av en myndighet i Finland eller i någon annan medlemsstat i Europeiska ekonomiska samarbetsområdet. Bestämmelsen har en övergångsperiod till utgången av 2018. Från och med 2019 kan ett identifieringsverktyg inte längre beviljas genom att använda endast körkort vid kontrollen av identiteten i den inledande identifieringen av en person. Ändringen av praxis är nödvändig för att körkort inte längre kan anses vara ett intyg om identitet utan ett intyg om körrätt.

Motivering till övergångsbestämmelsen: Enligt 2 mom. får en leverantör av identifieringsverktyg till och med den 31 december 2018 som ett i 17 § 2 mom. i denna lag avsett godkänt dokument också använda ett giltigt körkort som har beviljats

efter den 1 oktober 1990 av en medlemsstat i Europeiska ekonomiska samarbetsområdet. En inledande identifiering som gjorts med stöd av körkort senast den 31 december 2018 uppfyller kraven i den föreslagna lagen och den inledande identifieringen behöver inte ytterligare säkerställas på något annat sätt.

3.2 Bedömning av frågan

Enligt 2 § i autentiseringslagen avses med inledande identifiering verifiering av identiteten hos den som ansöker om ett identifieringsverktyg, när verifieringen sker i samband med att verktyget skaffas.

RP 74/2016:

Med inledande identifiering som definieras i paragrafens 7 punkt avses verifiering av identiteten hos en fysisk person eller verifiering av en juridisk persons status som juridisk person innan verktyget beviljas. Den inledande identifieringen är den centrala grundpelaren i fråga om tillförlitligheten i stark autentisering. Den regleras i 17 § i den gällande lagen. Inledande identifiering är en term som etablerats i autentiseringslagen. Med hjälp av den ville man tydligt skilja denna särskilda identifiering från senare identifieringstransaktioner som upprepas flera gånger.

Det verkar inte som om tolkningsbegäran handlar om en i förarbetena avsedd situation där identiteten hos den som ansöker om ett identifieringsverktyg verifieras innan verktyget beviljas.

Begäran har begränsats till en situation där en sökande saknas och det i stället finns en innehavare av ett redan tidigare beviljat identifieringsverktyg.

Traficom anser att ovannämnda rådgivningstillfälle inte handlar om inledande identifiering. Det kan även konstateras att det inte heller handlar om sådana identifieringstransaktioner med identifieringsverktyg som hänvisas till i slutet av den citerade punkten i förarbetena för lagen.

4 Bedömning utifrån lagbestämmelser: Vill krav kan tillämpas när det inte handlar om inledande identifiering?

Även om situationen i tolkningsbegäran inte handlar om inledande identifiering, är det utifrån detta faktum ännu inte möjligt att dra slutsatser av vilka krav som kan tillämpas vid identifiering av innehavare av identifieringsverktyg i situationer som avses i begäran.

4.1 Situationer som skiljs åt i förordningen om tillitsnivåer och autentiseringslagen

I förordningen om tillitsnivåer och autentiseringslagen behandlas separat *utfärdande/överlåtelse* och *förnyelse/ersättning*.

Dessutom behandlar förordningen om tillitsnivåer *återaktiveringen*. Autentiseringslagen innehåller inga bestämmelser om återaktivering.

Situationerna har inte definierats noggrant och därför ska följande frågor behandlas:

- Vilken betydelse har den omständigheten att endast en del av autentiseringsfaktorerna ersätts?

- Ett exempel är när en ny kodtabell levereras i stället för en förkommen tabell.
- Vilken betydelse har orsaken till ersättningsbehovet (förkommet, låst, föråldrat eller något annat)?
- Vilken betydelse har den faktorn att kontoret till exempel överlämnar alla autentiseringsfaktorer som behövs för att använda identifieringsverktyget till personen?
- Vilket är fallet om det vid leverans används andra processer än överlåtelse personligen?
- På vilket sätt klassificeras ibruktagandet av en kodapp (en mobilapp), om det inte sker på elektronisk väg utifrån det tidigare utfärdade identifieringsverktyget?

I fråga om *förnyelse* och *ersättning* påpekar förordningen om tillitsnivåer att samma krav som det ursprungliga styrkandet och kontrollen av identiteten måste uppfyllas med beaktande av riskerna för ändring i personuppgifterna.

