Anvisning om bedömning av elektroniska identifieringstjänster

211/2023 O

Transport- och kommunikationsverkets anvisning

Innehåll

1 Inledning

Denna anvisning gäller bedömningen av överensstämmelsen hos en elektronisk identifieringstjänst och den inspektionsberättelse som ska ges som resultat av bedömningen.

Bifogat till anvisningen finns allmänna modellkriterier för bedömning av överensstämmelsen hos en tjänst för stark autentisering, och särskilda kriterier gällande mobilappar.

Bifogat finns även en minneslista över innehållet i inspektionsberättelsen.

Anvisningen gäller identifieringstjänster som enligt 10 § eller 11 § i autentiseringslagen har anmält sig eller avser att anmäla sig som en tjänst för stark autentisering. Anvisningen gäller både leverantörer av elektroniska identifieringsverktyg och tjänster för identifieringsförmedling.

1.1 Syftet med anvisningen

Anvisningen är avsedd för leverantörer av tjänster för stark autentisering och bedömningsorgan av vilka identifieringstjänster skaffar bedömningar.

Syftet med anvisningen är att beskriva vilka faktorer kvalitetsrevisionerna av tjänsterna ska omfatta för att de ska inbegripa alla krävda delområden. I en bedömning går det att använda kriterierna i denna anvisning eller andra kriterier eller kombinationer av andra kriterier som inbegriper alla delområden som ska utvärderas. Det är med andra ord inte obligatoriskt att följa modellkriterierna, utan dessa är ett sätt att säkerställa att bedömningen är tillräckligt omfattande.

Som resultat av en kvalitetsrevision ska leverantören lämna en inspektionsberättelse till Transport- och kommunikationsverket. Syftet med anvisningen är att beskriva minimiuppsättningen uppgifter och presentationssättet för inspektionsberättelsen.

Med stöd av 42 § i lagen om stark autentisering och betrodda elektroniska tjänster (617/2009) är Transport- och kommunikationsverkets uppgift att ha tillsyn över efterlevnaden av den lagen och EU:s eIDAS-förordning[1]. Denna anvisning har utfärdats med stöd av denna allmänna fullmakt enligt 42 § i nämnda lag.

En särskild anvisning har utfärdats om de anmälningar som ska lämnas till Transport- och kommunikationsverket (214/2023 O). Bestämmelser om bedömning av överensstämmelse med kraven hos sådana system för elektronisk identifiering som ska anmälas till EU ingår i eIDAS-förordningen och förordningen om tillitsnivåer vid elektronisk identifiering (LoA)[2].

1.2 1.2 Anvisningens ikraftträdande

Anvisning 211/2023 O träder i kraft 13.7.2023

[1]Europaparlamentets och rådets förordning (EU) nr 910/2014 om elektronisk identifiering och betrodda tjänster för elektroniska transaktioner på den inre marknaden och om upphävande av direktiv 1999/93/EG
[2]Kommissionens genomförandebeslut (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

Anvisningen gäller tills vidare och den kompletteras och ändras vid behov. I så fall förblir anvisningens nummer oförändrat, medan datumet ändras och årtalet vid behov. De nya versionerna av anvisningen anges i tabellen nedan.

Gällande anvisning publiceras på Transport- och kommunikationsverkets webbplats på https://www.kyberturvallisuuskeskus.fi/sv/elektronisk-identifiering.

Version	Datum	Beskrivning/ändring	Författare
211/2023 O, Traficom/ 20767/ 09.02.00/2022	13.7.2023	3:e publicerade versionen ▪ kriterier för inledande identifiering på distans har lagts till ▪ kriterier som lämpar sig för plånbokslösningar har lagts till	Transport- och kommunikationsverket, Cybersäkerhetscentret
211/2019 O	9.10.2019	Den andra publicerade sammanslagna versionen ▪ de allmänna kriterierna ändrade genom att stryka en del kriterier och genom att förteckna kriterierna utifrån de lagstadgade kraven ▪ helt nya särskilda kriterier tillagda för att tillämpas på mobilappar för elektronisk identifiering ▪ delen i anvisningen 215/2016 O gällande inspektionsberättelse om bedömning av identifieringstjänster uppdaterad och sammanslagen med anvisningen	Transport- och kommunikationsverket, Cybersäkerhetscentret
211/2016 O modellkriterier för kvalitetsrevision hos leverantörer av identifieringstjänster 215/2016 O Berättelser för bedömning av identifieringstjänster och betrodda tjänster	2.11.2016	De första publicerade versionerna	Kommunikationsverket, Cybersäkerhetscentret

1.3 Hänvisningar till standarder och bestämmelser samt förkortningar

De allmänna kriterierna för bedömning av identifieringstjänster bygger på kraven på stark autentisering.

Kriterierna gällande mobilappar bygger på olika standarder och har kompletterats med kriterier som bygger på de uppställda kraven. De uppställda krav som bedömningskriterierna bygger på specificeras även i kriterierna gällande mobilappar.

Anvisningen om inspektionsberättelser bygger på lagstadgade krav.

Lagstiftning som innehåller bestämmelser om krav på identifieringstjänster:

- Lag om stark autentisering och betrodda elektroniska tjänster (617/2009, nedan *autentiseringslagen*)
- Kommissionens genomförandeförordning (EU) 2015/1502 (nedan *LoA* eller *förordningen om tillitsnivåer*)
  - Hänvisningar i autentiseringslagen till förordningen om tillitsnivåer
  - LoA-guidance, en inofficiell tillämpningsguide för förordningen om tillitsnivåer [3]
- Transport- och kommunikationsverkets föreskrift M72B/2022 (nedan M72)[4]
  - Genom föreskriften preciseras vissa krav som fastställs i autentiseringslagen

Hänvisningar till standarder[5]:

- ISO/IEC 27001:2013/2017 Information security management
  - I anslutning till kraven i de allmänna kriterierna finns en hänvisning till relevanta krav i standarden ISO 27001. Syftet med hänvisningarna är att göra det lättare att integrera bedömningen av överensstämmelsen hos en identifieringstjänst i den allmänna bedömningen av ledningen avseende informationssäkerhet.
- OWASP Mobile AppSec Verification v.1.4.2[6]
- ISO/IEC 29115
- ISO/IEC 15408–1
- ISO/IEC 18045
- ISO/IEC TS 29003:2018
- ISO/IEC 30107
- ETSI TS 102 165-1
- ETSI TS 119 461
- Common Criteria CCDB 2009 03

Förkortningar av tillitsnivåerna i tabellerna

- S = väsentlig (motsvarar eIDAS2, substantial)
- H = hög (motsvarar eIDAS3, high)

1.4 Definitioner av identifieringstjänster

Stark autentisering är en identifieringstjänst som uppfyller kraven i autentiseringslagen och vars tillhandahållande har anmälts till Transport- och kommunikationsverket för registrering i enlighet med autentiseringslagen.

I lagstiftningen och denna anvisning är *identifieringstjänster* en allmän benämning för leverantörer av identifieringsverktyg och tjänster för identifieringsförmedling.

[3] https://www.kyberturvallisuuskeskus.fi/sites/default/files/media/file/LoA_Guidance_Final_suomeksi.pdf
[4] Föreskrift M72B/2022 om elektroniska identifieringstjänster och betrodda elektroniska tjänster https://www.kyberturvallisuuskeskus.fi/sites/default/files/media/file/M72B_2022_M%C3%84%C3%84R%C3%84YS_72B_tunnistus-_ja_luottamuspalvelut_julkaistu.pdf
[5] I beredningen av kriterierna har som bakgrundsmaterial använts även följande: FIDO Security Reference: https://fidoalliance.org/specs/fido-v2.0-id-20180227/fido-security-ref-v2.0-id-20180227.html
[6] https://www.owasp.org/index.php/OWASP_Mobile_Security_Testing_Guide

En *leverantör av identifieringsverktyg* tillhandahåller slutanvändare elektroniska identifieringsverktyg.

En *tjänst för identifieringsförmedling* förmedlar identifieringstransaktioner till leverantörer av elektroniska ärendehanteringstjänster, dvs. parter som förlitar sig på en elektronisk identifiering.

Om leverantörer av tjänster för stark autentisering har gjort en anmälan enligt autentiseringslagen till Transport- och kommunikationsverket och om leverantörerna uppfyller kraven i lagen, utgör de ett *förtroendenät för stark autentisering*.

Denna anvisning har utfärdats utgående från kraven på de olika funktionerna i en identifieringstjänst, inte baserat på aktörernas roller. I avsnitt 2.3 i anvisningen klargörs begreppen identifieringsmetod och identifieringssystem.

Definitioner i lagstiftningen

Autentiseringslagen 2 § Definitioner

1) stark autentisering identifiering av en person, av en juridisk person eller av en fysisk person som företräder en juridisk person och verifiering av identifikatorns autenticitet och riktighet genom tillämpning av en elektronisk metod som motsvarar tillitsnivån väsentlig enligt artikel 8.2 b i EU:s förordning om elektronisk identifiering och betrodda tjänster eller tillitsnivån hög enligt artikel 8.2 c i den förordningen,

3) leverantör av identifieringstjänster en leverantör av tjänster för identifieringsförmedling eller en leverantör av identifieringsverktyg,

4) leverantör av identifieringsverktyg en tjänsteleverantör som tillhandahåller eller ger ut identifieringsverktyg för stark autentisering till allmänheten samt tillhandahåller sitt identifieringsverktyg till leverantörer av tjänster för identifieringsförmedling för förmedling i förtroendenätet,

5) leverantör av tjänster för identifieringsförmedling en tjänsteleverantör som förmedlar identifieringstransaktioner baserade på stark autentisering till en part som förlitar sig på en elektronisk identifiering,

10) förtroendenätet de leverantörer av identifieringstjänster som har gjort en anmälan till Transport- och kommunikationsverket,

1.5 Tjänsteleverantörers allmänna tillförlitlighet ingår inte i kriterierna

En oberoende bedömning behöver inte omfatta tjänsteleverantörens allmänna tillförlitlighet och inte heller uppgifter som lämnas om tjänsten till användare och förlitande parter (principer för identifiering, avtalsvillkor, prislistor). Därför behandlas dessa frågor inte i samband med kriterierna.

Det räcker med att **leverantören av identifieringstjänster lämnar en utredning** om dessa frågor till Transport- och kommunikationsverket för utvärdering En förteckning över frågorna finns i 16 punkten i föreskrift M72B.

Uppgifter som ska lämnas till Transport- och kommunikationsverket tillsammans med anmälningar om inledande, upphörande eller ändring av verksamhet beskrivs närmare i anvisningen **214/2023 O Anmälningar om identifieringstjänster och betrodda tjänster.**

BESTÄMMELSER

M72B punkt 16 Utredning av tillförlitligheten hos leverantören av en identifieringstjänst och de publicerade uppgifterna

Leverantören av en identifieringstjänst ska i sin anmälan enligt 10 § i autentiseringslagen genom en egen skriftlig utredning eller en oberoende och behörig utredning eller bedömning visa att följande krav på tillförlitligheten hos leverantören av identifieringstjänster och uppgifterna om identifieringstjänsten uppfylls:

1) en etablerad juridisk person som ansvarar för identifieringstjänsten samt de ansvarigas handlingsbehörighet och tillförlitlighet

2) offentliggjorda meddelanden och användaruppgifter, såsom identifieringsprinciper, dataskyddsprinciper, användningsbegränsningar, avtalsvillkor och prislistor.

3) tillräckliga ekonomiska resurser för att ordna verksamheten och täcka eventuellt skadeståndsansvar,

4) ansvar för underleverantörer, och

5) en plan för att avsluta eller överföra tjänsten på ett kontrollerat sätt, behandla uppgifterna samt göra anmälningar till myndigheter, förtroendenätet, de förlitande parter och användarna om verksamheten avslutas.

2 Bedömning av en identifieringstjänst samt inspektionsberättelse

2.1 Inlämnande av inspektionsberättelsen som bilaga till anmälan

BESTÄMMELSER

Autentiseringslagen 10 § Skyldighet för leverantörer av identifieringstjänster att anmäla att verksamheten inleds

En leverantör av identifieringstjänster som är etablerad i Finland ska göra en skriftlig anmälan till Transport- och kommunikationsverket innan verksamheten inleds. Anmälan kan också göras av en sådan sammanslutning av leverantörer av identifieringstjänster som administrerar en tjänst som ska betraktas som en enda identifieringstjänst.

Anmälan ska innehålla:

[…]

5) en inspektionsberättelse om oberoende bedömning i enlighet med 29 § utarbetad av ett organ för bedömning av överensstämmelse, något annat utomstående bedömningsorgan eller ett internt kontrollorgan

[…]

Leverantören av identifieringstjänster ska utan dröjsmål skriftligen underrätta Transport- och kommunikationsverket om ändringar i de uppgifter som avses i 2 mom. Anmälan ska också göras när verksamheten avslutas eller funktionerna överförs till en annan tjänsteleverantör.

Autentiseringslagen 11 § Leverantör av identifieringstjänster som är etablerad i en annan medlemsstat i Europeiska ekonomiska samarbetsområdet

Vad som föreskrivs i 10 § hindrar inte att en leverantör av identifieringstjänster som är etablerad i en annan medlemsstat i Europeiska ekonomiska samarbetsområdet gör en anmälan enligt nämnda paragraf.

Autentiseringslagen 31 § Inspektionsberättelse

En leverantör av identifieringstjänster och Befolkningsregistercentralen ska över bedömningen av överensstämmelse låta utarbeta en inspektionsberättelse som lämnas in till Transport- och kommunikationsverket.

Inspektionsberättelsen är i kraft den tid som anges i den standard som användes vid bedömningen, dock högst 2 år.

2.1.1 Anmälan om inledande av verksamhet

När en ny leverantör av identifieringstjänster gör anmälan om inledande av verksamhet till Transport- och kommunikationsverket, ska leverantören bifoga en berättelse om inspektion av identifieringstjänsterna till anmälan.

2.1.2 Anmälan om ändring av verksamhet

När en leverantör av identifieringstjänster anmäler en relevant ändring i identifieringssystemet till Transport- och kommunikationsverket, ska leverantören bifoga en berättelse om inspektion av identifieringstjänsterna till anmälan.

Vid relevanta ändringar i verksamheten ska en bedömning göras och en anmälan om ändringar och en inspektionsberättelse ska lämnas in innan ändringarna införs i produktionen.

Relevanta ändringar är till exempel

- ändringar i identifieringsmetoden, dvs. autentiseringsfaktorerna och autentiseringsmekanismen
- tekniska ändringar i identifieringssystemet, dvs. ändringar i underhålls- och produktionssystemets struktur, relevanta program eller andra relevanta komponenter och element
- byte eller ändringar i underleverantörernas underhåll, utrustning, system eller program
- ändringar i mobilapplikationen och/eller i de operativsystem som påverkar applikationen, om de på basis av den kontinuerliga riskhanteringen hos identifieringstjänsten och riskbedömningen förutsätter bedömning av överensstämmelse med kraven mellan periodiska bedömningar.

