Sammandrag av utlåtandena som lämnats in på Transport- och kommunikationsverkets begäran om utlåtande om Anvisningen om bedömning av elektroniska identifieringstjänster O211

1 Allmänt

Ämbetsverket tackar alla som lämnade in ett utlåtande. Sammanlagt fyra aktörer lämnade in ett utlåtande inom utsatt tid: Candour Oy, Myndigheten för digitalisering och befolkningsdata, Methics Oy och Nordea Abp.

En del av utlåtandena gällde hela anvisningen, medan en del endast tog ställning till en viss del. Utlåtandena behandlas var för sig och ämbetsverket bedömer varje punkt separat.

2 Utlåtande: Myndigheten för digitalisering och befolkningsdata

2.1 Särskilda frågor

Är de nya hänvisningarna till standarder uttömmande? Finns det någon standard som inte har uppmärksammats eller som enligt din åsikt inte är tillämplig?

Hänvisningarna till standarder är uttömmande och det finns ganska många hänvisningar, vilket leder till att risken för motstridigheter mellan standarder är stor då bedömningsanvisningen innehåller många onödigt detaljerade krav och begränsningar som gäller tillämpningen.

Ämbetsverkets bedömning: Ämbetsverkets O211 är en anvisning. Överensstämmelse med kraven hos en identifieringstjänst kan också verifieras med andra bedömningskriterier och standarder. Standarder och användning av andra bedömningskriterier kan också räknas till godo vid användning av ämbetsverkets anvisning 211. Åtgärd: Ingen åtgärd.

Är bedömningen av sessionsidentifikatoren och namnuppgiften om den förlitande parten tydlig?

Ja

Kriterierna för inledande identifiering på distans: Är de listade kriterierna tillämpliga?

Nej

Om inte, vad skulle du tillägga/ta bort?

Se kommentarerna till punkt 3.10 Observationer om uppvisande av identitetsbevis för inledande identifiering via distansuppkoppling.

Ämbetsverkets bedömning: Behandlas på punkt 3.10.

Är hänvisningarna till standarder i fråga om inledande identifiering på distans uttömmande?

Ja

Borde kraven för tillitsnivån hög också beaktas i kriterierna?

Ja

Övriga referensramar för bedömning: Använder ni andra referensramar för bedömning av mobila identifieringsappar?

Nej

Attribut: Är tilläggen till livscykelhanteringen av attribut lämpliga (kapitel 4)?

Nej

Kommentarer:

Se fritt formulerad respons samt kommentarerna till punkt C, mobilkriterier.

Ämbetsverkets bedömning: Behandlas på punkten mobilkriterier.

2.2 DEL 1 textdel och bilaga A

Kommentarer till punkt 3.10 Observationer om uppvisande av identitetsbevis för inledande identifiering via distansuppkoppling

I anvisningen konstateras att man ska hämta jämförelseuppgifter från befolkningsdatasystemet för att säkerställa att det uppvisade identitetsbeviset är äkta och giltigt, och att personen som visar upp identitetsbeviset är dess ägare. MDB påpekar att det är möjligt att ur befolkningsdatasystemet hämta personuppgifter om ägaren av ett identitetsbevis som polisen i Finland har beviljat men att dessa inte ensamma intygar att identitetsbeviset är äkta. Ett identitetsbevis kan också vara äkta även om dess uppgifter inte motsvarar uppgifterna i befolkningsdatasystemet till exempel i situationer där personens namn har ändrats efter att beviset beviljades. Befolkningsdatasystemet innehåller inte information om identitetsbevisets giltighetstid och det är inte möjligt att på basis av det på ett säkert sätt kontrollera att personen som visar upp identitetsbeviset är dess ägare.

Ämbetsverkets bedömning: Ämbetsverket tackar för observationen. Leverantörer av identifieringstjänster har enligt 7 b § i autentiseringslagen rätt att i elektronisk form få information ur polisens informationssystem om giltighet för pass eller identitetskort som används vid inledande identifiering. Uppgifterna i befolkningsdatasystemet kan användas för att kontrollera personuppgifter. Åtgärd: Punkten som gäller befolkningsdatasystemet korrigeras och förklarande text om styrkande av identitet och kontroll av identitetsbevis läggs till.

2.3 Bilaga B – Allmänna kriterier för bedömning

Kommentarer till punkt 1 Identifieringsmedlets egenskaper och skyddsförmåga

9. Att aktiveringskoden endast kan användas en gång är ett nytt krav, som är svårt att uppfylla med chipförsedda verktyg, se punkt 99.

Ämbetsverkets bedömning: Anvisningen har inte tidigare innehållit ett kriterium för användning av aktiveringskoder. Anvisningen kompletteras i fråga om detta. Punkt 2.2.2 i förordningen om tillitsnivåer förutsätter på tillitsnivån hög att aktiveringsprocessen kontrollerar att medlet för elektronisk identifiering endast

levererades till ägaren som det tillhör. På nivån väsentlig räcker det med att det kan antas att medlet levereras endast till ägaren.