Kraven på *utfärdande*, *leverans* och *överlåtelse* förutsätter att en leverantör säkerställer att verktyget inte obehörigt kommer i någon annans besittning.

4.2 Samlade krav på identifieringssystem och identifieringsmetod

8 § i autentiseringslagen (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 §,*

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,*

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 --.

2.2.1 i LOA Medel för elektronisk identifiering: egenskaper och utformning

Låg

2. *Medlet för elektronisk identifiering är utformat så att utfärdaren vidtar rimliga åtgärder för att kontrollera att det endast används under ägarens kontroll eller innehav.*

Tillämpningsguide¹:

När det hänvisas till åtgärder för att kontrollera att medlet för elektronisk identifiering används under ägarens kontroll bör hänsyn tas till att åtgärderna endast kan vara sådana som utfärdaren rimligen kan förväntas vidta. Det praktiska genomförandet har samband med de krav som nämns i avsnitt 2.2.2.

--

Väsentlig

--

2. Medlet för elektronisk identifiering är utformat så att det kan antas att det endast används under ägarens kontroll eller innehav.

--

4.3 Krav på överlåtelse, utfärdande, leverans och aktivering

21 § i autentiseringslagen (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 överlåtelser, 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.

RP 36/2009, s. 62: Den som tillhandahåller identifieringstjänsten står för risken i samband med att identifieringsverktyget, inklusive de specificerande uppgifter som behövs vid användningen av verktyget, skickas till betalaren. Ansvar övergår enligt 23 § 1 mom. till innehavaren av identifieringsverktyget först när denne har tagit emot verktyget. Tjänsteleverantören är skyldig att bevisa att innehavaren av identifieringsverktyget har tagit emot verktyget och de specificerande uppgifter som eventuellt behövs vid användningen av verktyget.

2.2.2 i LOA 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.

(Hög:

Aktiveringsprocessen kontrollerar att medlet för elektronisk identifiering endast levereras till ägaren.)

Tillämpningsguide:

Möjliga mekanismer är till exempel följande:

- personlig leverans
- leverans som ett rekommenderat brev
- en sådan aktiveringsmetod där det rimligen kan antas att endast personen har de uppgifter som behövs för aktivering, till exempel en standardpinkod som levereras åtskild från identifieringsmedlet.

På nivån "väsentlig" ska flera autentiseringsfaktorer användas. Aktiveringskoder behövs inte nödvändigtvis. Kraven på nivån "väsentlig" kan uppfyllas med många olika kombinationer av utfärdande, leverans och aktivering:

- Medlet för elektronisk identifiering kan levereras per post och aktiveringen kan göras genom att skicka koden till personens bankkonto. Sökanden

¹ En inofficiell rekommendation för tillämpning, utfärdad av medlemstaternas och kommissionens samarbetsgrupp

https://www.kyberturvallisuuskeskus.fi/sites/default/files/media/file/LOA_Guidance.pdf

anger en kod för att aktivera medlet för elektronisk identifiering. Antagandet är att bankens autentisering ska vara minst på nivån "väsentlig".

- Medlet för elektronisk identifiering och aktiveringskoden levereras åtskilda per post till personens adress som har autentiserats.
- Medlet för elektronisk autentisering levereras per post till sökandens adress.
- Medlet för elektronisk identifiering överlämnas när sökandens identitet har autentiserats.

4.4 Krav på förnyande och ersättning

22 § i autentiseringslagen (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.

2.2.4 i LOA Förnyelse och ersättning

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.

(Hög:

Nivå väsentlig, samt om förnyelse eller ersättning grundas på ett giltigt medel för elektronisk identifiering, kontrolleras identitetsuppgifterna mot en tillförlitlig källa.)

Traficom anser att kravet i förordningen om tillitsnivåer om att samma krav som det ursprungliga styrkandet och kontrollen av identiteten måste uppfyllas avser särskilt avsnitt 2.1.1 i förordningen, men att det även kan anses vara ett allmänt krav på att alla tidigare krav angående tilliten ska uppfyllas trots förnyelse/ersättning (som i fråga om återaktivering i avsnitt 2.2.3 punkt 3 i LOA).