2.1.3 Periodisk bedömning

När två år har gått sedan den senaste inspektionsberättelsen utarbetades, ska leverantören bifoga en berättelse om inspektion av identifieringstjänsterna till ändringsanmälan.

Enligt lagen är inspektionsberättelsen i kraft den tid som anges i den standard som användes vid bedömningen, dock högst i 2 år. Inspektionsberättelsens giltighetstid, eller högst två år, räknas från det datum då den föregående inspektionsberättelsen utarbetades. Leverantören av identifieringstjänster ska lämna en ny inspektionsberättelse till ämbetsverket två år efter att den föregående inspektionsberättelsen utarbetades om leverantören vill fortsätta att tillhandahålla tjänster för stark autentisering.

Inspektionsberättelsen kan helt eller delvis bygga på standarder enligt vilka bedömningsintervallet är kortare än två år. Leverantören av identifieringstjänster ska se till att bedömningarna i sådana fall görs med de intervall som anges i den tillämpliga standarden. Leverantören av identifieringstjänster ska till Transport- och kommunikationsverket lämna en fritt formulerad anmälan om att ett visst delområde i inspektionsberättelsen har ombedömts och är gällande. En inspektionsberättelse enligt denna anvisning ska lämnas in senast två år efter att den föregående inspektionsberättelsen utarbetats.

Transport- och kommunikationsverket strävar efter att behandla alla regelbundna inspektionsberättelser som leverantörerna av identifieringstjänster har gjort samtidigt och publicerar ett datum då inspektionsberättelserna ska lämnas in, senast 6 månader innan tidpunkten i fråga.

Minimiuppsättningen uppgifter i anmälningar om inledande eller ändring av verksamhet finns beskriven i Kommunikationsverkets anvisning 214/2023 O.

2.2 Delområden som ska bedömas i identifieringstjänster

De delområden där överensstämmelsen ska bedömas oberoende har fastställts i autentiseringslagen och beskrivits närmare i Kommunikationsverkets föreskrift M72B.

Bedömningsorgan kan använda kriterierna i denna anvisning och även andra kriterier eller metoder såvida bedömningsorganet i inspektionsberättelsen kan visa att de uppställda kraven uppfylls genom den använda metoden.

Bilaga B till anvisningen innehåller allmänna kriterier för bedömning av identifieringstjänster. Kriterierna omfattar alla krav oberoende av hur en identifieringsmetod eller ett identifieringssystem har genomförts.

Bilaga C innehåller kriterier gällande mobilappar. Kriterierna kompletterar de allmänna kriterierna, när en mobilapp är integrerad i identifieringsmetoden och identifieringssystemet.

I punkt 16 i föreskriften preciseras de kravområden som en leverantör av identifieringstjänster kan visa en egen utredning om.

Alla punkter gäller leverantörer av **identifieringsmetoder**, dvs. identifieringsverktyg.

Punkterna 1a–1e och underpunkt 2g i 15 punkten i föreskrift M72B gäller **tjänster för identifieringsförmedling**.

BESTÄMMELSER

Autentiseringslagen 29 § Bedömning av överensstämmelse hos en elektronisk identifieringstjänst

En leverantör av identifieringstjänster ska regelbundet låta ett sådant bedömningsorgan som nämns i 28 § bedöma om identifieringstjänsten uppfyller kraven på interoperabilitet, informationssäkerhet, dataskydd och annan tillförlitlighet enligt denna lag.

[…]

Autentiseringslagen 42 § Allmän styrning samt Transport- och kommunikationsverkets föreskrifter

[…]

Transport- och kommunikationsverket får meddela närmare föreskrifter om

[…]

5) grunderna för bedömningen enligt 29, 30 och 32 § av överensstämmelsen hos en identifieringstjänst, en betrodd tjänst och den nationella noden,

[…]

M72B, 15 Kriterier för kvalitetsrevision

15.1 Funktioner som ska bedömas i identifieringssystemet och identifieringsmedlet

En bedömning enligt 29 § i autentiseringslagen måste omfatta alla de krav som ställs i lagen och i denna föreskrift som gäller

1) funktioner som påverkar tillhandahållandet av identifieringstjänsten (ett identifieringssystem):

a) ledningen avseende informationssäkerhet
b) förvaringen och behandlingen av uppgifter
c) lokalerna och personalen
d) tekniska åtgärder, och
e) interoperabiliteten i förtroendenätet, samt

2) identifieringsmedlet, dvs. identifieringsverktyget:

a) ansökan och registreringen
b) styrkandet och kontrollen av den sökandes identitet
c) identifieringsmedlets egenskaper och utformning
d) utfärdandet, leveransen och aktiveringen
e) upphävande, återkallelse och återaktivering
f) förnyelse och ersättning, och
g) autentiseringsmekanismerna.

15.2 Kriterier för kvalitetsrevision

Bedömningen av överensstämmelsen kan basera sig på Transport- och kommunikationsverkets bedömningsanvisning eller bestämmelser eller anvisningar som utfärdats av EU eller något annat internationellt organ, offentliggjorda och allmänt eller regionalt tillämpade anvisningar om informationssäkerhet eller allmänt använda standarder eller förfaranden för informationssäkerhet. Bedömningen kan basera sig på en kombination av flera av ovan nämnda källor.

2.3 Identifieringsmetod, identifieringssystem och underleverantörer

2.3.1 Definitioner

Med **identifieringsmetod** avses ett identifieringsverktyg som tillhandahålls en användare, och ett tekniskt genomförande av identifieringstransaktioner.

Till en identifieringsmetod hör autentiseringsfaktorer och en autentiseringsmekanism.

Med **identifieringssystem** avses en teknisk och organisatorisk identifieringstjänsthelhet som det fastställs krav på i regleringen av stark autentisering.

Till ett identifieringssystem hör exempelvis identifieringstjänstleverantörens egna eller köpta datakommunikationsförbindelser och informationssystem, underhåll, databehandling, ledning avseende informationssäkerhet och de övriga delområden som ingår i de uppställda kraven.

Definitioner i lagstiftningen

Autentiseringslagen 2 § Definitioner

2) identifieringsverktyg ett sådant medel för elektronisk identifiering som avses i artikel 3.2 i EU:s förordning om elektronisk identifiering och betrodda tjänster,

Jfr Autentiseringslagen 8 § Krav på system för elektronisk identifiering

Jfr 8 a § Autentiseringsfaktorer som ska användas i identifieringsmetoden i autentiseringslagen

Artikel 3 i eIDAS-förordningen

2) medel för elektronisk identifiering en materiell och/eller immateriell enhet som innehåller personidentifieringsuppgifter och som används för autentisering för nättjänster,

4) system för elektronisk identifiering ett system för elektronisk identifiering genom vilket medel för elektronisk identifiering utfärdas till en fysisk eller juridisk person eller en fysisk person som företräder en juridisk person,

Jfr artikel 7 Berättigande till anmälan av system för elektronisk identifiering i eIDAS

... c) Systemet för elektronisk identifiering och det medel för elektronisk identifiering som utfärdats inom ramen för det ska uppfylla kraven för åtminstone en av de tillitsnivåer som anges i den genomförandeakt som avses i artikel 8.3.

Jfr artikel 8 Tillitsnivåer för system för elektronisk identifiering i eIDAS

UNDERLEVERANS I LAGSTIFTNINGEN

Autentiseringslagen 13 § Allmänna skyldigheter för leverantörer av identifieringstjänster

[...]

Leverantören av identifieringstjänster svarar för att tjänster och produkter som produceras av personer som leverantören anlitar är tillförlitliga och fungerar.

2.3.2 Bedömning och underleverantörer

Tillhandahållande av en identifieringstjänst är ofta endast en del av företagets eller organisationens verksamhet, och samma system kan användas i både identifieringstjänsten och den övriga verksamheten. Bedömningen av överensstämmelsen ska göras med tanke på identifieringstjänsten. Granskningen av kraven ska riktas på systemet för stark autentisering i organisationens identifieringstjänst, dvs. all verksamhet som påverkar uppfyllandet av kraven på stark autentisering.

Bedömningen ska även omfatta alla underleverantörer (inklusive så kallade molntjänster) till den del de genomför delar av identifieringstjänsten. Hur ingående bedömningen av underleverantörerna är kan sättas i proportion till hur kritisk den funktion som ska skaffas är i identifieringssystemet. Genomförare av inledande identifiering hör också till identifieringssystemet.

Vid användning av molntjänster ska leverantörer av identifieringstjänster försäkra sig om att Transport- och kommunikationsverkets tillsynsrätt uppfylls. Här är det bra att beakta att även internationella molntjänster kan godkänna att Cybersäkerhetscentret vid Transport- och kommunikationsverket får information.

I en **tjänst för identifieringsförmedling** är relevanta krav på **identifieringsmetod** kraven på autentiseringsmekanism till den del förmedlingstjänsten förmedlar identifieringstransaktioner mellan tillhandahållaren av identifieringsverktyg och tjänsten för ärendehantering. Kraven på autentiseringsmekanism är också relevanta för underleverantören till tjänsten för identifieringsförmedling till den del underleverantörens system påverkar säkerheten i identifieringstransaktionerna.

Hänvisningarna till ISO/IEC 27001:2013/2017 om underleverantörer har inte angetts separat i tabellen om bedömningskriterier. I en bedömning enligt ISO-standarden av ledningen av informationssäkerheten behandlas underleverans överlag i punkten A.15.1 Informationssäkerhet i leverantörsrelationer.

Exempel på bedömning av en identifieringsmetod:

- Hur fungerar en kodapp eller en mobiltelefon som en andra autentiseringsfaktor och vilken är i så fall den första autentiseringsfaktorn? I bedömningen gäller det att utreda hur identifieringen i appen sker och finns det flera sätt för användaren att identifiera sig (särskilt med tanke på autentiseringsfaktorerna). Krävs det alltid någon annan faktor eller andra faktorer som bygger på data utöver det engångslösenord som appen meddelar? Är andra autentiseringsfaktorer än en kodapp eller mobilapp bundna till mobil användning?

- Om en leverantör har en mobilapp för identifiering, ska appen bedömas till de delar den påverkar identifieringens överensstämmelse med kraven. I bedömningen gäller det att redogöra för hur leverantören kan säkerställa att appen är

bunden till rätt person i terminalutrustningen och bakgrundssystemet. Om det också finns andra funktioner i appen, behöver funktionerna inte inkluderas i bedömningen till de delar de inte kan påverka tillförlitligheten för identifieringen.

- - Om identifieringen i en tjänst för ärendehantering endast kan ske med en mobilapp, gäller det även att se till att autentiseringsfaktorerna är tillräckligt olika. I bedömningen gäller det med andra ord att utreda hur metoden säkerställer att autentiseringsfaktorer som bygger på data eller egenskaper inte ska hamna i orätta händer, om en annan person har kommit över telefonen antingen fysiskt eller till följd av en säkerhetsincident. På vilket sätt har det förhindrats att en kopia eller en knäckbar hash av pinkoden inte blir lagrad i mobiltelefonen så att identifieringen äventyras enbart till följd av att telefonen blir stulen?

Exempel på faktorer som ska beaktas i bedömningen av identifieringssystem:

- Datacentret
- Applikationsservrar och serverplattformar (en virtuell plattform)
- Hantering av åtkomsten till serverplattformen
- Kontorsnätet (säkerheten i systemet för administration av identifieringstjänsten jämfört med det övriga kontorsnätet)
- Datakommunikationsförbindelse till servern (administrationsförbindelse)
- Informationssäkerhet i den virtuella plattformen (åtkomsthantering, uppdateringar)
- Informationssäkerhet i identifieringsappen (åtkomsthantering, uppdateringar)
- Åtskillnad av administrationsmiljön och produktionsmiljön
- Informationssäkerhet i produktionsmiljön och servicemiljön (informationssäkerhet/kundgränssnitt i apptrafiken)
- Säkerhet avseende anläggningar, personal, användning, datakommunikation och program relaterade till de ovannämnda.

Molntjänster

- Identifieringstjänster kan anlita sådana molntjänster vars överensstämmelse med krav kan säkerställas antingen genom en egen bedömning eller genom en omsorgsfull bedömning av resultat av en annan oberoende och kompetent bedömningsorgan. Därför är det nödvändigt att man noggrant identifierar de tjänster/funktioner/produkter som används via molntjänster och granskar deras certifikat eller övriga bevis.

2.3.3 Inspektionsberättelse: Beskrivning av vilken del av identifieringsmetoden och/eller identifieringssystemet bedömningen omfattar

Revisionen ska riktas till den del av identifieringstjänstleverantörens system där identifieringstjänsten produceras. Leverantören av identifieringstjänster kan beställa bedömningen i delar även hos två eller flera bedömningsorgan så att varje bedömningsorgan bedömer en viss del av identifieringssystemet. Det är viktigt att det av inspektionsberättelsen framgår på ett entydigt sätt om bedömningsorganets inspektionsberättelse omfattar endast en del av identifieringssystemet eller hela systemet. Bedömningsorganet ska på ett tydligt sätt beskriva vilka delar av identifieringssystemet bedömningsorganets bedömning omfattar. Av inspektionsberättelsen ska det dessutom framgå att alla de delar av identifieringstjänstleverantörens system där identifieringstjänsten produceras har inspekterats.

2.3.4 Inspektionsberättelse: Namn (alla) på den identifieringstjänst som är föremål för bedömning

Inspektionsberättelsen ska innehålla uppgifter om produkt- eller tjänstenamn så att användare och tjänster för ärendehantering kan identifiera tjänsten.

Dessutom är det bra att uppge de benämningar som identifieringstjänsten använder internt, om benämningarna förekommer i inspektionsberättelsen eller dokumentationen om identifieringstjänsten.

2.3.5 Inspektionsberättelse: Beskrivning av identifieringsmetoden (identifieringsverktyget)

En beskrivning och/eller dokumentation om identifieringsmetoden och autentiseringsmekanismen ska bifogas inspektionsberättelsen.

Beskrivningen ska vara tekniskt så noggrann att det är möjligt att fastslå att alla faktorer som är relevanta med tanke på kraven har beaktats i bedömningen.

- ✓ Vilka är de autentiseringsfaktorer som har använts för metoden (minst två faktorer från olika kategorier)?
- ✓ På vilket sätt har oberoendet mellan faktorerna säkerställts?
- ✓ På vilket sätt är autentiseringsfaktorerna bundna till innehavaren av identifieringsverktyget?
- ✓ Autentiseringsmekanism, dvs. en teknisk beskrivning av hur identifieringstransaktionerna genomförs

Beskrivningarna ska omfatta underleverantörerna.