Att aktiveringskoden endast kan användas en gång diskuteras närmare i punkt 2.2.3 i förordningen om tillitsnivåer (Upphävande, återkallelse och återaktivering) som inte hänvisas till i autentiseringslagen. Punkten förutsätter att det ska föreligga åtgärder för att förhindra att upphävande, återkallelse och/eller återaktivering sker på otillåtet sätt. Dessutom ska återaktivering ske endast om samma krav angående tilliten som fastställts före upphävandet eller återkallelsen fortsätter att uppfyllas.

Om samma aktiveringskod alltid är giltig och kan användas under identifieringsverktygets hela livscykel, avlägsnar eller försvagar detta betydligt skyddet för autentiseringsfaktorn som baserar sig på information ur perspektivet för identifieringsverktygets äkta innehavare, det vill säga användaren. Användaren, för vilken identifieringsverktyget har beviljats, kan inte skydda användningen av det beviljade identifieringsverktyget om aktiveringskoder som används på nytt kan användas för att annullera, alltså överskriva den verifikationsfaktor (PIN) som endast användaren känner till.

En separat PUK-kod som endast skapas på begäran, efter användarens aktiva åtgärder och autentisering av den som ansöker om PUK-kod, har ansetts skydda faktorn som baserar sig på information från att en utomstående person återställer den.

Ämbetsverket har bekantat sig med andra chipförsedda identitetskortalternativ och aktiveringsprocessen för dessa samt med processen för att återställa en bortglömd autentiseringsfaktor som baserar sig på information (PIN) för att kunna återaktivera den som identifieringsverktyg. I samband med dessa har det inte lyfts fram några genomförandetekniska svagheter som skulle hindra användningen av en aktiveringskod som endast kan användas en gång för att ta i bruk ett identifieringsverktyg. I de lösningar som ämbetsverket har sett och som är i bruk har man också kunnat lösa skapandet av en så kallad PUK-kod på begäran och förmedlingen av den på ett säkert sätt till identifieringsverktygets innehavare som behöver koden för att återaktivera identifieringsverktyget.

I punkt 6.4 i ämbetsverkets föreskrift M72B konstateras att leverantören av identifieringstjänsten inte får kopiera hemliga uppgifter om identifieringsverktyget. Detta förutsätter alltså också att den som beviljar identifieringsverktyget inte har en kopia av PIN-/PUK-/aktiveringskoderna.

Enligt 8.1 § 4 punkten i autentiseringslagen ska åtminstone de villkor uppfyllas 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. I de ovan nämnda punkterna förutsätts bland annat att medlet använder minst två autentiseringsfaktorer från olika kategorier och är utformat så att det kan antas att det endast används under ägarens kontroll eller innehav, autentiseringsmekanismen genomför säkerhetskontroller, varför det är högst osannolikt att gissningar av kommunikation kan underminera autentiseringsmekanismerna, elektroniska kommunikationskanaler som används för att utbyta känslig information skyddas mot avlyssning samt att känsligt kryptografiskt material, om sådant används för utfärdande av medel för elektronisk identifiering och autentisering, ska skyddas från manipulation.

Kraven förutsätter således att leverantören av identifieringstjänsten följer upp hur branschen utvecklas för att kartlägga angreppspotentialen och planerar trygg användning av identifieringsverktyget endast för den användare för vilken

verktyget har beviljats. Med anledning av det ovan nämnda anser ämbetsverket att kravet på flera autentiseringsfaktorer från olika kategorier har ingått i kraven redan tidigare och att det således inte är fråga om ett nytt krav.

Eftersom autentiseringslagen inte innehåller någon direkt hänvisning till punkt 2.2.3 i förordningen om tillitsnivåer kan det i anvisningen konstateras att det att aktiveringskoden endast kan användas en gång är god praxis. Aktören kan dock föreslå kompenserande åtgärder för att säkerställa skyddet för autentiseringsfaktorer som baserar sig på information.

Åtgärd: En förklarande text läggs till där det framgår att det är fråga om god praxis och att syftet är att trygga skyddet för autentiseringsfaktorer som baserar sig på information.

Kommentarer till punkt 3 Tekniska krav på informationssäkerhet

22. (uppdaterat: 25.) Inspektionen ska omfatta en genomgång av arkitekturen och datakommunikationssystemet på en tillräcklig nivå, och det borde inte vara nödvändigt att bifoga beskrivningar till inspektionsberättelsen. En rapport av ett ackrediterat utomstående bedömningsorgan ska vara ett tillräckligt bevis på att tjänsten uppfyller kraven i stället för att fungera som en grund och material för en annan bedömning som görs av Traficom.

Ämbetsverkets bedömning: Det är inte syftet att ämbetsverket gör överlappande bedömningar. Genom att bifoga en arkitekturbeskrivning till bedömningsberättelsen kan det säkerställas att leverantören av identifieringstjänsten använder aktuella arkitekturbeskrivningar av sin egen miljö.

Åtgärd: Ingen förändring.