2.1.2 i LOA Styrkande och kontroll av identitet

Väsentlig:

Nivå låg, samt ett av de alternativ som anges i punkterna 1–4 måste vara uppfyllt: 1. Kontroll har skett av att personen innehar ett bevis som erkänns i den medlemsstat där ansökan om medlet för elektronisk identitet görs och som avser den påstådda identiteten,

och

beviset kontrolleras för att fastställa att det är äkta, eller enligt en tillförlitlig källa existerar det och avser en verklig person,

och

åtgärder har vidtagits för att minimera risken att personens identitet inte är den påstådda identiteten, varvid det tas hänsyn till exempelvis risken för att beviset har förlorats, stulits, upphävts, återkallats eller löpt ut,

eller

2. en identitetshandling uppvisas under ett registreringsförfarande i den medlemsstat där handlingen utfärdades, och handlingen tycks avse den person som uppvisar den,

och

åtgärder har vidtagits för att minimera risken att personens identitet inte är den påstådda identiteten, varvid det tas hänsyn till exempelvis risken för att handlingen har förlorats, stulits, upphävts, återkallats eller löpt ut,

3. om förfaranden som tidigare använts av ett offentligt eller privat företag i samma medlemsstat för andra ändamål än utfärdandet av medel för elektronisk identifiering ger en tillit som är likvärdig de förfaranden som anges i avsnitt 2.1.2 för tillitsnivån väsentlig, behöver den enhet som ansvarar för registreringen inte upprepa de tidigare förfarandena, förutsatt att en sådan likvärdig tillit bekräftas av ett sådant organ för bedömning av överensstämmelse som anges i artikel 2.13 i Europaparlamentets och rådets förordning (EG) nr 765/2008 ⁽¹⁾ eller av ett likvärdigt organ,

eller

4. om medel för elektronisk identifiering utfärdas på grundval av ett giltigt anmält medel för elektronisk identifiering med tillitsnivån väsentlig eller hög, och riskerna för ändring i personidentifieringsuppgifterna beaktas, krävs det inte att förfarandena för styrkande och kontroll av identitet upprepas. Om medlet för elektronisk identifiering som utgör utgångspunkt inte har anmälts, ska tillitsnivån väsentlig eller hög bekräftas av det organ för bedömning av överensstämmelse som avses i artikel 2.13 i förordning (EG) nr 765/2008 eller av ett likvärdigt organ.

4.5 Endast i LOA: upphävande, återkallelse och återaktivering

2.2.3 i LOA Upphävande, återkallelse och återaktivering

Låg, väsentlig, hög:

2. Åtgärder ska föreligga för att förhindra att upphävande, återkallelse och/eller reaktivering sker på otillåtet sätt.

3. Återaktivering ska ske endast om samma krav angående tilliten som fastställts före upphävandet eller återkallelsen fortsätter att uppfyllas.

4.6 Tolkning

4.6.1 Konsekvensbedömning:

I situationer som avses i tolkningsbegäran är godtagande av körkortet dock en betydligt svagare lösning med tanke på tillförlitligheten för ett identifieringssystem. Å andra sidan är det även fråga om att nå en tillräckligt hög tillitsnivå utifrån en riskbaserad bedömning och att ta en kommersiell risk: ett fel som beror på att körkortet har godtagits kan leda till ett skadeståndsansvar för leverantören av identifieringsverktyg.

I samarbetsgruppen för förtroendenätet har flera leverantörer av identifieringstjänster lyft fram konsekvenserna för de praktiska processerna för ärendehantering, särskilt om underhållstillfällena alltid kräver en personlig identifiering (på plats). Å andra sidan lyfte en aktör fram att även 2.2.3 i LOA måste uppfyllas för att ett identifieringsverktyg kan anmälas.

4.6.2 Tolkning

Traficom anser att förarbetena för autentiseringslagen inte direkt stöder en tolkning om att identitetskort eller pass ska krävas i alla situationer när identifieringsverktyget har utfärdats före den 1 januari 2019. Enligt regeringens proposition ska ett verktyg för stark autentisering inte längre kunna *beviljas* enbart på basis av körkort från ingången av 2019, och en inledande identifiering som gjorts med stöd av körkort senast den 31 december 2018 uppfyller kraven i den föreslagna lagen och den inledande identifieringen behöver inte ytterligare säkerställas på något annat sätt.

4.7 Vilka krav är tillämpliga? Hur bör läget struktureras?

Rekommendationen för tillämpning av LOA innehåller inga närmare tillämpningsanvisningar vad gäller förnyelse/ersättning och återaktivering.