2.3.6 Inspektionsberättelse: Beskrivning av identifieringssystemet (systemarkitekturen)

En bild, ett schema eller någon annan tydlig presentation av identifieringssystemets helhetsarkitektur ska bifogas inspektionsberättelsen. Utifrån arkitekturutredningen och inspektionsberättelsen ska det vara möjligt att säkerställa att alla relevanta faktorer som påverkar säkerheten i systemet har beaktats och att systemets arkitektur är säker. Beskrivningarna ska omfatta underleverantörerna. Beskrivningarna ska omfatta underleverantörerna.

- ✓ Systemkomponenterna för identifiering ska framgå av beskrivningen av systemets arkitektur.
- ✓ Utifrån utredningen ska det vara möjligt att uppfatta delarna av identifieringssystemet och leverantörerna av delarna, förbindelserna/bryggorna mellan olika delar, praxisen för skydd av förbindelser, gränssnitten mellan olika delar av systemet och andra faktorer.
- ✓ Alla funktionella relationer mellan de olika komponenterna i hela identifieringssystemet ska framgå av beskrivningen, bland annat åtskillnad av datalager, åtskillnad av presentationsskiktet och affärslogiken, kopplingar mellan bryggor/miljöer och skydd av kopplingarna samt säkerhetskontroller mellan externa aktörer.
- ✓ Beskrivningen bör innehålla information om nättopologi, komponenter på L3-nivå, till exempel brandväggar, servrar och kopplingar till övriga miljöer samt administrationsförbindelser om de har skilts åt.
- ✓ Dataläckagen i identifieringsprocessen ska också beskrivas.
- ✓ Om systemet utnyttjar kommersiella komponenter eller produkter från molntjänster (Amazon Web Services, Google, Microsoft Azure osv.), ska produktkomponenterna uppges vid namn och inkludera dessa externa komponenter i bedömningen gällande underleverantörer.

2.4 Uppgifter om bedömningsorganet

BESTÄMMELSER

Autentiseringslagen 28 § Organ för bedömning av överensstämmelse

Överensstämmelsen hos en tjänst enligt detta kapitel kan bedömas av följande bedömningsorgan så som föreskrivs nedan:

1) ett organ för bedömning av överensstämmelse,

2) ett annat utomstående bedömningsorgan som är verksamt enligt en allmänt använd metod (annat utomstående bedömningsorgan), eller

3) ett oberoende bedömningsorgan inom tjänsteleverantörens organisation som uppfyller en allmänt använd standard (internt kontrollorgan).

Inspektionsberättelsen ska bygga på en bedömning som har gjorts av ett sådant bedömningsorgan som avses i 4 kap. i lagen om stark autentisering och elektroniska signaturer. På tillitsnivån väsentlig kan den som gör bedömningen av identifieringstjänsten vara ett utomstående bedömningsorgan eller ett internt kontrollorgan. På tillitsnivån hög ska bedömningsorganet vara ett utomstående bedömningsorgan.

En bedömning av överensstämmelsen hos ett identifieringssystem kan utgöras av bedömningar som har gjorts av flera bedömningsorgan. Dessa kan utgöra separata inspektionsberättelser eller slås samman till en enda inspektionsberättelse. Uppgifter om samtliga bedömningsorgan ska lämnas.

Inspektionsberättelsen om bedömning av identifieringstjänst ska innehålla åtminstone basuppgifterna nedan.

2.4.1 Inspektionsberättelse: Bedömningsorganets identifierings- och kontaktuppgifter

- ✓ Företagets eller organisationens namn och unika registreringsnummer
- ✓ om företaget eller organisationen har etablerat sig i någon annan stat i EES-området än i Finland, det register där den utländska organisationen eller det utländska företaget har förts in
- ✓ postadress och kontaktpersoner
- ✓ e-postadresser med tanke på förfrågningar från Transport- och kommunikationsverket.

2.4.2 Inspektionsberättelse eller anmälan: Bedömningsorganets kompetens och oberoende

En redogörelse kan lämnas i inspektionsberättelsen eller i övrigt tillsammans med anmälan.

Grunden för bedömningsorganets oberoende och kompetens ska framgå av redogörelsen (enligt en standard som ska iakttas eller någon annan grund enligt punkt 18 eller 19 i M72B).

Autentiseringslagen 42 § Allmän styrning samt Transport- och kommunikationsverkets föreskrifter

[…]

Transport- och kommunikationsverket får meddela närmare föreskrifter om

[…]

6) kompetenskraven enligt 33 § för organ för bedömning av överensstämmelse med beaktande av vad som föreskrivs i EU:s förordning om elektronisk identifiering,

[…]

Bestämmelse M72B, 18 § Krav på utomstående organ för bedömning av identifieringstjänster

18.1 Bevisningsförfaranden

Att de oberoende- och kompetenskrav som ställs på bedömningsorgan i 33 § i autentiseringslagen är uppfyllda kan visas genom

1) ackreditering utifrån standarden ISO/IEC 27001, eller kompetensen för en bedömning enligt standarden ska visas på något annat sätt

2) kompetens som har visats i enlighet med en internationellt känd självregleringsmetod som bygger på WebTrust-reglerna,

3) ackreditering utifrån betalkortsstandarden PCI DSS, eller kompetensen för en bedömning enligt standarden ska visas på något annat sätt

4) kompetens som har visats i enlighet med ISACAs tillsynsram för standarder och informationssystem, eller

5) att visa eller följa en sådan kompetens som förutsätts i andra, med de ovannämnda jämställbara bestämmelser, anvisningar eller standarder för allmän ledning avseende informationssäkerhet eller sektorspecifik reglering eller standardisering.

18.2 Kompetens

Att visa kompetensen för bedömning av identifieringssystem förutsätter att man också visar hur och till vilka delar de bestämmelser, anvisningar eller standarder som avses i punkt 18.1 gäller kraven på identifieringssystem.

Bestämmelse M72B, 19 Krav på interna kontrollorgan för identifieringstjänster

19.1 Oberoende

Att de oberoendekrav som ställs på interna kontrollorgan i 33 § i autentiseringslagen är uppfyllda kan visas genom att iaktta

1) IIA:s professionella standarder (oberoende och objektivitet i intern kontroll, inkl. organisatorisk oberoende),

2)I SACAs tillsynsram för standarder och informationssystem,

3) BIS (Bank for International Settlements) guide som gäller intern kontroll,

4) föreskrifterna och anvisningarna om intern kontroll i Finansinspektionens samling av föreskrifter och anvisningar,

5) anvisningar eller föreskrifter som motsvarar anvisningar och föreskrifter som utfärdats av tillsynsmyndigheterna i övriga medlemsstater inom EES-området, eller

6) andra, med de ovannämnda jämställbara standarderna för myndighetsreglering eller allmän hantering av oberoende intern kontroll.

19.2 Kompetens

Att visa kompetensen för bedömning av identifieringssystem förutsätter att man också visar hur och till vilka delar en intern kontroll som är organiserad enligt de bestämmelser, anvisningar eller standarder som avses i punkt 19.1 riktas mot kraven på identifieringssystemet.

2.5 Genomförande av bedömningen

2.5.1 Inspektionsberättelse: Tidpunkt för bedömning och bedömningens längd enligt personarbetstiden

Tidpunkten för bedömning anges som datum och bedömningens längd som dagsverken eller timmar. Avsikten är att på en allmän nivå redogöra för hur aktuell och ingående bedömningen är.

Ingen minimilängd ställs upp för bedömningen. Bedömningen påverkas av flera faktorer som kan förlänga eller förkorta den tid som används för bedömningen. Om man i bedömningen av tjänsten kan tillgodoräkna flera tidigare eller giltiga bedömningar eller certifikat så förkortas tiden som används för bedömningen. Bedömningen ska täcka hela identifieringssystemet och alla de delområden som räknas upp i den här anvisningen och den ska även innehålla tekniska prover eller bedömningar.

2.5.2 Inspektionsberättelse: Bedömningsmetoder

Inspektionsberättelsen ska innehålla en beskrivning av vilka metoder som har använts vid bedömningen av varje delområde. Inga noggranna krav ställs på antalet källor som ska användas vid bedömning.

Bedömningsorganet och leverantören av identifieringstjänst överväger själva vilka källor som ska användas vid bedömningen och vilka delområden som ska verifieras utifrån flera källor.

En sådan bedömning av samtliga delområden som endast görs utifrån en skriftlig dokumentation kan inte anses vara tillräcklig. **Transport- och kommunikationsverket anser att inspektionsmetoderna är otillräckliga om tekniska observationer inte till någon del har gjorts** utanför systemet eller på något annat sätt vid inspektionen.

Enbart förteckningar över standarder eller hänvisningar kan inte heller anses vara tillräckliga.

Om bedömningen bygger på en bedömning som har gjorts av ett annat bedömningsorgan, gäller det att sätta sig in i en sådan bedömning och dess resultat. Dessutom ska det av inspektionsberättelsen framgå vilka konkreta faktorer som har använts som grund för att bedöma överensstämmelsen hos tjänsten, dvs. hur bedömningsorganet har satt sig in i materialet om sådana övriga bedömningar och bedömt bedömningarnas kvalitet och omfattning och de korrigeringar som har gjorts utifrån bedömningarna samt tidsplanen för korrigeringarna.

2.5.3 Uppgifter om den dokumentation som har använts vid bedömningen av överensstämmelsen

Inspektionsberättelsen ska innehålla en förteckning över tjänsteleverantörens dokument som har utvärderats.

Allt material som gäller bedömningen behöver inte bifogas den inspektionsberättelse som lämnas till Transport- och kommunikationsverket. Vid behov kan Transport- och kommunikationsverket be leverantören lämna en mer detaljerad dokumentation. Rätten till information bygger på 43 § i lagen om stark autentisering och betrodda elektroniska tjänster. Enligt paragrafen har Transport- och kommunikationsverket trots sekretessbestämmelserna rätt att få den information som behövs för skötseln av uppgifterna av dem vars rättigheter och skyldigheter den aktuella lagen gäller och av dem som handlar för dessas räkning.

Den dokumentation som utarbetas vid en bedömning ska förvaras minst under inspektionsberättelsens giltighetstid. Dessutom ska hänsyn tas till att tillämpliga metoder också kan ställa vissa krav på förvaringen av dokumentationen och på förvaringstiden.

2.5.4 Riskbedömning av identifieringsmetoden

Enligt punkt 6.1.1 i föreskrift M72B ska skyddsförmågan basera sig på en riskbedömning, där man separat bedömer hot mot autentiseringsfaktorer och -mekanismer som baserar sig på innehav, information och egenskaper samt säkerhetsåtgärder som skyddar mot hoten.

Vid riskbedömningen kan man även utnyttja beräkningen av attackpotentialen t.ex. enligt Common Criteria CCDB 2009 03 avsnittet 3 eller ETSI 102 165-1 avsnittet 6.6 och 6.7.

2.6 Proportionalitet mellan bedömning och tillitsnivå respektive risker

Det finns två tillitsnivåer för graden av tillit till stark autentisering, nämligen väsentlig och hög.[7] I tabellerna om bedömningskriterier används förkortningarna S = väsentlig (motsvarar eIDAS2, substantial) och H = hög (motsvarar eIDAS3, high).

På flera ställen i lagstiftningen har vissa krav specificerats för olika tillitsnivåer, men inte alla krav.

Ett allmänt krav som skiljer på olika tillitsnivåer är hur väl en identifieringsmetod och ett identifieringssystem skyddar identifieringen mot olika informationssäkerhetsrisker och hot. Hänsyn ska tas till riskerna och hoten under hela livscykeln för tillhandahållandet av identifieringstjänster och identifieringsmetoden. På tillitsnivån hög gäller det att till alla delar ha kapacitet att skydda mot angripare med en relativt avancerad angreppspotential. Kapaciteten ska vara utmärkt även på tillitsnivån väsentlig.

I kriterierna behandlas tillitsnivåerna främst i kombination. Om det saknas ett krav eller kriterium för tillitsnivån hög, är den allmänna anvisningen då att identifieringstjänstens skyddskapacitet och åtgärder ska bedömas i proportion till en hög angreppspotential.

I framtiden kan kriterierna uppdateras och tillitsnivån hög kan också beaktas noggrannare, när vi har fått erfarenhet av tillämpningen i Finland och en gemensam europeisk praxis om tolkning av eIDAS-kraven.

Grunden för säkerheten utgörs av identifiering och en systematisk hantering av risker och hot samt av skydd mot risker och hot genom tekniska och organisatoriska åtgärder.

JFR

LoA 2.3 Autentisering

Detta avsnitt handlar om hot vid användning av autentiseringsmekanismen och förtecknar de krav som gäller för varje tillitsnivå. I detta avsnitt ska kontroller antas stå i proportion till riskerna på en viss nivå.

LoA guidance, avsnitt 2.3

[7] EU:s förordning om tillitsnivåer ställer även krav på tillitsnivån låg, men denna nivå beaktas inte i den finska autentiseringslagen. Kraven i eIDAS på ömsesidigt erkännande gäller inte heller identifieringsmetoder på tillitsnivån låg, utan det är frivilligt att beakta dem.

De autentiseringsmekanismer som används i autentiseringsskedet kan inte helt förhindra alla angrepp, utan de kan endast stå emot angrepp på vissa säkerhets- eller tillitsnivåer. Det vanliga sättet att mäta vilken tålighet olika mekanismer ger är att ordna mekanismerna enligt hur väl de klarar angrepp av olika angreppspotential (dvs. angriparens kraft).

De termer som används för de olika angreppspotentialerna på tillitsnivån är ”förhöjd/grundläggande” (enhanced-basic), ”måttlig” (moderate) och ”hög” (high). Dessa termet är lånade från ISO/IEC 15408 ”Information technology – Security techniques – Evaluation criteria for IT security” och ISO/IEC 18045 ”Information technology – Security techniques – Methodology for IT security evaluation”. Standardernas text kan läsas fritt på adressen www.commoncriteriaportal.org/cc (CCPART1-3 motsvarar standarden ISO/IEC 15408 och CEM standarden ISO/IEC 18045).

I standarden ISO/IEC 15408-1 definieras angreppspotential som den arbetsmängd som ett angrepp [mot en mekanism] kräver, uttryckt som angriparens sakkunskap, resurser och motivation.

I standarden ISO/IEC 18045 / bilaga B.4 till CEM ges anvisningar för hur man beräknar den angreppspotential som krävs för att utnyttja en viss svaghet i en autentiseringsmekanism.

Uppfyllandet av kraven i genomförandeförordningen förutsätter en bedömning av tåligheten mot eventuella angrepp.

I bedömningen ska man beakta relevanta hot. I standarden ISO 29115 nämns exempelvis följande: gissande via nätet och utanför nätet, omspelning av identifierande uppgifter, fiske efter information, avlyssning, replay-attack, sessionskapning, man-i-mitten-attack, stöld av identifierande uppgifter, spoofing-attack och att utge sig för att vara någon annan.