33. (uppdaterat: 35.) Definitionen av produktionsnät borde preciseras så att den uttryckligen gäller tekniska produktionsnät genom vilka till exempel datakommunikationsutrustning, virtuella maskiner och appar hanteras. Definitionen av produktionsnät ska inte tillämpas på till exempel registreringsarbetsstationer som inte används för ovan nämnda hanteringsåtgärder utan endast för nödvändiga appar som designats för beviljande av identifieringsmetoder.

Ämbetsverkets bedömning: Registreringsstället deltar i hanteringen av identifieringsmetodens livscykel. Programvaran som används för beviljande av en identifieringsmetod används på registreringsställets arbetsstation, varvid arbetsstationen i fråga är en väsentlig del av produktionen av identifieringsverktyget och dess livscykel.

Åtgärd: Ingen förändring.

Kommentarer till punkt 9 Styrkande och kontroll av identitet hos sökande av identifieringsverktyg (inledande identifiering)

76. (uppdaterat: 85.) Ett bevis som undertecknats och stämplats elektroniskt borde kunna anses vara en tillförlitlig källa i sig om dess giltighetstid ingår i den undertecknade informationen eller anges i själva underskriften.

Ämbetsverkets bedömning: Enligt 17.1 § i autentiseringslagen kan kontrollen av identiteten 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.

Ämbetsverket bedömer vid behov användning av en godkänd elektronisk underskrift eller en utvecklad elektronisk underskrift kopplad till ett godkänt certifikat, som har beviljats för elektronisk underskrift, som en del av processen för inledande identifiering. När ett nytt identifieringsverktyg överlämnas ska man i detta fall på andra sätt säkerställa att det nya identifieringsverktyget överlämnas till rätt person.

Ämbetsverket påpekar att enligt 7 § i autentiseringslagen ska det dock säkerställas att personuppgifterna är uppdaterade och korrekta enligt uppgifterna i befolkningsdatasystemet.

Åtgärd: Preciserande text läggs till i kriterium 85.

Kommentarer till punkt 10 Identifieringsverktygs, eller identifieringsmetoders, livscykel

99. (uppdaterat: 103.) Förfarandet med en aktiveringskod som endast kan användas en gång är svårt att genomföra i chipförsedda produkter och lämpar sig inte för befintliga produkter. Förändringen förutsätter betydande förändringar i chipförsedda produkter och för genomförandet av dem behövs en tillräckligt lång övergångsperiod. Skärpningen är betydande och den har inte motiverats till exempel med upptäckta och verifierade svagheter i den nuvarande modellen. MDB anser att det nuvarande förfarandet med aktiveringskoder är tillräckligt och ändamålsenligt.

Ämbetsverkets bedömning: Anvisningen har inte tidigare innehållit ett kriterium för aktiveringskoder. Att aktiveringskoden endast kan användas en gång är god praxis.

Se ämbetsverkets bedömning av kriterium 9 ovan.

Åtgärd: En förklarande text läggs till där det framgår att det är fråga om god praxis och att syftet är att trygga skyddet för autentiseringsfaktorer som baserar sig på information.

102. (uppdaterat: 106.) ”Om förnyelse eller ersättning grundas på ett giltigt medel för elektronisk identifiering, kontrolleras identitetsuppgifterna mot en tillförlitlig källa.” De uppgifter som identifieringsmetoden förmedlar borde kunna anses vara tillförlitliga källor, eftersom de övriga förfarandena i regel borde garantera att uppgifterna inte förändras efter att identifieringsmetoden har beviljats. Det finns inte alltid tillgängliga tillförlitliga källor till exempel i gränsöverskridande fall och alla av dem har inte förfaranden för integration, vilket leder till att medborgare i olika medlemsstater har olika ställning när det gäller ansökan om ett nytt verktyg.

Ämbetsverkets bedömning: Enligt 7 § i autentiseringslagen ska leverantörer av identifieringsverktyg hämta och uppdatera de uppgifter som de behöver för tillhandahållandet av identifieringstjänster för fysiska personer med användning av befolkningsdatasystemet.

Ämbetsverket bedömer inte vilka källor som kunde anses vara tillförlitliga utöver/vid sidan av befolkningsdatasystemet. De uppgifter som identifieringsmetoden förmedlar kan i regel vara en tillförlitlig källa men de garanterar inte att uppgifterna inte har förändrats i en situation där till exempel personens namn eller personbeteckning har förändrats. Därför ska leverantören säkerställa att uppgifterna inte har förändrats.

Enligt 17.6 § i autentiseringslagen har en leverantör av identifieringsverktyg som litar på en tidigare inledande identifiering rätt att få ersättning för sin skada av den leverantör av identifieringsverktyg som begått felet vid den inledande identifieringen om leverantören blir ansvarig för en skada vid den inledande identifieringen. Detta gäller dock endast situationer där den inledande identifieringen kedjas genom ett chainlevel-attribut enligt ämbetsverkets OIDC-gränssnittsrekommendation S213/2023 (Traficom/21543/09.02.00/2022) eller SAML-gränssnittsrekommendation S212/2023 (Traficom/26442/09.02.00/2022). Med andra ord gäller ersättningsansvaret för den egentliga inledande identifieringen.