⇒ Med förnyelse/ersättning avses antagligen även en sådan situation som avses i tolkningsbegäran, dvs. där autentiseringsfaktorer helt eller delvis behöver ersättas med nya.

Kravet på återaktivering i förordningen om tillitsnivåer ska inte tillämpas direkt med stöd av autentiseringslagen, eftersom lagen inte hänvisar till kravet.

⇒ Ur ett terminologiskt perspektiv kan det vara fråga om återaktivering om låsta bankkoder öppnas på nytt eller om pinkoden för ett mobilcertifikat återställs.

En noggrann klassificering av olika situationer har dock inte nödvändigtvis avgörande betydelse för att specificera tillämpliga krav.

⇒ Som det konstateras ovan i anslutning till avsnitt 2.2.4 i förordningen om tillitsnivåer, kan det som ett allmänt krav i förordningen anses vara att alla tidigare krav angående tilliten fortfarande ska uppfyllas trots förnyelse/ersättning.

I 8 § i autentiseringslagen finns allmänna krav på hela identifieringssystemet, bland annat följande:

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.

Leverantören av identifieringsmetoder ska vidta rimliga åtgärder för att kontrollera att det endast används under ägarens kontroll eller innehav.

Dessutom förutsätter 2.2.3 i LOA särskilt åtgärder för att förhindra återaktivering på otillåtet sätt.

- ⇒ Kravet i 8 § i autentiseringslagen och 2.2.1 i LOA på att kontrollera att identifieringsverktyget endast används av ägaren till verktyget har även vad gäller överlåtelse samband med ett separat krav i 21 § på att leverantören av identifieringstjänster ska säkerställa att verktyget inte obehörigt kommer i någon annans besittning vid överlåtelsen.
- ⇒ Kravet ska även uppfyllas i situationer där en del eller alla autentiseringsfaktorer eller aktiveringskoder överläts vid förnyelsen/ersättningen eller återaktiveringen.

Ett allmänt krav är dessutom att en identifieringsmetod ska grunda sig på autentisering enligt 17 § (8 § 1 mom. 1 punkten).

⇒ Denna grund får inte heller äventyras på grund av förnyelse/ersättning eller återaktivering.

Det är med andra ord viktigt att alla tidigare erforderliga, uppfyllda krav angående tilliten uppfylls trots förnyelse, ersättning eller återaktivering.

4.8 Handlingar som ska användas vid identifieringen

De tillämpliga kraven har utretts ovan, och nu kan den egentliga tolkningsfrågan behandlas, dvs. vad kraven innebär med tanke på de handlingar som används vid identifieringen av en person.

Kan körkortet fortfarande vara en godtagbar handling för kontroll vid förnyelse/ersättning eller återaktivering, eftersom övergångstiden för handlingar som enligt 17 § är giltiga gick ut den 31 december 2018 och en persons identitet vid *inledande identifiering* inte längre kan kontrolleras med hjälp av körkortet?

⇒ Om en identifieringsmetod/ett identifieringsverktyg (alla faktorer som behövs för att använda identifieringsverktyget) överläts genom att personens identitet kontrolleras utifrån identitetsbeviset, kan körkortet inte anses vara en godtagbar handling ens i fråga om de identifieringsverktyg som ursprungligen har kunnat beviljas utifrån körkortet.

⇒ Till denna del bör det på så sätt anses att ett sådant identitetsbevis som avses i kravet i 2.1.2 i LOA bestäms med stöd av 17 § och övergångsbestämmelsen gällande paragrafen så att körkortet inte längre är en godtagbar handling för att kontrollera en persons identitet.

⇒ Det innebär att en persons rätt att få ett identifieringsverktyg inte kan kontrolleras enbart utifrån körkortet. Alla autentiseringsfaktorer kan inte överlåtas enbart utifrån körkortet.

⇒ Kravet på att ett identifieringsverktyg vid förnyelse/ersättning eller återaktivering endast kommer i ägarens besittning kan dock totalt sett uppfyllas med olika kombinationer av kontroller för att styrka personens identitet, leverera verktyget och aktivera verktyget. Att visa upp körkortet kan också ingå i dessa kontroller.

⇒ Som en del av helhetsbedömningen kan övriga kontroller som bör beaktas vara till exempel att leverera en förkommen autentiseringsfaktor till en tidigare autentiserad postadress till ägaren av identifieringsverktyget.