I bedömningen av tåligheten mot angrepp bör man beakta hela autentiseringsmekanismen, även de risker som hänför sig till verifieringen av innehavet av metoden för elektronisk identifiering.

[…]

Vid en riskbedömning ska hänsyn tas till rimliga antaganden om säkerhetsnivån för komponenter som ett autentiseringssystem använder, men som inte ingår i systemet (till exempel användarens miljö, webbläsare och smarttelefon).

Komponenterna kan användas i olika sammansättningar och med olika skyddsinställningar.

[…]

LoA 2.4 Hantering och organisation

Alla deltagare som tillhandahåller en tjänst för elektronisk identifiering ... (nedan kallad en tillhandahållare av tjänster) ska i dokumenterad form ha praxis, policyer och strategier för ledning av informationssäkerhet vad avser risker samt andra erkända kontroller som ger styrningsorganen för system för elektronisk identifiering i respektive medlemsstat garantier att effektiva förfaranden föreligger. Alla krav/beståndsdelar i hela avsnitt 2.4 ska antas stå i proportion till riskerna på en viss nivå.

LoA guidance, avsnitt 2.4

[…]

En allmän princip för riskhanteringen är att organisationen själv måste välja vilken risknivå den anser godtagbar. Genom kravet i avsnitt 2.4 ändras denna allmänna princip, eftersom det föreskriver att organisationens säkerhetsåtgärder ska ställas i relation till riskerna på respektive nivå.

[…]

2.7 Inspektionsberättelsens noggrannhet

Av inspektionsberättelsen ska det framgå på vilket sätt uppfyllandet av kraven har bedömts.

Inspektionsberättelsen ska innehålla en verbal beskrivning av vilka praktiska faktorer och observationer som har använts som grund för att bedöma och fastslå överensstämmelsen av varje krav.

Berättelsen ska innehålla en förteckning över vilka av tjänsteleverantörens dokument som har utvärderats i varje punkt och vilka metoder som har använts.

Noggranna uppgifter krävs vid behov särskilt om bedömning av

- ✓ lagring/behandling av uppgifter
- ✓ tekniska åtgärder
- ✓ autentiseringsmekanism
- ✓ ledningssystem för informationssäkerhet
- ✓ bedömning av säkerheten i anläggningar.

På tillitsnivån hög krävs det noggrannare uppgifter än på tillitsnivån väsentlig.

Redogörelsen ska även omfatta alla underleverantörer.

2.8 Rapportering av avvikelser i inspektionsberättelsen

Vid bedömning av överensstämmelse hittas vanligen avvikelser som korrigeras under bedömningen eller kort därefter.

Observationer och korrigering av avvikelser är en viktig del av underhållet och ledningen avseende informationssäkerhet. Därför är det bra att inspektionsberättelsen innehåller en redogörelse för observationer och korrigering av avvikelser. Avvikelserna kan beskrivas per krav eller i en sammanfattning.

Som bilaga till denna anvisning finns en rapporteringstabell i Excel-format som är bra att använda som verktyg för bedömningen och som verktyg för rapporteringen till Transport- och kommunikationsverket. I tabellen finns punkter som behövs för rapportering av observationerna och för att anmäla korrigeringsåtgärderna.

Invid varje observerad avvikelse antecknas observatörens åtgärdsförslag samt den plan som leverantören av identifieringstjänsten har för korrigeringen och korrigerande åtgärder eller för kompenserande åtgärder. För redan korrigerade avvikelser ska man anmäla hur de har korrigerats.

Transport- och kommunikationsverket kommer inte att ta fram någon allvarlighetsskala för avvikelser, utan leverantören av identifieringstjänst och bedömningsorganet får bestämma om en bedömning av hur allvarliga avvikelserna är. Transport- och kommunikationsverket gör en slutlig bedömning av om avvikelserna kan godtas för att de är obetydliga, planen för korrigering av avvikelserna är tillräcklig eller leverantören vidtar kompenserande åtgärder. Vid behov kräver Transport- och kommunikationsverket korrigering av upptäckta avvikelser.

2.9 Korrigering av avvikelser och rapportering om korrigeringarna

Kritiska avvikelser ska korrigeras omedelbart och de korrigerande åtgärderna ska genomföras inom 6 månader från att avvikelsen har observerats. Även för andra observerade avvikelser ska man meddela tidtabellen för korrigeringen samt de korrigerande åtgärderna.

De korrigerande åtgärderna ska bedömas i samband med nästa bedömning, eller senast om 6 månader från att avvikelsen observerades **ifall det är frågan om en kritisk avvikelse.** Den nya bedömningen tillställs till Transport- och kommunikationsverket då den står klar.

3 Delområden som ska bedömas

Detta avsnitt innehåller en förteckning över kraven på de delområden som ska bedömas, och en eventuell anvisning om bedömning och rapportering i inspektionsberättelsen.

Denna indelning används i de allmänna kriterierna för bedömning av identifieringstjänster. Allmänna kriterier för bedömning av identifieringstjänster finns i bilaga B till anvisningen.

3.1 Identifieringsmetodens egenskaper och autentiseringsmekanism

Kraven föreskrivs i följande bestämmelser:

- Autentiseringslagen 8 a § Autentiseringsfaktorer som ska användas i identifieringsmetoden i autentiseringslagen
- Bilagan till LoA: 2.2.1 Medel för elektronisk identifiering: egenskaper och utformning
- Autentiseringslagen 8 § Krav på system för elektronisk identifiering 1 mom. 3 punkt
- Bilagan till LoA: 2.3.1 Autentiseringsmekanism
- Bilagan till LoA: 2.4.6 Tekniska kontroller (controls), punkt 2
- M72B, 6 Krav på informationssäkerhet i identifieringsmetoder
- M72B 7, Krypteringskrav på identifieringssystemets gränssnitt
- M72B 8, Verifiering av parterna i datakommunikationen
- M72B 9, Identifieringsmeddelandenas integritet och sekretess

- LoA Bilaga, 1. Tillämpliga definitioner
- 2) med autentiseringsfaktor avses en faktor som bekräftas vara bunden till en person och som tillhör någon av följande kategorier […]
- 3) med dynamisk autentisering avses 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,

Av inspektionsberättelsen ska det framgå på vilket sätt identifieringsmetodens egenskaper och autentiseringsmekanism har bedömts och hur metoden ger skydd mot hot och risker i informationssäkerheten på det sätt som tillitsnivån kräver.

Leverantören av identifieringsverktyg ansvarar för att identifieringsmetodens egenskaper stämmer överens med de uppställda kraven.

För överensstämmelsen hos en autentiseringsmekanism ansvarar även tjänsten för identifieringsförmedling, eftersom tjänstens system ingår i förmedlingen av identifieringstransaktioner.

Dessutom ska en scanningsrapport om den bedömning som avses i punkt 7 i M72B lämnas in utöver inspektionsberättelsen. Rapporten ska visa TLS- och krypteringsprofilerna för gränssnittet utåt.

3.2 Interoperabilitet

Kraven föreskrivs i följande bestämmelser:

- Autentiseringslagen 12 a § Förtroendenätet för leverantörer av identifieringstjänster
- SRF 169/2016 Statsrådets förordning om förtroendenätet för leverantörer av tjänster för stark autentisering: 1 § Förtroendenätets tekniska gränssnitt
- M72B, 12 Minimiuppsättning uppgifter som ska förmedlas i förtroendenätet
- M72B, 14 Protokoll som används vid dataöverföring samt övriga krav

Inspektionsberättelsen ska innehålla en bedömning av vilka gränssnitt som tillhandahålls i förtroendenätet och vilka attribut (identifieringsuppgifter) som tillhandahålls med autentiseringsmetod. Av berättelsen ska det även framgå på vilket sätt beredskapen att tillhandahålla optionella attribut har bedömts.

Bedömning av attribut gäller endast leverantörer av identifieringsmetoder.

3.3 Tekniska krav på informationssäkerhet

Kraven granskas med tanke på säkerheten i datakommunikation, informationssystem och användning.

Kraven föreskrivs i följande bestämmelser:

- Autentiseringslagen 8 § Krav på system för elektronisk identifiering, 1 mom. 4 punkten
- LoA Bilaga, 2.3.1 Autentiseringsmekanism
- LoA Bilaga, 2.4.6 Tekniska kontroller (controls), punkterna 1–3
- M72B, 5 Krav på informationssäkerhet i identifieringsmetoder

Av inspektionsberättelsen ska det framgå på vilket sätt man har bedömt skyddet av identifieringssystemet och säkerheten i datakommunikation, informationssystem och användning vid utformningen, genomförandet och underhållet av identifieringssystemet genom tekniska åtgärder mot konsekvenser av måttliga eller höga informationssäkerhetshot och säkerhetsöverträdelser på det sätt som tillitsnivån kräver.

Av inspektionsberättelsen ska det framgå på vilken grund man har bedömt om de delar av identifieringssystemet som underleverantörer har genomfört uppfyller kraven.

I bedömningen och inspektionsberättelsen är det bra att i tillämpliga delar beakta
- Datakommunikationsförbindelser
- Administrationsförbindelser
- Indelning av datakommunikationsnätet i zoner
- Datakommunikationsutrustning och datakommunikationssystem
- Åtskillnad av produktions-, underhålls- och hanteringsnät samt utvecklingsmiljö
- Filtrering
- Förbindelser till ett offentligt nät
- Klassificering av informationssystem
- Åtkomstbehörigheter och identifiering av användare
- Farliga arbetskombinationer
- Härdande
- Krypteringslösningar
- Säkerhet i kryptografiskt material
- Särskilda krav på arbetsstationer på distans
- Skadliga program
- Hantering av förändringar
- Programsårbarheter
- Säkerhetskopiering

3.4 Förmåga att observera avvikelser, hantering av avvikelser och störningsanmälningar

Kraven föreskrivs i följande bestämmelser:

- Autentiseringslagen 8 § Krav på system för elektronisk identifiering, 1 mom. 4 punkten
- LoA Bilaga, 2.4.6 Tekniska kontroller (controls), punkterna 1 och 4
- Autentiseringslagen 16 § Skyldighet för leverantörer av identifieringstjänster att anmäla hot och störningar som riktas mot verksamheten eller skyddet av uppgifter
- M72B, 5 Krav på informationssäkerhet i identifieringsmetoder
- M72B, 11 Anmälningar om störningar från leverantören av identifieringstjänsten till Transport- och kommunikationsverket.

Av inspektionsberättelsen ska det framgå på vilken grund följande faktorer utifrån bedömningen uppfyller de uppställda kraven:

- ✓ förmåga att observera avvikelser
- ✓ insamling av loggdata om incidenter och om hantering
- ✓ övervakning för att observera avvikelser
- ✓ allvarlighetsklassificering och systematisk behandling av avvikelser
- ✓ systematik i korrigeringsåtgärder
- ✓ beredskap att fullgöra skyldigheten att anmäla störningar till olika instanser

3.5 Lagring och behandling av uppgifter

Kraven föreskrivs i följande bestämmelser:

- Autentiseringslagen 13 § Allmänna skyldigheter för leverantörer av identifieringstjänster
- LoA Bilaga, 2.4.4 Registerföring, punkterna 1–2
- Autentiseringslagen 8 § Krav på system för elektronisk identifiering, 1 mom. 4 punkten
- LoA Bilaga, 2.4.6 Tekniska kontroller (controls), punkt 1 (observera kravet på skydd av känsligt kryptografiskt material på tillitsnivåerna väsentlig och hög) och punkt 5
- M72B, 5 Krav på informationssäkerhet i identifieringsmetoder
- M72B 7, Krypteringskrav på identifieringssystemets gränssnitt
- Autentiseringslagen 24 § Registrering och användning av uppgifter om identifieringstransaktioner och identifieringsverktyg

Av inspektionsberättelsen ska det framgå på vilken grund följande faktorer utifrån bedömningen överensstämmer med de uppställda kraven:

- ✓ klassificering av information avseende identifieringssystem och identifiering
- ✓ kontroll av tillgången till uppgifter
- ✓ risker med koncentration av uppgifter
- ✓ säkerhet i behandling och lagring av uppgifter (inkl. krypteringar)
- ✓ spårning och återställande av uppgifter
- ✓ hantering av uppgifternas livscykel, inbegripet lagringstid och radering av uppgifter.

3.6 Säkerhet i anläggningar

Kraven föreskrivs i följande bestämmelser:

- Autentiseringslagen 8 § Krav på system för elektronisk identifiering, 1 mom. 4 punkten
- LoA Bilaga, 2.4.5 Anläggningar och personal, punkterna 3–4

Inspektionsberättelsen ska innefatta observationer utifrån vilka man har bedömt att den fysiska säkerheten och övervakningen av anläggningar som påverkar säkerheten i identifieringssystemet överensstämmer med de uppställda kraven.

I bedömningen och inspektionsberättelsen är det bra att i tillämpliga delar beakta:

- ✓ Skydd mot miljöhändelser (brand, värme, gas, damm, vibrationer, vatten)

- ✓ Skydd mot obehörig åtkomst (inbrott)
- ✓ Avbrott i elförsörjning
- ✓ Skydd mot skadegörelser
- ✓ Indelning av anläggningar i zoner
- ✓ Konstruktivt skydd
- ✓ Passerkontroll
- ✓ Kvalitet på säkerhetssystem
- ✓ Olovliga utrustningar och förbindelser

3.7 Tillräckliga och kvalificerade personalresurser

Kraven föreskrivs i följande bestämmelser:

- Autentiseringslagen 13 § Allmänna skyldigheter för leverantörer av identifieringstjänster
- LoA Bilaga, 2.4.5 Anläggningar och personal, punkterna 1–2

Inspektionsberättelsen ska innefatta observationer utifrån vilka man har bedömt:

- ✓ att personalresurserna operativt sett är tillräckliga i proportion till den elektroniska identifieringstjänstens karaktär (24/7/365)
- ✓ kunskapen inom nödvändiga delområden (teknik, juridik bl.a. på grund av behandling av personuppgifter)
- ✓ att köpta tjänster och funktioner (kontorssystem, drifttjänster, programvaror, infrastruktur osv.) är tillräckliga och kvalificerade

3.8 Ledning avseende informationssäkerhet

Kraven föreskrivs i följande bestämmelser:

- Autentiseringslagen 8 § Krav på system för elektronisk identifiering, 1 mom. 5 punkten
- LoA Bilaga, 2.4 Hantering och organisation, ingress
- LoA Bilaga, 2.4.3 Ledning avseende informationssäkerhet
- LoA Bilaga, 2.4.7 Efterlevnad och revision
- M72B, 4 Ledningssystem för informationssäkerhet hos leverantörer av identifieringstjänster

- LoA Bilaga, 1. Tillämpliga definitioner
  4) med ledningssystem för informationssäkerhet avses en uppsättning processer och förfaranden avsedda att hantera godtagbara risknivåer förknippade med informationssäkerhet.