Åtgärd: Ingen förändring.

2.4 Bilaga C – Mobilkriterier

Övriga kommentarer till bilaga C

I kriterierna har lagts till en hänvisning till en plånbok vid sidan av appen (app/wallet). MDB påpekar att den pågående kompletteringen av eIDAS-förordningen definierar en ny betrodd tjänst, europeisk identitetsplånbok. Identitetsplånbokens tekniska krav och krav på informationssäkerhet fastställs i det så kallade Toolbox-arbetet som pågår. För att kriterierna inte ska tolkas gälla den europeiska identitetsplånboken föreslår MDB att hänvisningarna till plånböcker raderas och att endast hänvisningen till appen bevaras (app/wallet à application).

Kriterierna omfattar krav som endast gäller plånbokslösningar. Exempelvis tar kraven 457 och 458 ställning till kraven för registrering av förlitande parter men dessa har ännu inte vid tidpunkten för utarbetandet av detta utlåtande fastställts i fråga om den europeiska identitetsplånboken. Andra exempel på krav som gäller plånböcker är kriterierna 453, 454 och 456. Enligt MDB:s åsikt borde kraven som gäller plånböcker fastställas först när de tekniska kraven och kraven gällande informationssäkerhet för identitetsplånböcker har fastställts för att undvika en situation där de nationella kriterierna avviker sig från EU:s krav.

Ämbetsverkets bedömning: Plånbok är en allmän benämning eller marknadsföringsbenämning på till exempel en mobilapp. Om en mobilapp används som verktyg för stark elektronisk autentisering, ska den bedömas. Utöver den europeiska identitetsplånboken enligt nationella bestämmelser/bestämmelserna enligt eIDAS2 kan det på marknaden också finnas flera andra plånbokslösningar. Det ska tilläggas kontrollobjekt för plånbokslösningar/mobilappar som utför stark elektronisk autentisering på samma sätt som plånböcker genom att direkt kommunicera med en ärendehanteringstjänst. I fråga om eIDAS2 är det också möjligt att ha en övergångsperiod under vilken den europeiska identitetsplånboken bedöms i jämförelse med de nationella kriterierna tills det är möjligt att göra alleuropeiska certifieringar enligt eIDAS2.

Åtgärd: Preciserande text där begreppet plånbok förklaras läggs till i början av bilaga C.

2.5 Fritt formulerad respons

MDB lyfter också fram att bedömningsanvisningen borde gälla sådana tjänster och produkter för elektronisk autentisering och digital identitet som omfattas av den befintliga regleringen och som tillhandahålls med stöd av regleringen i fråga. När det gäller digitala identitetsplånböcker finns det inte någon gällande reglering och inte heller sådan reglering som skulle fastställa Traficoms roll med tanke på tillhandahållandet av en identitetsplånbok.

Ämbetsverkets bedömning: Om en identitetsplånbok eller vilken som helst plånbokslösning eller mobilapp fungerar som ett verktyg för stark elektronisk autentisering, ska den bedömas. Se föregående punkt. Åtgärd: se föregående punkt.

Det har föreslagits betydande ändringar i kraven för tillitsnivån hög trots att redan de nuvarande kraven enligt vår uppfattning är på en tillräcklig nivå. Produktionen av identifieringstjänster på nivån hög enligt de striktare kraven är ännu mindre lockande, vilket i sin helhet kan leda till att verktyg på nivån hög i praktiken inte används eller produceras i Finland. Verktyg på nivån hög som beviljats i andra medlemsstater borde dock kunna användas för identifiering i Finland och dessa verktyg omfattas inte av Traficoms bedömning. Produktionen av identifieringsmetoder på nivån hög för Finlands marknad ser inte lockande ut.

Ämbetsverkets bedömning: Ämbetsverkets syfte har varit att uppdatera anvisningen i enlighet med branschens goda praxis. Myndigheten för digitalisering och befolkningsdata preciserar inte vilka skärpta krav som utlåtandet hänvisar till. Åtgärd: Inga åtgärder.

3 Utlåtande: Candour Oy

3.1 Särskilda frågor

Kriterierna för inledande identifiering på distans: Är de listade kriterierna tillämpliga?

Nej

Om inte, vad skulle du tillägga/ta bort?

Observationen av livlighet med dator kan basera sig på slumpmässiga händelser eller begäran som riktas till den kund som gör den inledande identifieringen på distans, men systemet ska ha ett förfarande för att upptäcka deep fake-bedrägeriförsök i realtid.

Observationen av en persons livlighet med dator kan också basera sig på ett passivt tillförlitligt förfarande där till exempel en eller flera biosignaler av den person som ska identifieras observeras i samband med att ansiktsbilden tas.