Av inspektionsberättelsen ska det framgå på vilken grund följande faktorer utifrån bedömningen överensstämmer med de uppställda kraven:

- ✓ ledningen avseende informationssäkerhet hos leverantören av identifieringstjänster är omfattande, konsekvent, organiserad, systematisk och kontinuerligt övervakad
- ✓ kraven på identifieringstjänster (autentiseringslagen, eIDAS, LoA och föreskrift 72) har beaktats i ledningssystemet
- ✓ ledningen avseende informationssäkerhet hos underleverantörerna uppfyller de uppställda kraven

3.9 Styrkande och kontroll av identitet hos sökande av identifieringsverktyg (inledande identifiering)

Kraven föreskrivs i följande bestämmelser:

- Autentiseringslagen 8 § Krav på system för elektronisk identifiering, 1 mom. 1 och 2 punkterna

- Autentiseringslagen 17 § Identifiering av en fysisk person som ansöker om ett identifieringsverktyg
- LoA Bilaga, 2.1.2 Styrkande och kontroll av identitet (fysisk person)
- Autentiseringslagen 7 b § Information om giltighet för pass eller identitetskort
- M72B, 6 Krav på informationssäkerhet i identifieringsmetoder

Krav på styrkande och kontroll av identitet hos juridisk person

- Autentiseringslagen 7 a § Användning av uppgifter i företags- och organisationsregister
- Autentiseringslagen 17 a § Identifiering av en juridisk person som ansöker om ett identifieringsverktyg
- LoA Bilaga, 2.1.3 Styrkande och kontroll av identitet (juridisk person)
- LoA, Bilaga 2.1.4 Bindning mellan fysiska och juridiska personers medel för elektronisk identifiering

- LoA Bilaga, 1. Tillämpliga definitioner
  1. tillförlitlig källa: en källa oavsett form som är tillförlitlig när det gäller att tillhandahålla korrekta uppgifter, information och/eller bevis som kan användas för att styrka en identitet.

Av inspektionsberättelsen ska det framgå på vilket sätt och på vilken grund förfarandena för inledande identifiering av personer utifrån bedömningen överensstämmer med de uppställda kraven.

Möjliga förfaranden för inledande identifiering

1) Inledande identifiering utgår från att en person visar ett identitetsbevis som är godkänt i Finland
2) Inledande identifiering med elektroniskt identifieringsverktyg
3) Inledande identifiering utifrån en identifiering som sker för annat ändamål
4) Inledande identifiering som utförs av polisen
5) (Inledande) identifiering via distansuppkoppling till exempel med hjälp av videoförbindelse eller fotografiserie samt distansavläsning av identitetsbeviset

3.10 Observationer om uppvisande av identitetsbevis för inledande identifiering via distansuppkoppling

OBS. När anvisningen bereddes, saknades ännu etablerade tolkningar om de förutsättningar under vilka uppvisande av identitetsbevis via distansuppkoppling kan uppfylla kraven på tillitsnivån väsentlig respektive hög.

Därför innefattar anvisningen synvinklar som bör beaktas vid risk- och hotbedömningen och planeringen av genomförandet. Identifieringsverktyg för stark autentisering kan användas i flera olika e-tjänster. Därför gäller det att på tillitsnivån väsentlig förhålla sig sträng till att endast rätta personer beviljas identifieringsverktyg. På tillitsnivån hög ska hänsyn tas till kapaciteten att skydda mot angripare med hög angreppspotential.

De observationer som har samlats till anvisningen är inte en uttömmande förteckning, utan de är exempel på frågor som har dryftats vid utfärdandet av anvisningen.

Bland annat följande ska beaktas vid inledande identifiering utifrån identitetsbevis (pass eller id-kort):

- Kontrollera att identitetsbeviset är äkta
- Jämföra den person (egenskaperna) som visar ett identitetsbevis med uppgifterna i beviset

  - Jämföra fotot på identitetsbeviset med personens ansikte. Det går även att jämföra signaturer, beviset kan ha en bild på signaturen. Be personen att skriva sitt namn.
- **Användning av befolkningsdatasystemet**
- **Kontroll i tillgängliga databaser av att ett personbevis är äkta eller giltigt**
- Om det går att visa personbevis via distansuppkoppling, gäller det att i bedömningen grundligt beakta riskerna och metoderna för att skydda mot hot om att ett identitetsbevis visas av fel person eller ett förfalskat identitetsbevis. Hänsyn ska även tas till följande
  - kontrollera säkerhetsdetaljerna i identitetsbevis och
  - kontrollera att det foto eller den video som personen har överlämnat om sig själv är äkta.

Synpunkter på inledande identifiering via distansuppkoppling

- Om det går att visa personbevis via distansuppkoppling, gäller det att i bedömningen grundligt beakta riskerna och metoderna för att skydda mot hot om att ett identitetsbevis visas av fel person eller ett förfalskat identitetsbevis.

- Hänsyn ska tas till kontroll av säkerhetsdetaljerna i identitetsbeviset och av att det foto eller den video som personen har skickat om sig själv är äkta.

- Endast identitetsbevis med chip kan användas för identifiering på distans vid beviljande av ett identifieringsverktyg för stark autentisering.

  - Säkerhetsdetaljerna i identitetsbevis är utformade så att de ska kontrolleras på plats och till exempel med hjälp av UV-ljus. Därför är det inte nödvändigtvis möjligt att på ett tillförlitligt sätt kontrollera en identitetshandlings äkthet enbart utifrån en bild på handlingen, eftersom säkerhetsfaktorerna inte kan ses på bilden. På bilden går det närmast att kontrollera att handlingens layout är av rätt typ.

  - Situationen förändras väsentligt vid användning av chip i identitetsbevis. Passiv autentisering (Passive Authentication), dvs. kontroll av signatur, verifierar att den aktuella uppgiften härrör från ett äkta dokument och att uppgifterna inte har ändrats. Alla chipförsedda pass har denna signaturegenskap.

- Uppgifterna kan dock ha kopierats från chipet när som helst. Det krävs ingen särskild angreppspotential för att kopiera uppgifterna, eftersom uppgifterna, utom fingeravtrycket, i regel får avläsas fritt på chipet.

- För pass och identitetskort går det även att göra en aktiv autentisering eller en chipautentisering. Genom chipautentisering är det möjligt att försäkra sig om att chipet är äkta och om att uppgifterna inte har kopierats, dvs. att det just för tillfället finns ett äkta dokument bakom distansuppkopplingen.

- När kontrollen av att chipet och dess uppgifter är äkta och inte kopierade har gjorts, kan man lita på ansiktsfotot som har avlästs på chipet. Det är i regel av god kvalitet och betydligt större än fotot på beviset. Därför kan man lita på bilduppgiften. Eftersom fotot på chipet är av högre kvalitet, lämpar det sig bättre för en ansiktsjämförelse än ett foto och/eller en video som har förmedlats via distansuppkoppling.

- Ett ansiktsfoto på ett elektroniskt identitetsbevis har inte nödvändigtvis lagrats på chipet och därför kan fotot inte avläsas på chipet och användas vid identifiering. I biometriska pass har fotot lagrats på chipet.

- 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. Leverantörer av identifieringstjänster ska dessutom säkerställa att de uppgifter som de behöver för tillhandahållandet av identifieringstjänster är uppdaterade enligt uppgifterna i befolkningsdatasystemet.

- 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.

- Om det finns möjlighet att använda även ett annat lands motsvarande register eller tjänster där man kan kontrollera att ett identitetsbevis eller pass är giltigt samt att identiteten är befintlig och att personen som uppger identiteten har samma identitet så kan dessa utnyttjas.

    - (Jfr Förordningen om tillitsnivå 2.1.2 låg, punkt 3: Den tillförlitliga källan känner till att den anmälda identiteten är befintlig och man kan anta att personen som uppger identiteten har denna samma identitet.

    - och höjd, punkt 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).

- En situation där uppgifterna som påvisar identiteten inte stämmer överens med uppgifterna i Befolkningsdatasystemet (om till exempel namnet eller personbeteckningen har bytts, eller om den handling som uppvisas är beviljat av exempelvis ett annat EU-land) ska man på annat sätt försäkra sig om sökandens identitet och handlingens giltighet.

- Det gäller att kontrollera att de via distansuppkoppling förmedlade uppgifterna om den som visar upp identitetsbeviset är äkta och kommer från denna person. Hänsyn ska tas till att datakommunikationen och systemet är tillförlitliga, huruvida det finns en risk för att det insända materialet är förfalskat eller om personens utseende har ändrats på ett sätt som är svårt att upptäcka via distansuppkoppling. I regel är kravet att videoförbindelsen används via en mobilapplikation eftersom en videoförbindelse som sker via datorns webbläsare lätt kan knäckas.

- Belysningsförhållandena och kvalitetskraven på videon ska vara definierade. Belysningen ska vara god och eventuella artefakter ska kunna iakttas, eftersom dessa är tecken på eventuell videomanipulation. Resolutionen ska vara god under hela den inledande identifieringen på distans. Om det förekommer störningar på videon ska identifieringshändelsen avbrytas och vid behov inledas på nytt.

- Vid identifiering via distansuppkoppling finns det genom att rikta uppmärksamhet på personens livlighet bättre möjligheter att försäkra sig om att innehavaren av identitetsbeviset är på plats när identitetsbeviset visas upp och om att det inte är fråga om en falsk inspelning. Personen gör till exempel begärda slumpmässiga gester i realtid. Olika metoder kan användas för att observera livligheten, såsom slumpmässig input i videoanalysen eller biosignaler som observerats på bilden. Personalen ska ha tillräcklig utbildning och omfattande anvisningar för observationen av livlighet. Observationen av livlighet med dator ska basera sig på slumpmässiga händelser eller begäran som riktas mot den kund som gör den inledande identifieringen på distans.

- Det ska vara möjligt att på ett tillförlitligt sätt jämföra egenskaperna hos en person på en video eller ett insänt foto med uppgifterna i identitetsbeviset (FAR-värde).

- Det finns inga specifikationer av hur en sådan jämförelse kan göras på ett tillförlitligt sätt. Via distansuppkoppling kan det i princip innebära en jämförelse som görs av en människa eller en automatisk elektronisk jämförelse i ett bakgrundssystem som båda ansiktsfotona har skickats till. I bedömningen av tillförlitligheten kan en jämförelsepunkt anses vara att en anställd i identifieringstjänsten observerar personen på plats och överensstämmelsen hos uppgifterna i identitetsbeviset och även kan observera personens beteende.

- Man bör beakta att observationer som datorn gör i regel är mer tillförlitliga än människors observationer. Därmed är det inte tillräckligt att endast använda en tjänsteman vid identifiering med distansuppkoppling.

Jfr även LoA guidance:

Det ska också finnas variationer i de egenskapsbaserade autentiseringsfaktorerna mellan olika personer för att det ska vara möjligt att specifiera en person. Exempel är fingeravtryck, handavtryck, handens blodkärl, ansikte, handens geometri och ögats iris.

Vid användning av biometriska faktorer är det viktigt att säkerställa att den person som en autentiseringsfaktor är knuten till är fysiskt närvarande på kontrollstället. På så sätt minskar risken för bedrägerier eller kopiering.

Synpunkter på lagstiftning som gäller avläsningen av chipet

- Enligt 5 a § i passlagen 671/2006 innehåller ett pass en teknisk del enligt rådets förordning (EG) nr 2252/2004 om standarder för säkerhetsdetaljer och biometriska kännetecken i pass och resehandlingar som utfärdas av medlemsstaterna (EU:s passförordning).

  I den tekniska delen lagras passinnehavarens ansiktsbild och de fingeravtryck som avses i 6 a § inklusive nödvändiga tilläggsuppgifter i enlighet med vad som bestäms i EU:s passförordning. I den tekniska delen kan också de uppgifter lagras som avses i 5 § 1 mom. I EU:s passförordning finns bestämmelser om passinnehavarens rätt att kontrollera de uppgifter om honom eller henne som finns lagrade i passets tekniska del.

  Bestämmelser om passets säkerhetsdetaljer och biometriska kännetecken finns i EU:s passförordning. På pärmen till ett pass med ett biometriskt kännetecken finns en symbol som anger detta.

- Enligt 5 b § i passlagen får fingeravtryck som har lagrats i passets tekniska del avläsas endast så som bestäms i EU:s passförordning. Fingeravtryck får avläsas av en passmyndighet som avses i 10 § och av en polis- eller gränskontrollmyndighet. […]

  Vid avläsning av fingeravtryck får uppgifter om passinnehavaren inte behandlas på annat sätt än vad som bestäms i EU:s passförordning och i denna lag.

  Utöver vad som i denna lag bestäms om avläsande av fingeravtryck ska gemenskapens lagstiftning och internationella avtal som är bindande för Finland iakttas.

- I passlagen har avläsningen av fingeravtrycken begränsats till utsedda myndigheter, men avläsningen av ansiktsbilden har inte begränsats.

- Enligt 5 a § i lagen om identitetskort (663/2016) får de fingeravtryck och den ansiktsbild som har lagrats i identitetskortets tekniska del avläsas endast på det sätt som föreskrivs i EU:s förordning om identitetskort. Fingeravtryck får avläsas av en utfärdande myndighet som avses i 18 §, av polisen och av Gränsbevakningsväsendet. Dessutom får fingeravtryck avläsas av Tullen när den är förundersökningsmyndighet eller fullgör uppgifter som gränskontrollmyndighet. [...]

- Avläsningen av fingeravtryck har alltså begränsats bara till vissa myndigheter, men avläsningen av ansiktsbilden har inte begränsats i lagen.

- Enligt artikel 11 punkt 6 i EU:s ID-förordning (EU) 2019/1157 får biometriska uppgifter som lagrats på lagringsmedium på identitetskort och uppehållshandlingar bara användas i enlighet med unionsrätten och nationell rätt av vederbörligen bemyndigad personal vid behöriga nationella myndigheter och unionsbyråer.

  Enligt förordningens recital 22 bör biometriska kännetecken samlas in och lagras på lagringsmedium på identitetskort och uppehållshandlingar i syfte att kontrollera handlingens äkthet och innehavarens identitet. En sådan kontroll bör kunna göras endast av vederbörligen bemyndigad personal när uppvisande av handlingen krävs enligt lag eller annan författning. Enligt recital 19 bör medlemsstaterna som allmän praxis för att kontrollera handlingens äkthet och innehavarens identitet i första hand kontrollera ansiktsbilden och, om det behövs för att med säkerhet bekräfta handlingens äkthet och innehavarens identitet, även kontrollera fingeravtrycken. Enligt recital 17 krävs säkerhetsdetaljer för att kontrollera om en handling är äkta och för att fastställa en persons identitet. Införande av minimisäkerhetsstandarder och införlivande av biometriska uppgifter på identitetskort [...] är viktiga steg på vägen för att göra användningen av dessa handlingar säkrare i unionen. **Införlivande av sådana biometriska kännetecken bör ge unionsmedborgarna möjlighet att till fullo utnyttja sin rätt till fri rörlighet.** Enligt recital 15 även särskilt ”Denna **förordning påverkar inte medlemsstaternas användning av identitetskort** och uppehållshandlingar med elektronisk identifieringsfunktion i **andra syften** och **påverkar inte heller reglerna** i Europaparlamentets och rådets **förordning (EU) nr 910/2014**, som föreskriver ömsesidigt erkännande inom hela unionen av elektronisk identifiering för **tillgång till offentliga tjänster** och underlättar för medborgare som flyttar till en annan medlemsstat genom att kräva öm-

sesidigt erkännande av elektronisk identifiering med förbehåll för vissa villkor. **Förbättringar av identitetskorten bör underlätta identifiering och bidra till bättre tillgång till tjänster**."

- Enligt punkt 2.1.2 i bilagan till kommissionens genomförandeförordning som utfärdats med stöd av eIDAS-förordningen (EU) 2015/1502 (LoA, förordningen om tillitsnivå) förutsätts tillitsnivå hög **när en person** har kontrollerats och befunnits inneha fotografiskt eller **biometriskt identifieringsbevis** som erkänns i den medlemsstat där ansökan om medlet för elektronisk identitet görs, och den bevisningen avser den påstådda identiteten, **kontrolleras beviset** för att fastställa om det är giltigt enligt en tillförlitlig källa.

- Största delen av uppgifterna på identitetskorten kan fritt läsas, men en del är förhindrade utan rätt certifikat. Förhindrade är särskilt fingeravtryck vars avläsning genom lag har avgränsats endast till utsedda myndigheter. Läsningen av ansiktsbilden har oftast inte förhindrats och på marknaderna finns det många avgiftsfria applikationer för att avläsa ansiktsbilden. (OBS! Dessa är i regel inte som sådana användbara som informationssäkra metoder)

- Enligt artikel 9 punkt 1 i dataskyddsförordningen är behandling av [...] biometriska uppgifter för att entydigt identifiera en fysisk person [...] förbjuden. Enligt punkt 2 underpunkt g) i artikeln är behandlingen av uppgifterna som nämns i punkt 1 tillåten på grundval av medlemsstaternas nationella rätt, vilken ska stå i proportion till det eftersträvade syftet, vara förenligt med det väsentliga innehållet i rätten till dataskydd och innehålla bestämmelser om lämpliga och särskilda åtgärder för att säkerställa den registrerades grundläggande rättigheter och intressen.

- I situationer där man skulle avläsa ansiktsbilden kan kunden i regel neka till detta och i stället gå för personlig identifikation. Kunden kan även välja att godkänna avläsningen av ansiktsbilden och då sköta identifieringen på distans.

- European Banking Authority (EBA) har publicerat en anvisning om identifiering av kunden på distans (https://www.eba.europa.eu/eba-publishes-guidelines-remote-customer-onboarding).

    - Paragraph 35:
      "In situations where the device the customers use to prove their identity allows the collection of relevant data, for example because the data is contained in the chip of a national identity card, and it is technically feasible for the credit and financial institutions to access this data, credit and financial institutions should consider using this information to verify its consistency with the information obtained through other sources, such as the submitted data or other documents submitted by the customer. "

    - Paragraph 39:
      "Where the remote customer onboarding solution involves the use of biometric data to verify the customer's identity, credit and financial institutions should make sure that the biometric data is sufficiently unique to be unequivocally linked to a single natural person. [...]"

- EBA gör tolkningen att det är tillåtet och lönar sig att på identitetsbevisen avläsa bl.a. ansiktsbilden då kunden identifieras på distans.

- Transport- och kommunikationsverket stöder sig i sin tolkning på EBA:s anvisning och även på att EU:s ID-förordning inte begränsar tillämpningen av eIDAS-förordningen och att avläsningen av biometriska uppgifter möjliggörs i förordningen om tillitsnivå som utfärdats med stöd av eIDAS-förordningen. På grundval av dessa konstaterar verket att avläsningen av ansiktsbild på ett identitetskort eller ett pass inte verkar vara förbjudet enligt lag och att det rent av enligt förordningen om tillitsnivå verkar förutsättas på tillitsnivån hög. Därmed är det ett bra sätt att möjliggöra identifiering av kunden på distans.

3.11 Identifieringsverktygs, eller identifieringsmetoders, livscykel

Kraven föreskrivs i följande bestämmelser:

- Ansökan och registrering: 7 § och 20 § i autentiseringslagen, M72B, 6.3
- Utfärdande, leverans och aktivering, 20 § och 21 § i autentiseringslagen, LoA Bilaga, 2.2.2
- Upphävande, återkallelse och återaktivering, 25 § och 26 § i autentiseringslagen (LoA Bilaga, 2.2.3)
- Förnyelse och ersättning, 22 § i autentiseringslagen, LoA Bilaga, 2.2.4

Av inspektionsberättelsen ska det framgå på vilket sätt och på vilken grund man har bedömt att

- ✓ de personuppgifter som gäller identifieringsverktyget är riktiga
- ✓ leverans, upphävande, återkallelse, återaktivering, förnyelse och ersättning av identifieringsverktyget i sin helhet har genomförts så att det har säkerställts att identifieringsverktyget kontinuerligt besitts av rätt innehavare.

I december 2018 offentliggjorde Transport- och kommunikationsverket en anvisningspromemoria[8] som behandlar kontroll av identitet i anslutning till underhåll.

3.12 Testning

Identifikationssystemet och dess komponenter ska testas omfattande och regelbundet. Varje ändring ska testas innan de tas i produktion. Särskilt ska man testa även negativa testfall för att sträva efter uppkomsten av felaktiga händelser.

[8] Se Tolkningsställningstagande *dnr: Traficom/106/09.02.00/2019 (25.3.2019) Transport- och kommunikationsverkets tolkningspromemoria om 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.* Ställningstagandet finns på ämbetsverkets webbplats på https://www.kybertur-vallisuuskeskus.fi/sv/elektronisk-identifiering

BILAGA A: Minneslista om anvisningen om inspektionsberättelse

Denna bilaga innehåller en minneslista över innehållet i anvisningen om inspektionsberättelse. Inom parentes står hänvisningen till den punkt där frågan behandlas i anvisningen.

1. Bedömningsorganets identifierings- och kontaktuppgifter (2.4.1)

    1) Företagets eller organisationens namn och unika registreringsnummer

    2) om företaget eller organisationen har etablerat sig i någon annan stat i EES-området än i Finland, det register där den utländska organisationen eller det utländska företaget har förts in

    3) postadress och kontaktpersoner

    4) e-postadresser med tanke på förfrågningar från Transport- och kommunikationsverket.

2. Bedömningsorganets kompetens och oberoende (2.4.2)

    - En redogörelse kan lämnas i inspektionsberättelsen eller i övrigt tillsammans med anmälan.

3. Tidpunkt för bedömning och bedömningens längd enligt personarbetstiden (2.5.1)

4. Bedömningsmetoder (2.5.2)

5. Uppgifter om den dokumentation som har använts vid bedömningen av överensstämmelsen (2.5.3)

6. Beskrivning av vilken del av identifieringsmetoden och/eller identifieringssystemet bedömningen omfattar (2.3.3)

7. Namn (alla) på den identifieringstjänst som är föremål för bedömning (2.3.4)

8. Beskrivning av identifieringsmetoden (identifieringsverktyget) (2.3.5)

9. Beskrivning av identifieringssystemet (systemarkitekturen) (2.3.6)

10. Avvikelser (2.8-2.9)

11. Resultat av bedömning av olika delområden (3.1–3.12 i tillämpliga delar)

Anvisning om bedömning av elektroniska identifieringstjänster

Transport- och kommunikationsverkets anvisning

211/2023 O Bilaga C Mobilkriterier

BILAGA B: Allmänna kriterier för bedömning av en identifieringstjänst

B 1 Identifieringsmedlets egenskaper och skyddsförmåga

CENTRALA BESTÄMMELSER

M72B 15.1 Funktioner som ska bedömas i identifieringssystemet och identifieringsmedlet
En bedömning enligt 29 § i autentiseringslagen måste omfatta alla de krav som ställs i lagen och i denna föreskrift som gäller
[…]
2) identifieringsmetod, dvs. identifieringsverktyg
[…]
c) identifieringsmedlets egenskaper och utformning;
[…]
g) autentiseringsmekanismer.

6 § Krav på informationssäkerhet i identifieringsmetoder
6.1 Identifieringsmedlets egenskaper och skyddsförmåga
6.1.1
Identifieringsmedlets autentiseringsfaktorer, autentiseringsmekanism och säkerhetsåtgärder ska planeras, genomföras och upprätthållas så att de skyddar identifieringsmedlets integritet och sekretess. Identifieringsmedlet ska ha skyddsförmåga åtminstone på tillitsnivån väsentlig eller hög mot hot och angreppspotential enligt punkt 2.3 i bilagan till förordningen om tillitsnivåer vid elektronisk identifiering, i enlighet med identifieringstjänstens tillitsnivå.
Skyddsförmågan ska basera sig på en riskbedömning, där man separat bedömer hot mot autentiseringsfaktorer och -mekanismer som baserar sig på innehav, information och egenskaper samt säkerhetsåtgärder som skyddar mot hoten.

6.1.2
Genom identifieringsmedlets egenskaper och säkerhetsåtgärder ska man förhindra att äventyrande av en autentiseringsfaktor äventyrar tillförlitligheten hos andra autentiseringsfaktorer. Genom identifieringsmedlets säkerhetsåtgärder ska man separera och skydda autentiseringsfaktorerna i synnerhet om de används på samma terminal.

6.1.3
I identifieringsmedlet och autentiseringen måste man använda krypteringslösningar som rekommenderas internationellt eller nationellt. I datakommunikationsförbindelsen mellan identifieringsverktyget och identifieringssystemet ska man till de delar det är tekniskt tillämpligt använda krypteringslösningar enligt punkt 7 i föreskriften, om inte skyddsförmågan bedömd som helhet förverkligas genom andra säkerhetsåtgärder.

6.2 Särskilda säkerhetsåtgärder
6.2.1

Vid identifieringen ska identifieringstjänsten visa användaren av identifieringsverktyget information utifrån vilken användaren kan säkerställa att den begäran om identifiering som användaren får i identifieringsverktyget gäller användarens ärende. Visning av informationen är obligatorisk vid sådana identifieringsmedel där det är tekniskt möjligt.

6.2.2
Vid identifieringen ska identifieringstjänsten visa användaren av identifieringsverktyget information om den förlitande parten till vilken identifieringen förmedlas. Visning av informationen är obligatorisk vid sådana identifieringsmedel där det är tekniskt möjligt.

6.2.3
Med engångsinloggning avses i denna föreskrift att identifieringstjänsten erbjuder fler än en förlitande part bekräftelse utifrån en autentisering av en innehavare av ett identifieringsverktyg som gjorts med ett starkt elektroniskt identifieringsmedel.
Identifieringstjänsten ska i planeringen, genomförandet och upprätthållandet av engångsinloggning sörja för säkerhetsåtgärder som anknyter till hanteringen av engångsinloggningssessionernas längd samt överföringen och avslutandet av dem samt

6.3 Koppling av ett identifieringsverktyg till en person
6.3.1
Identifieringsmedlets autentiseringsfaktorer ska kopplas till innehavaren av identifieringsverktyget i identifieringssystemet.

6.3.2
Identifieringsverktyg får inte kopplas med den sökande förrän en inledande identifiering av den sökande har gjorts, eller så ska det vid processen för beviljande av identifieringsverktyg på annat sätt säkerställas att identifieringsverktyget inte kan användas innan en inledande identifiering av sökanden enligt 17 § i autentiseringslagen har gjorts.

6.4 Behandling av innehavarspecifika uppgifter i identifieringsmedlet
6.4.1
Leverantören av identifieringstjänsten ska säkerställa att hemliga uppgifter om identifieringsverktyget inte under några omständigheter röjs för dess personal.

6.4.2
Leverantören av identifieringstjänsten får inte kopiera hemliga uppgifter om identifieringsverktyget.

NR	TILL-LITS-NIVÅ	SAMMANDRAG ÖVER KRAVEN PÅ IDENTIFIERINGSTJÄNS-TEN	BESTÄMMELSER	STANDARD HÄNVIS-NING	OBSERVATIONER
1.	S, H	Det finns en riskbedömning för identifieringsmetoden (uträk-nande av angreppspotentialen)	**Autentiseringslagen 8 § Krav på system för elektronisk identifiering** 8 § 1 mom. 3) med hjälp av identifieringsmet-oden går det att säkerställa att endast innehava-	ISO 29115 ISO/IEC 15408-1	T.ex. Common Criteria CCDB 2009 03, avsnitt 3, eller ETSI TS 102 165-1, avsnitt 6.6 och 6.7 om ut-

			ren 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. **LoA Bilaga 2.3.1 Autentiseringsmekanism** 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 (”moderate”) kan underminera autentiseringsmekanismerna. **M72B 6.1.1** Identifieringsmedlets autentiseringsfaktorer, autentiseringsmekanism och säkerhetsåtgärder ska planeras, genomföras och upprätthållas så att de skyddar identifieringsmedlets integritet och sekretess. Identifieringsmedlet ska ha skyddsförmåga åtminstone på tillitsnivån väsentlig eller hög mot hot och angreppspotential enligt punkt 2.3 i bilagan till förordningen om tillitsnivåer vid elektronisk identifiering, i enlighet med identifieringstjänstens tillitsnivå. Skyddsförmågan ska basera sig på en **riskbedömning**, där man separat bedömer hot mot autentiseringsfaktorer och -mekanismer som baserar sig på innehav, information och egenskaper samt säkerhetsåtgärder som skyddar mot hoten.	ISO/IEC 18045, bilaga B Common Criteria CCDB 2009 03, stycke 3 ETSI TS 102 165-1, stycken 6.6 och 6.7	räkningen av angreppspotentialen. Att riskbedömningen genomförs på ändamålsenligt sätt är utgångspunkten för uträkningen av angreppspotentialen.
2.	S, H	Autentiseringsmetoden använder minst två autentiseringsfaktorer från olika kategorier.	**Autentiseringslagen 8 a § Autentiseringsfaktorer som ska användas i identifieringsmetoden i autentiseringslagen** […] 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. […] **LoA bilaga 2.2.1 Medel för elektronisk identifiering: egenskaper och utformning** Medlet för elektronisk identifiering använder minst två autentiseringsfaktorer från olika kategorier.		
3.	S, H	Autentiseringsfaktorerna är oberoende av varandra.	**LoA bilaga 2.2.1 Medel för elektronisk identifiering: egenskaper och utformning** Metoden för elektronisk identifiering är planerad så att den kan antas användas endast om den innehas av den person som den tillhör. **M72B 6.1.2** Genom identifieringsmedlets egenskaper och säkerhetsåtgärder ska man förhindra att äventyrande av en autentiseringsfaktor äventyrar tillförlitligheten hos andra autentiseringsfaktorer. Genom identifieringsmedlets säkerhetsåtgärder ska man separera och skydda autentiseringsfaktorerna i synnerhet om de används på samma terminal.		Vid identifieringsmetoder som används med mobilutrustning ska särskild uppmärksamhet fästas vid att autentiseringsfaktorerna är oberoende av varandra.
4.	S, H	Vid utformningen av en identifieringsmetod har hänsyn tagits till att olika autentiseringsfaktorer är utsatta för olika hot.	**LoA bilaga 2.2.1 Medel för elektronisk identifiering: egenskaper och utformning** Metoden för elektronisk identifiering är planerad så att den kan antas användas endast om den innehas av den person som den tillhör. **M72B 6.1.2** Genom identifieringsmedlets egenskaper och säkerhetsåtgärder ska man förhindra att äventyrande av en autentiseringsfaktor äventyrar tillförlitligheten hos andra autentiseringsfaktorer. Genom identifieringsmedlets säkerhetsåtgärder ska		