Ämbetsverkets bedömning: Det finns flera olika metoder för observation av livlighet. Syftet med anvisningen är att lista några metoder för observation av livlighet som exempel. Det är inte möjligt att skapa en allomfattande lista, eftersom teknologierna utvecklas snabbt i området. Åtgärd: Preciserande text om inledande identifiering på distans läggs till och det preciseras att eventuella listade åtgärder är exempel. Läggs till att det valda förfarandet ska motsvara kraven på tillitsnivå (väsentlig/hög) enligt kommissionens genomförandeförordning (EU) 2015/1502 (LoA, förordningen om tillitsnivåer).

3.2 Bilaga B – Allmänna kriterier för bedömning

Kommentarer till punkt 9 Styrkande och kontroll av identitet hos sökande av identifieringsverktyg (inledande identifiering)

Observationen av livlighet med dator kan basera sig på slumpmässiga händelser eller begäran som riktas till den kund som gör den inledande identifieringen på distans, men systemet ska ha ett förfarande för att upptäcka deep fake-bedrägeriförsök i realtid.

Observationen av en persons livlighet med dator kan också basera sig på ett passivt tillförlitligt förfarande där till exempel en eller flera biosignaler av den person som ska identifieras observeras i samband med att ansiktsbilden tas.

Ämbetsverkets bedömning: se föregående punkt. Åtgärd: se föregående punkt.

4 Utlåtande: Methics Oy

4.1 Särskilda frågor

Är de nya hänvisningarna till standarder uttömmande? Finns det någon standard som inte har uppmärksammats eller som enligt din åsikt inte är tillämplig?

Vilken standard har inte uppmärksammats:

1. eIDAS2 (https://www.europarl.europa.eu/news/en/press-room/20230315IPR77508/parliament-ready-to-negotiate-with-council-for-an-eu-wide-digital-wallet)

2. EN 419 241-2 och EN 419 221-5 för undertecknande på distans

3. CEN EN 419211-2 och ETSI TR 102 206 (säkra verktyg för skapande av underskrift som baserar sig på UICC-kort (SSCD))

4. SGP.05 EUICC PP v4.0 och ETSI TR 102 206 (säkra verktyg för skapande av underskrift som baserar sig på eUICC-kort (SSCD))

5. ETSI:s samtliga ESI-standarder: https://www.etsi.org/committee/esi

6. Hänvisningar till TEE- och SE-standarder saknas.

Ämbetsverkets bedömning: eIDAS2, det vill säga förnyelsen av eIDAS-förordningen pågår fortfarande. Undertecknande på distans är ett alternativ för stark elektronisk autentisering och används redan i några EU-medlemsstater. Ämbetsverket har inte fått kännedom om lösningar som baserar sig på undertecknande på distans i Finland. I fråga om SIM/eSIM (UICC/eUICC) används i Finland autentisering med mobilcertifikat som baserar sig på SIM/UICC. Vad gäller stark elektronisk autentisering på nivån väsentlig har det inte ansetts vara nödvändigt att separat lista Trusted Execution Environment (TEE)- eller Secure Element-standarderna. Situationen kan förändras om också de starka elektroniska identifieringsverktyg som används på mobila enheter vill höjas på nivån hög. Dessutom kan identifieringsmetoder genomföras med flera andra olika teknologier: lösenord som kan används en gång (TOTP), principen med en delad nyckel (split key), och så vidare. Det är inte möjligt att skapa och upprätthålla en heltäckande lista. Överensstämmelse med kraven hos en identifieringsmetod kan bevisas med en ändamålsenlig standard och/eller certifiering. Åtgärd: Inga åtgärder.

Är bedömningen av sessionsidentifikatoren och namnuppgiften om den förlitande parten tydlig?

Nej

Kommentarer:

Hänvisningar till standarder samt definitioner saknas.

Ämbetsverkets bedömning: Ämbetsverket har publicerat gränssnittsrekommendationer för Open ID Connect och SAML där förmedlingen av namnuppgiften till den förlitande parten behandlas. I fråga om sessionsidentifikatorer har ämbetsverket inte kännedom om lämpliga standarder. Åtgärd: Inga åtgärder.

Kriterierna för inledande identifiering på distans: Är de listade kriterierna tillämpliga?

Nej

Om inte, vad skulle du tillägga/ta bort?

Nej. Eftersom:

1. Hänvisningar till standarder samt definitioner saknas.

2. IPP-standarder (Identity Proofing) som fastställts av ETSI: ETSI EN 319 401-standarden saknas.

3. Tillitsnivån hög har inte beaktats vid inledande identifiering på distans.

Ämbetsverkets bedömning: I bilaga B finns en förteckning över standardreferenser som gäller inledande identifiering på distans. Överensstämmelse med kraven hos en identifieringstjänst kan också verifieras med andra bedömningskriterier och standarder. Standarder och användning av andra bedömningskriterier kan också räknas till godo vid användning av ämbetsverkets anvisning 211. Kraven för nivån hög har ännu inte övervägts. Ämbetsverket fortsätter att utveckla anvisningen så att också kraven för tillitsnivån hög antecknas i den. Åtgärd: Inga åtgärder.

Är hänvisningarna till standarder i fråga om inledande identifiering på distans uttömmande?

Nej

Om inte, vad skulle du tillägga/ta bort?

Se ovan.

Ämbetsverkets bedömning: se föregående punkt. Åtgärd: se föregående punkt.

Borde kraven för tillitsnivån hög också beaktas i kriterierna?

Ja

Kommentarer:

Absolut. Enligt ARF ska EUDIW (EU:s digitala identitetsplånbok) använda tillitsnivån hög (den ska innehålla personens identifieringsuppgift (PID)).

Ämbetsverkets bedömning: EUDIW-kraven och eIDAS2-regleringen är ännu inte färdiga. Åtgärd: Ämbetsverket inleder arbetet i fråga om kraven för tillitsnivån hög i slutet av 2023.

Övriga referensramar för bedömning: Använder ni andra referensramar för bedömning av mobila identifieringsappar?

Ja

Om ja, vilka?

Ja, se svaren ovan.

4.2 DEL 1 – textdel och bilaga A

Kommentarer till punkt 2.5.1 Inspektionsberättelse: Tidpunkt för bedömning och bedömningens längd enligt personarbetstiden

Bedömningskriterierna är inte precisa. Till följd av detta kommer kostnadseffekterna att vara stora.

Ämbetsverkets bedömning: Enligt denna punkt i anvisningen ska bedömningen vara uttömmande. En indikator som kan observeras för att bedöma bedömningens omfattning är dess längd. Åtgärd: Inga åtgärder.

Kommentarer till punkt 3.10 Observationer om uppvisande av identitetsbevis för inledande identifiering via distansuppkoppling

Fråga: Ska tillhandahållaren av en betrodd tjänst (TSP) bevisa att alla skeden för att styrka identiteten har genomförts?

Ämbetsverkets bedömning: Syftet med anvisningen är att lyfta fram faktorer som bör beaktas vid inledande identifiering på distans. Det finns många slags tekniker som används, varför alla observationer inte kan tillämpas på alla av dem. Åtgärd: Ämbetsverket fortsätter att utveckla avsnittet om inledande identifiering på distans i slutet av 2023.

Övriga kommentarer till anvisningens text

Anvisningarna är lite oklara.

4.3 Bilaga B – Allmänna kriterier för bedömning

Kommentarer till punkt 1 Identifieringsmedlets egenskaper och skyddsförmåga

1. Om den huvudsakliga standarden är ISO 29115, var finns hänvisningarna till den?

2. Hänvisningen borde inte hänvisa till hela standarddokumentet utan till det aktuella kapitlet/avsnittet.

3. Varför har dessa standarder valts? Vilka andra standarder har övervägts?

4. Hur kan detta kriterium jämföras med kriterierna i andra medlemsstater?

5. Baserar sig kriterierna på tillitsnivån väsentlig i stället för nivån hög i fråga om gränsöverskridande autentisering?

Ämbetsverkets bedömning: Överensstämmelse med kraven hos en identifieringstjänst kan också verifieras med andra bedömningskriterier och standarder. Standarder och användning av andra bedömningskriterier kan också räknas till godo vid användning av ämbetsverkets anvisning 211. Målet med bedömningen är att säkerställa överensstämmelse med kraven enligt lagen om stark autentisering och betrodda elektroniska tjänster och ämbetsverkets föreskrift M72B. Anvisningen är en syn på hur kraven på nationell nivå kan bedömas. Den tar inte ställning till gränsöverskridande autentisering (eIDAS, notified schemes). Åtgärd: Inga åtgärder.

Kommentarer till punkt 2 Interoperabilitet

Interoperabilitet är inte möjlig om det inte finns adekvata hänvisningar till standarder.

Ämbetsverkets bedömning: Det finns flera olika teknologialternativ för att genomföra stark elektronisk autentisering. Ämbetsverket har publicerat beskrivningar av gränssnitten Open ID Connect och SAML. Syftet med beskrivningarna är att harmonisera tekniska gränssnitt och främja interoperabiliteten. Åtgärd: Inga åtgärder.

Interoperabiliteten mellan tillitsnivåerna väsentlig och hög har inte alls beaktats.

Ämbetsverkets bedömning: I detta skede är beskrivningarna av gränssnitten samma för nivåerna väsentlig och hög. Åtgärd: Ämbetsverket inleder arbetet för att skapa en gränssnittsrekommendation för nivån hög.

4.4 Bilaga C – Mobilkriterier

Kommentarer till punkt 1 Arkitektur, planer och modeller för hotbiler

Goda hänvisningar.

Kommentarer till punkt 2 Lagring av uppgifter och dataskydd

Goda hänvisningar.

Kommentarer till punkt 3 Krypteringskrav

Goda hänvisningar.

Kommentarer till punkt 8 Säkerhetskontroller och skydd (EN: resilience)

PKI-valideringskrav har inte definierats.

Ämbetsverkets bedömning: I krav 492 beskrivs ett ersättande förfarande för hur certifikatet hos appens/plånbokens motpart kontrolleras och godkänns. Det är ett strängt arrangemang där certifikaten ska permanent fästas på appen/plånboken. Åtgärd: Inga åtgärder. Ett ersättande förfarande för godkännande av certifikat beskrivs i samband med krav 492.