			man separera och skydda autentiseringsfaktorerna i synnerhet om de används på samma terminal.		
5.	S, H	Personalen och underleverantörerna till en leverantör av identifieringstjänster får inte kännedom om hemliga uppgifter om identifieringsmetoden.	**M72B 6.4 Behandling av innehavarspecifika uppgifter i identifieringsmedlet** 6.4.1 Leverantören av identifieringstjänsten ska säkerställa att hemliga uppgifter om identifieringsverktyget inte under några omständigheter röjs för dess personal. 6.4.2 Leverantören av identifieringstjänsten får inte kopiera hemliga uppgifter om identifieringsverktyget.		Hemliga uppgifter är till exempel pinkoder och andra kunskapsbaserade autentiseringsfaktorer. Syftet med kravet är att beakta risken för att anställda i identifieringstjänsten är oärliga.
6.	S, H	Autentiseringsfaktorerna har bekräftats vara bundna till en person.	**LoA Bilaga 1 Tillämpliga definitioner** 2) med ”autentiseringsfaktor” avses en faktor som bekräftas vara bunden till en person och som tillhör någon av följande kategorier […] **LoA bilaga 2.2.1 Medel för elektronisk identifiering: egenskaper och utformning** Metoden för elektronisk identifiering är planerad så att den kan antas användas endast om den innehas av den person som den tillhör. **M72B 6.3 Koppling av ett identifieringsverktyg till en person** 6.3.1 Identifieringsmedlets autentiseringsfaktorer ska kopplas till innehavaren av identifieringsverktyget i identifieringssystemet. 6.3.2 Identifieringsverktyg får inte kopplas med den sökande förrän en inledande identifiering av den sökande har gjorts, eller så ska det vid processen för beviljande av identifieringsverktyg på annat sätt säkerställas att identifieringsverktyget inte		Till exempel bindning mellan en identifieringsapp och en person, personifiering av chipet, bindning mellan en person och en kodtabell eller enhet.

			kan användas innan en inledande identifiering av sökanden enligt 17 § i autentiseringslagen har gjorts.		
7.	S, H	Vid utformningen av en identifieringsmetod har hänsyn tagits till att olika autentiseringsfaktorer är utsatta för olika hot.	**Autentiseringslagen 8 a § Autentiseringsfaktorer som ska användas i identifieringsmetoden i autentiseringslagen** […] 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. **LoA Bilaga 1 Tillämpliga definitioner** 3) med dynamisk autentisering avses 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, **LoA Bilaga 2.3.1 Autentiseringsmekanism** Innan personidentifieringsuppgifter lämnas ut sker en tillförlitlig kontroll av medlet för elektronisk identifiering och dess giltighet med hjälp av en dynamisk autentisering.		Även identifieringsförmedlingstjänster LoA guidance (utdrag) Det primära syftet med dynamisk autentisering är att minska risken för exempelvis man-i-mitten-attacker eller risken för att verifieringsuppgifterna från ett tidigare sparat autentiseringstillfälle används på nytt. […] Man bör komma ihåg att autentisering som baserar sig på flera faktorer inte är detsamma som dynamisk autentisering. I autentisering som baserar sig på flera faktorer krävs inte att autentiseringen sker dynamiskt (exempel är PIN-kod och fingeravtrycksuppgifter), så ett sådant autentiseringssätt kan vara mer sårbart för replay-angrepp än dynamisk autentisering. […] Om en persons privata nyckel har lagrats som distanstjänst (centraliserat exempelvis på en HSM-enhet som används av en leverantör av identifieringsuppgifter), måste det autentiseringssätt som krävs

					för användning av den privata nyckeln också vara dynamiskt.
8.	S, H	Identifieringshändelsens elektroniska verifikat baserar sig på autentiseringsfaktorer kopplade till personen	**LoA Bilaga 1 Tillämpliga definitioner** 3) med dynamisk autentisering avses 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, **M72B 6.3 Koppling av ett identifieringsverktyg till en person** 6.3.1 Identifieringsmedlets autentiseringsfaktorer ska kopplas till innehavaren av identifieringsverktyget i identifieringssystemet. **LoA Bilaga 2.3.1 Autentiseringsmekanism** Väsentlig: 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 (”moderate”) kan underminera autentiseringsmekanismerna.		Autentiseringsfaktorerna ska inte gå att kopiera.
9.	H	Användaren kan på ett tillförlitligt sätt skydda metoden (verktyget) och sina autentiseringsfaktorer mot användning av andra.	**LoA bilaga 2.2.1 Medel för elektronisk identifiering: egenskaper och utformning** Metoden för elektronisk identifiering är planerad så att personen det tillhör kan skydda det på ett tillförlitligt sätt från användning av andra.		Exempel LoA-guidance: Med ”tillförlitligt skydd” avses åtgärder för att skydda ett medel för elektronisk identifiering så

			Även **LoA Bilaga 2.2.2 Utfärdande, leverans och aktivering** Aktiveringsprocessen kontrollerar att medlet för elektronisk identifiering endast levererades till ägaren som det tillhör. **M72B 6.1 Identifieringsmedlets egenskaper och skyddsförmåga** 6.1.1 Identifieringsmedlets autentiseringsfaktorer, autentiseringsmekanism och säkerhetsåtgärder ska planeras, genomföras och upprätthållas så att de skyddar identifieringsmedlets integritet och sekretess. Identifieringsmedlet ska ha skyddsförmåga åtminstone på tillitsnivån väsentlig eller hög mot hot och angreppspotential enligt punkt 2.3 i bilagan till förordningen om tillitsnivåer vid elektronisk identifiering, i enlighet med identifieringstjänstens tillitsnivå. 6.1.2 Genom identifieringsmedlets egenskaper och säkerhetsåtgärder ska man förhindra att äventyrande av en autentiseringsfaktor äventyrar tillförlitligheten hos andra autentiseringsfaktorer. Genom identifieringsmedlets säkerhetsåtgärder ska man separera och skydda autentiseringsfaktorerna i synnerhet om de används på samma terminal. **M72B 6.4 Behandling av innehavarspecifika uppgifter i identifieringsmedlet** 6.4.1 Leverantören av identifieringstjänsten ska säkerställa att hemliga uppgifter om identifieringsverktyget inte under några omständigheter röjs för dess personal. 6.4.2		att medlet inte kan användas utan att ägaren har kännedom om användning och inte har gett ett aktivt samtycke till användning. Exempelvis en privat nyckel till koden för en krypteringsnyckel kan inte vara en sådan nyckel som kan användas utan användarens aktiva samtycke, (såsom att ge pinkoden), i maskinella processer. Detta krav skyddar mot hot om kopiering, gissning, omspelning och manipulation av kommunikation. Följande kan också användas utöver ovannämnda tekniker (se även LOA guidance: 2.2.1 hög): - Starka statiska lösenord - Biometrisk identifiering av användare - Kontroll av miljö med tanke på skadliga koder - Identifiering utanför bandet - Vid alla autentiseringsfaktorer som utgår från sekretess (statiska lösenord, engångslösenord till hårdvara) utgör gissning ett hot som ska minskas för att tillitsnivån hög ska nås. Detta kan göras till

			Leverantören av identifieringstjänsten får inte kopiera hemliga uppgifter om identifieringsverktyget.		exempel genom att begränsa antalet försök, använda fördröjningsmekanismer och säkerställa en tillräcklig entropi. LoA-guidance punkt 2.2.2 hög: På nivån ”hög” ska man med aktiveringsprocessen säkerställa att endast den lagliga ägaren kan aktivera metoden för elektronisk identifiering och att aktiveringsprocessen är skyddad från att förstöras i misstag samt från insiderhot, såsom falskt samarbete. OBS! Användaren ska säkerställa att säkerhetsfaktorer eller till exempel återställningskoden kopplad till identifieringsverktyget inte är tillgängliga för andra. En eventuell aktiverings- eller återställningskod kan användas en gång. Med detta säkerställs att aktiveringskoder som används på nytt inte kan användas för att annullera, alltså överskriva den verifikationsfaktor (PIN) som endast användaren känner till utan att denne vet om

					detta. I autentiseringslagen finns ingen hänvisning till LoA punkt 2.2.3 (”Åtgärder ska föreligga för att förhindra att upphävande, återkallelse och/eller reaktivering sker på otillåtet sätt.”). Att koden endast kan användas en gång är dock bra praxis, om man inte på annat sätt kan skydda identifieringsverktyget mot olovlig reaktivering.
10.	S, H	Identifieringsuppgifter lämnas inte till förlitande parter. Det innebär att en identifieringstransaktion inte genomförs förrän identifieringsverktyget/identifieringsmetoden har kontrollerats med hjälp av en dynamisk autentisering.	**LoA Bilaga 2.3.1 Autentiseringsmekanism** Innan personidentifieringsuppgifter lämnas ut sker en tillförlitlig kontroll av medlet för elektronisk identifiering och dess giltighet med hjälp av en dynamisk autentisering.	A.14.1 Anskaffning, utveckling och underhåll av system/Säkerhetskrav på informationssystem A.14.1.2 Säkerställande av programtjänster på publika nätverk A.14.1.3 Skydd av transaktioner i tillämpningstjänster	Även identifieringsförmedlingstjänster
11.	S,H	Identifieringsuppgifter (personuppgifter) som lagras i identifieringstransaktioner skyddas.	**LoA Bilaga 2.3.1 Autentiseringsmekanism** 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.		Även identifieringsförmedlingstjänster Hänsyn ska tas till alla tekniska miljöer som del-

			M72B 7.1 Krypteringsmetoder för datakommunikationen 7.1.1 Trafiken i gränssnitten mellan leverantörer av identifieringstjänster och mellan leverantörer av identifieringstjänster och förlitande parter ska krypteras [se metoder i föreskriften eller nedan]. **M72B 9.1 Kryptering av meddelanden mellan identifieringstjänster och en part som förlitar sig på tjänsten** 9.1.1 I datakommunikation mellan identifieringstjänster samt mellan en identifieringstjänst och en förlitande part måste man trygga integriteten och sekretessen hos identifieringsmeddelanden som innehåller personuppgifter antingen a) genom att säkerställa datakommunikationsförbindelsens integritet och sekretess genom att knyta parternas datakommunikation till certifikat eller nycklar som levererats enligt punkt 8, eller b) genom att kryptera och underteckna meddelandena med nycklar som levererats enligt punkt 8.		tar i identifieringstransaktioner och där identifieringsuppgifter lagras.
12.	S	Säkerhetskontroller som en autentiseringsmekanism genomför skyddar mot angripare med måttlig angreppspotential.	**Autentiseringslagen 8 § Krav på system för elektronisk identifiering** 8 § 1 mom. 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. **LoA Bilaga 2.3.1 Autentiseringsmekanism** Autentiseringsmekanismen genomför säkerhetskontroller för att verifiera medlet för elektronisk identifiering, varför det är högst osannolikt att ex-	ISO 29115 ISO/IEC 15408-1 ISO/IEC 18045, bilaga B Common Criteria CCDB 2009 03, stycke 3	Jfr kriterium 1 riskbedömningen och uträknande av angreppspotentialen I bedömningen ska man beakta relevanta hot. I standarden ISO 29115 nämns exempelvis följande: gissande via nätet och utanför nätet, omspelning av identifierande uppgifter, fiske efter information, avlyssning, replay-attack, sessionskapning, man-i-mitten-attack, stöld

			empelvis gissningar, tjuvlyssning, omspelning eller manipulation av kommunikation som görs av en angripare med måttlig angreppspotential (”moderate”) kan underminera autentiseringsmekanismerna.	ETSI TS 102 165-1, stycken 6.6 och 6.7	av identifierande uppgifter, spoofing-attack och att utge sig för att vara någon annan. I standarden ISO/IEC 15408-1 definieras angreppspotential som den arbetsmängd som ett angrepp [mot en mekanism] kräver, uttryckt som angriparens sakkunskap, resurser och motivation. I standarden ISO/IEC 18045 / bilaga B.4 till CEM ges anvisningar för hur man beräknar den angreppspotential som krävs för att utnyttja en viss svaghet i en autentiseringsmekanism. Common Criteria och ETSI 102 165-1 innehåller anvisningar för uträkningen av angreppspotentialen. I autentiseringsmekanismer ska hänsyn även tas till hot som föranleds av att fel ärendehanteringstjänst har lämnat en identifieringsbegäran eller kapat identifieringssessioner (phishing). Se beskrivning i punkt 2.3.1 i LoA guidance

					Även identifieringsförmedlingstjänster
13.	H	Säkerhetskontroller som en autentiseringsmekanism genomför skyddar mot angripare med hög angreppspotential.	**Autentiseringslagen 8 § Krav på system för elektronisk identifiering** 8 § 1 mom. 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. **LoA bilaga 2.2.1 Medel för elektronisk identifiering: egenskaper och utformning** Medlet för elektronisk identifiering skyddar mot kopiering och manipulering samt mot angripare med hög (”high”) angreppskapacitet. **LoA Bilaga 2.3.1 Autentiseringsmekanism** 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 (”high”) kan underminera autentiseringsmekanismerna.	se ovan	Även identifieringsförmedlingstjänster Alla säkerhetsfaktorer för en autentiseringsmekanism i proportion till en hög angreppspotential
14.	S, H	Autentiseringsmekanismen visar e-tjänstens namn i de medel och skeden av identifieringsprocessen där det är möjligt	**M72B 6.2.2** Vid identifieringen ska identifieringstjänsten visa användaren av identifieringsverktyget information om den förlitande parten till vilken identifieringen förmedlas. Visning av informationen är obligatorisk vid sådana identifieringsmedel där det är tekniskt möjligt. **M72B 12.1 Obligatoriska uppgifter** Följande uppgifter ska förmedlas via gränssnitten mellan leverantörer av identifieringsverktyg och leverantörer av tjänster för identifieringsförmedling: [...] 4) information som verifierats av tjänsten för identifieringsförmedling om den förlitande parten		Även identifieringsförmedlingstjänster