4.5 Fritt formulerad respons

Enligt eIDAS-bestämmelserna är Traficom tillsynsmyndigheten i Finland. Traficom har dock varit mycket passivt vad gäller denna roll.

Till exempel finns det inte några kriterier för tillägg av produkter som producerats i Finland på EU Trust-listan över betrodda tjänster.

Således,

1. Har denna definition utarbetats av eIDAS:s tillsynsmyndighet eller finska statens ämbetsverk? – Vilka ärenden är nationella och vilka omfattas av eIDAS?

Ämbetsverkets bedömning: Traficoms Cybersäkerhetscenter är en del av ett statligt ämbetsverk (Traficom). Cybersäkerhetscentret är också den myndighet som övervakar stark elektronisk autentisering och betrodda tjänster.

2. Vad är det nationella ackrediteringsorganets (NAB) roll i Finland i fråga om identifieringstjänster? (Om det inte finns något nationellt ackrediteringsorgan, är SB det nationella ackrediteringsorganet och certifierar plånboksappar? Om eIDAS-bestämmelser iakttas behöver finländska företag tjänster av ett organ för bedömning av överensstämmelse (CAB). Meddelar Traficom vilka organ för bedömning av överensstämmelse som har godkänts?)

Ämbetsverkets bedömning: I Finland är det nationella ackrediteringsorganet (NAB, national accreditation body) FINAS. FINAS ackrediterar organ för bedömning av överensstämmelse i Finland. Tills vidare finns det inga ackrediterade bedömningsorgan för eIDAS (CAB, conformity assessment body, eIDAS betrodda tjänster) i Finland. I 28 § i autentiseringslagen finns en förteckning över de organ för bedömning av överensstämmelse som kan bedöma överensstämmelsen hos en elektronisk identifieringstjänst. Organ för bedömning av stark elektronisk autentisering behöver ingen ackreditering.

5 Utlåtande: Nordea

5.1 Bilaga C – Mobilkriterier

410. I lösningen ingår en mekanism som säkerställer att appen är äkta och att den inte har behandlats osakligt då den uppvisar verifikations-/attributinformation till den förlitande parten.

Det är svårt att genomföra detta, åtminstone på Android-enheter. Enligt vår kännedom har Android inte någon fullständig mekanism för att hindra osaklig behandling. Kravet borde alltså tillåta ”bästa möjliga” genomförande för att upptäcka sådana fall.

Ämbetsverkets bedömning: Verifiering av appar är en viktig riskhanteringsmetod. För verifieringen kan också användas metoder som inte beror på operativsystemet. Åtgärd: Inga åtgärder.

411. Appen/plånboken stöder inte versioner av mobiloperativsystemen vars support/säkerhetsuppdateringar har upphört hos erbjudarna av operativsystem och fungerar inte på dessa.

Traficom borde upprätthålla denna lista och göra den tillgänglig för alla medlemmar i Finlands förtroendenät och därigenom fastställa ”den äldsta godtagbara versionen av operativsystemet”.

Således skulle alla medlemmar ha samma utgångspunkter.

Ämbetsverkets bedömning: Identifieringsmetoden ska basera sig på en riskbedömning. Om leverantören i sina riskbedömningar kan konstatera att också sådana versioner av enheters operativsystem vars uppdateringar redan har upphört är godtagbara, kan den konstatera det till exempel i samband med detta kriterium. Denna faktor ska dock framgå av bedömningen. Aktuella uppgifter finns på offentliga webbplatser för de aktörer som utvecklar operativsystem. Åtgärd: Förklarande text läggs till i samband med kriteriet. Traficom ser inte ett behov av att upprätthålla en lista över de operativsystem som stöds, eftersom en sådan lista finns tillgänglig och uppdaterad hos de aktörer som utvecklar operativsystem.

450. Appen/plånboken genomför enhetsbindningen utifrån enhetens fingeravtryck som skapats enligt flera unika egenskaper i enheten.

Detta är svårt att genomföra i praktiken. I synnerhet erbjuder Android-plattformen för närvarande inte unika identifikatorer, som kunde garanteras förbli oförändrade och som vi kunde använda som information vid enhetsbindning. Om sådana fasta värden inte anges finns det en för stor risk för att till exempel en uppdatering av operativsystemet ändrar de parametrar som använts för kalkylen och förstör appen. Detta är också ett vanligt problem i andra lösningar, eftersom enhetens fingeravtryck inte alltid är detsamma i de olika lösningarna och fingeravtryck också kan förändras ibland. Om detta krav tas med borde det vara frivilligt, men endast det att enhetens identifikator förändras innebär inte automatiskt att appen borde avslutas.

Ämbetsverkets bedömning: Att binda appen till enheten är en riskhanteringsmetod i synnerhet i sådana fall där enheten hamnar i fel händer. Om operativsystemets/enhetens tillverkare försöker hindra användningen av enhetens identifikatorer för skapande av fingeravtryck kan kravet som sådant visa sig vara svårt att genomföra. Åtgärd: Kriteriet förändras och genomförandesättet för fingeravtryck/bindning lämnas öppet.

462. För lagring av hemligheter som används vid identifiering används om möjligt tjänster som tillhandahålls av plattformen i en terminalbaserad säker miljö.

Många befintliga aktörer som tillhandahåller lösningar använder egen kryptering som förvaras i appens container. Således är det inte möjligt att använda en terminalbaserad säker miljö eller dylik.
I vissa Android-telefoner, i synnerhet i äldre, finns det inte heller några öppna terminalbaserade mekanismer. Vi rekommenderar att en terminalbaserad säker miljö inte krävs på tillitsnivån väsentlig utan endast på nivån hög.
Om detta krav ändå tas med kräver det en lämplig övergångsperiod, och Traficom ska hjälpa i kommunikationen med kunder och definiera bland annat ”den äldsta godtagbara versionen av operativsystemet” för iOS och Android.

Ämbetsverkets bedömning: Förändringar i hotmiljön och det ökade antalet skadliga program på mobila plattformar betonar behovet av att bättre skydda kritiska uppgifter i identifieringsappar. Ämbetsverket påpekar att det ska göras en riskbedömning av identifieringsmetoden. Om det på basis av riskbedömningen kan konstateras att skydd på enhetsnivå inte behövs är det helt acceptabelt. Detta ska dock tydligt framgå av riskbedömningen och riskhanteringsmetoderna ska beskrivas.

Åtgärd: Text om riskbedömningen och dess inverkan på kriteriet läggs till i fältet för tilläggsinformation.

469. Om personer som är registrerade i terminalutrustningen inte kan skiljas åt vid genomförande av autentiseringsfaktorn på grund av plattformens egenskaper, gäller det att använda en kombination så att användaren kan specificeras på ett tillförlitligt sätt (t.ex. terminalutrustning = administration, pinkod för hemlighet = information och fingeravtryck = egenskap).

Detta borde omformuleras så att sådana fall beaktas där samma enhet används av flera personer med olika biometriska uppgifter. Om det på enheten har sparats flera olika användares biometriska uppgifter och biometrisk identifiering tas i bruk i identifieringsappen är det omöjligt att veta vilka uppgifter som hör till vilken användare.
Det borde inte alltid vara obligatoriskt att specificera användaren, men risken borde minskas på ett ändamålsenligt sätt.

Ämbetsverkets bedömning: Kriteriet har funnits med redan i versionen från 2019. Om det på grund av plattformens begränsningar inte är möjligt att skilja en faktor som baserar sig på en egenskap bland användarna, borde appen erbjuda en faktor som baserar sig på någon annan faktor med vilken användaren kan specificeras. Den följande punkten i kriterierna tar ställning till en situation där en faktor som baserar sig på en egenskap används.

Åtgärd: Inga åtgärder.

473. Vid genomförande av en biometrisk autentiseringsfaktor används endast gränssnitt som tillhandahålls av plattformen.

Identifiering på distans (pass + ansikte) borde godkännas som en form av biometrisk identifiering i undantagsfall även om plattformen inte erbjuder den.

Ämbetsverkets bedömning: Vid inledande identifiering på distans, eller när ett befintligt verktyg för stark elektronisk identifiering används till exempel över en NFC-förbindelse, används fortfarande enhetens egna gränssnitt.

Åtgärd: Preciserande text läggs till i samband med kriteriet i fråga om användning av pass och identitetskort med enheten.

505. Appen/plånboken skyddar sig själv mot attacker som baserar sig på ett fönster som döljer andra (overlay attack).

Det har bevisats att denna metod ofta ger för många falska positiva resultat för att kunna vara ett nyttigt eller användbart skydd.
Det finns andra metoder som i praktiken kan minska detta problem.

Föreskriften borde alltså INTE innehålla ett noggrant krav, förutom om Traficom vet att genomförandet av det på alla telefoner är möjligt utan att användbarheten minskar.

Ämbetsverkets bedömning: Enligt ämbetsverkets åsikt möjliggör attacker av overlay-typ genomförandet av en skalad attack och är således risker som borde försöka hanteras. Från och med Android 9 API-versionen är det möjligt att genomföra begränsad riskhantering i fråga om detta hot. Åtgärd: Kriteriet bevaras men kravet förklaras i fältet för tilläggsinformation. Kriteriet binds till användningen av metoder som plattformen erbjuder och till påminnelsen om riskanalys.

507. Säkerställs att appen/plånboken förhindrar användningen av tredje parters tangentbord vid inmatning av känslig information.

Några avvikelser borde läggas till för att täcka anordningar som utvecklats för bland annat kunder med nedsatt syn (t.ex. braille-tangentbord).

Ämbetsverkets bedömning: Ämbetsverket har redan funderat på denna aspekt. Vi tackar för det konkreta exemplet. Åtgärd: Ett exempel på en avvikelse läggs till i fältet för tilläggsinformation.