15.	S, H	Autentiseringsmekanismen visar identifieraren för sessionen i de medel och skeden av identifieringsprocessen där det är möjligt	**M72B 6.2.1** Vid identifieringen ska identifieringstjänsten visa användaren av identifieringsverktyget information utifrån vilken användaren kan säkerställa att den begäran om identifiering som användaren får i identifieringsverktyget gäller användarens ärende. Visning av informationen är obligatorisk vid sådana identifieringsmedel där det är tekniskt möjligt.		Även identifieringsförmedlingstjänster
16.	S, H	I en autentiseringsmekanism följs obligatoriska krypteringskrav **mellan en leverantör av identifieringsverktyg och en identifieringsförmedling**.	**LoA Bilaga 2.4.6 Tekniska kontrolle**r (controls) 2. Elektroniska kommunikationskanaler som används för att utbyta personuppgifter eller känslig information skyddas mot avlyssning, manipulation och omspelning. **M72B 7.1 Krypteringskrav på identifieringssystemets gränssnitt** 7.1.1 Trafiken i gränssnitten mellan leverantörer av identifieringstjänster och mellan leverantörer av identifieringstjänster och förlitande parter ska krypteras. Följande metoder ska användas vid kryptering, vid nyckelutbyte, i certifikat 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) Underskrift eller asymmetrisk kryptering: Vid användning av RSA för elektronisk underskrift eller kryptering ska nyckeln utgöra minst 2 048 bitar. Vid användning av metoder för elliptisk kurva från ECDSA eller EdDSA ska storleken på den ändliga kroppen vara minst 224 bitar. 3) Symmetrisk kryptering: Krypteringsalgoritmen ska vara AES, Serpent eller ChaCha20. Nyckeln ska utgöra minst 128	A.10.1.1 Regler för användning av kryptografiska säkerhetsåtgärder A.13.2.3 Informationsöverföring: Elektronisk meddelandehantering	Även identifieringsförmedlingstjänster

			bitar. Krypteringsläget ska vara CBC, CCM, GCM eller CTR. 4) Hashfunktioner: Hashfunktionen eller autentiseringskoden ska vara SHA-2, SHA-3, Whirlpool eller Poly1305. 7.1.2 Utöver de som nämns i punkt 7.1.1 kan man följa metoder och värden som har bedömts vara säkra för sådan användning som avses i underpunkterna 1–4 i de aktuella versionerna av följande dokument: a) Anvisningen Kryptografiset vahvuusvaatimukset luottamuksellisuuden suojaamiseen – kansalliset turvallisuusluokat (Dnr 190/651/2015) av myndigheten för godkännande av krypteringsprodukter (Crypto Approval Authority) inom Transport- och kommunikationsverket, eller b) dokumentet SOG-IS Crypto Evaluation Scheme Agreed Cryptographic Mechanisms, utgivet av vissa certifieringsorgan i EU-medlemsstater eller i medlemsstater i EES-området (Senior Officers Group for Information Systems, Mutual Recognition Agreement SOGIS-MRA). 7.1.3 Krypteringsinställningarna ska tekniskt tvingas till miniminivåerna ovan för att handskakningen inte ska resultera i inställningar som är sämre än miniminivåerna. **7.2 Krypteringsprotokoll för datakommunikationen** Om man använder TLS-protokoll ska man använda minst version 1.2. Integriteten och sekretessen för meddelanden med personuppgifter ska skyddas förutom med		

			kryptering som avses i 1 mom. också på meddelandenivå enligt 1 mom. **M72B 8 Verifiering av parterna i datakommunikationen** **8.1 Identifiering av parterna i en datakommunikationsförbindelse** När man upprättar en datakommunikationsförbindelse mellan identifieringstjänster eller mellan en identifieringstjänst och en förlitande part måste man autentisera äktheten och integriteten hos de certifikat som används för att kryptera datakommunikationen eller meddelandena samt deras innehavare. Autentiseringen ska basera sig på en kvalificerad elektronisk underskrift eller en kvalificerad elektronisk stämpel enligt eIDAS-förordningen eller direkt på ett bilateralt förfarande. Autentiseringen kan inte baseras endast på ett certifikat som det råder allmänt förtroende för. **8.2 Förnyande av certifikat och nycklar** De certifikat och nycklar som avses ovan i punkt 8.1 ska förnyas regelbundet. För att säkerställa äktheten och integriteten hos nya certifikat och nycklar ska förnyelsen göras antingen a) enligt det förfarande som beskrivs i punkt 8.1, b) genom att skicka de nya nycklarna via en datakommunikationsförbindelse vars integritet och sekretess har säkerställts genom att knyta parternas datakommunikation till certifikat eller nycklar som levererats enligt punkt 8.1, eller c) genom att underteckna den nya nyckeln med en nyckel som levererats enligt punkt 8.1 eller en sådan kedjad nyckel.		

			M72B 9 Identifieringsmeddelandenas integritet och sekretess **9.1 Kryptering av meddelanden mellan identifieringstjänster och en förlitande part** 9.1.1 I datakommunikation mellan identifieringstjänster samt mellan en identifieringstjänst och en förlitande part måste man trygga integriteten och sekretessen hos identifieringsmeddelanden som innehåller personuppgifter antingen a) genom att säkerställa datakommunikationsförbindelsens integritet och sekretess genom att knyta parternas datakommunikation till certifikat eller nycklar som levererats enligt punkt 8, eller b) genom att kryptera och underteckna meddelandena med nycklar som levererats enligt punkt 8. 9.1.2 I datakommunikation mellan tjänsten för identifieringsförmedling och den förlitande part måste identifieringsmeddelanden autentiseras genom underskrift. **9.2 Kryptering av meddelanden i användargränssnittet** Om identifieringsmeddelanden förmedlas via användarens webbläsare eller terminal, måste de krypteras och undertecknas enligt underpunkt 9.1.1.b. **9.3 Krypteringsalgoritmer och metoder** Vid krypteringen och undertecknandet av meddelanden ska man till tillämpliga delar använda metoder enligt punkt 7.1.		
17.	S, H	I en autentiseringsmekanism följs obligatoriska kryp-	**LoA Bilaga 2.4.6 Tekniska kontrolle**r (controls) 2. Elektroniska kommunikationskanaler som används för att utbyta personuppgifter eller känslig	A.10.1.1 Regler för användning av kryptografiska	Obs. även identifieringsförmedlingstjänster

		teringskrav **mellan en identifieringstjänst och en tjänst för ärendehantering**.	information skyddas mot avlyssning, manipulation och omspelning. **M72B 7–8 (ovan)** **M72B 9 Identifieringsmeddelandenas integritet och sekretess** **9.1 Kryptering av meddelanden mellan identifieringstjänster och en förlitande part** 9.1.1 I datakommunikation mellan identifieringstjänster samt mellan en identifieringstjänst och en förlitande part måste man trygga integriteten och sekretessen hos identifieringsmeddelanden som innehåller personuppgifter antingen a) genom att säkerställa datakommunikationsförbindelsens integritet och sekretess genom att knyta parternas datakommunikation till certifikat eller nycklar som levererats enligt punkt 8, eller b) genom att kryptera och underteckna meddelandena med nycklar som levererats enligt punkt 8. **9.2 Kryptering av meddelanden i användargränssnittet** Om identifieringsmeddelanden förmedlas via användarens webbläsare eller terminal, måste de krypteras och undertecknas enligt underpunkt 9.1.1.b. **9.3 Krypteringsalgoritmer och metoder** Vid krypteringen och undertecknandet av meddelanden ska man till tillämpliga delar använda metoder enligt punkt 7.1.	säkerhetsåtgärder A.13.2.3 Informationsöverföring: Elektronisk meddelandehantering A 14.1.1. Analys och specifikation av informationssäkerhetskrav A 14.1.2 Säkerställande av programtjänster på publika nätverk	
18.	S, H	I en autentiseringsmekanism följs obligatoriska krypteringskrav i användargränssnitt	**LoA Bilaga 2.4.6 Tekniska kontrolle**r (controls) 2. Elektroniska kommunikationskanaler som används för att utbyta personuppgifter eller känslig information skyddas mot avlyssning, manipulation och omspelning.	A.10.1.1 Regler för användning av kryptografiska	Obs. även identifieringsförmedlingstjänster

		(webbläsare, mobil användning)	**M72B 7 (ovan)** **M72B 9.2 Kryptering av meddelanden i användargränssnittet** Om identifieringsmeddelanden förmedlas via användarens webbläsare eller terminal, måste de krypteras och undertecknas enligt underpunkt 9.1.1.b. **M72B 9.3 Krypteringsalgoritmer och metoder** Vid krypteringen och undertecknandet av meddelanden ska man till tillämpliga delar använda metoder enligt punkt 7.1.	säkerhetsåtgärder A.13.2.3 Informationsöverföring: Elektronisk meddelandehantering A 14.1.1. Analys och specifikation av informationssäkerhetskrav A 14.1.2 Säkerställande av programtjänster på publika nätverk	
19.	H	I en autentiseringsmekanism följs de skärpta krypteringskrav som fastställs i **rekommendationen**/krypteringskraven på tillitsnivån hög, när autentiseringsmekanismen används mellan leverantören av identifieringsverktyget och en leverantör av en identifieringsförmedlingstjänst, mellan en identifieringstjänst och en ärendehanteringstjänst och i användargränssnitt (webbläsare, mobil användning).	**MPS M72B punkt 4.7.1.3 (20.5.2022) rekommendation** För tillitsnivån hög i identifieringssystem rekommenderas det att man i stället för de värden som förutsätts för tillitsnivån väsentlig enligt 7.1 i föreskriften tillämpar följande värden inom parentes, **med vilka man uppnår en styrka på 128 bitar**: 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 (**4 096 på tillitsnivån hög**) bitar i DHE-metoden och minst 224 (**256 på tillitsnivån hög**) bitar i ECDHE-metoden.*	A.10.1.1 Regler för användning av kryptografiska säkerhetsåtgärder A.13.2.3 Informationsöverföring: Elektronisk meddelandehantering	Obs. även identifieringsförmedlingstjänster

			DH-grupperna 14-21, 23, 24 och 26 (***16-21 på tillitsnivån hög***) enligt IANAs IKEv2-parametrar uppfyller kraven ovan. 2) Underskrift eller asymmetrisk kryptering: Vid användning av RSA för elektronisk underskrift eller kryptering ska nyckeln utgöra minst 2 048 (**3 072 på tillitsnivån hög**) bitar. Vid användning av ECDSA- eller EdDSA-metoden för elliptisk kurva ska den ändliga kroppen nedan utgöra minst 224 (**256 på tillitsnivån hög**) bitar. 3) Symmetrisk kryptering: *Krypteringsalgoritmen ska vara AES, Serpent eller ChaCha20 (***på tillitsnivån hög AES eller Serpent***). Nyckeln ska utgöra minst 128* (**128 på tillitsnivån hög**) bitar. Krypteringsläget ska vara CBC, CCM, GCM eller CTR. 4) Hashfunktioner: Hashfunktionen eller autentiseringskoden ska vara SHA-2, SHA-3, Whirlpool eller Poly1305. *Med SHA-2 avses funktionerna SHA224, SHA256, SHA384 och SHA512* (**på tillitsnivån hög SHA-3-256, SHA-3-384, SHA-3-512**)		

B 2 Interoperabilitet

CENTRALA BESTÄMMELSER

Autentiseringslagen 29 § Bedömning av överensstämmelse hos en elektronisk identifieringstjänst
En leverantör av identifieringstjänster ska regelbundet låta ett sådant bedömningsorgan som nämns i 28 § bedöma om identifieringstjänsten uppfyller kraven på interoperabilitet, informationssäkerhet, dataskydd och annan tillförlitlighet enligt denna lag.
[…]

M72B 15 Bedömningskriterier för överensstämmelse
En bedömning enligt 29 § i autentiseringslagen måste omfatta alla de krav som ställs i lagen och i denna föreskrift som gäller
1) funktioner som påverkar tillhandahållandet av identifieringstjänsten (ett identifieringssystem)
d) tekniska åtgärder
e) interoperabiliteten i förtroendenätet

Autentiseringslagen 12 a § Förtroendenätet för leverantörer av identifieringstjänster
[…]
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.
[…]

M72B 12 Minimiuppsättning uppgifter som ska förmedlas i förtroendenätet
12.1 Obligatoriska uppgifter
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 som autentiserats av leverantören av identifieringsverktyget samt personens förnamn, efternamn och födelsedatum,
2) vid identifiering av en juridisk person åtminstone den identifieringsuppgift som autentiserats av leverantören av identifieringsverktyget som identifierar den fysiska personen som företräder den juridiska personen, personens efternamn och förnamn samt den identifieringsuppgift som identifierar organisationen,
3) information om huruvida identifieringsverktyget ligger på tillitsnivån väsentlig eller hög, och
4) information som verifierats av tjänsten för identifieringsförmedling om den förlitande parten

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

1) information om huruvida 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, och
3) vid identifiering av en juridisk person:
   a) nuvarande adress,
   b) momsregistreringsnummer,
   c) skatteregisteringsnummer,
   d) Den identifikator som avses i artikel 3.1 i Europaparlamentets och rådets direktiv 2009/101/EG,
   e) den identifieringskod för juridiska personer (LEI) som avses i kommissionens genomförandeförordning (EU) nr 1247/20122,
   f) det registrerings- och identitetsnummer för ekonomiska aktörer (EORI-nummer) som avses i kommissionens genomförandeförordning (EU) nr 1352/20133, och
   g) punktskattenummer som avses i artikel 2.12 i rådets förordning nr 389/20124.

12.3 Pseudonymisering av identifiering
De skyldigheter som definieras ovan i punkterna 12.1 och 12.2 gäller gränssnittet mellan identifieringsverktyget och tjänsten för identifieringsförmedling vid autentisering av identifieringsverktygets användare även i fall där tjänsten för identifieringsförmedling på det sätt som avses i 8 § 2 mom. i autentiseringslagen endast meddelar den förlitande parten en pseudonym för användaren av identifieringsverktyget eller en begränsad mängd personuppgifter.

14 Protokoll som används vid dataöverföring samt övriga krav
14.1 Protokoll som används vid dataöverföring

Leverantören av identifieringstjänsten ska för egen del möjliggöra sammankoppling av inledande identifieringar enligt 17 § i autentiseringslagen samt förmedling av identifieringar i förtroendenätet enligt 12 a § i autentiseringslagen åtminstone via gränssnitt enligt Open IDConnect- eller SAML-protokollet.

14.2 Gränssnittets övriga egenskaper
Leverantörer av identifieringsverktyg, leverantörer av tjänster för identifieringsförmedling och förlitande parter samt genomföraren av den nationella noden kan sinsemellan avtala om sådana övriga egenskaper för gränssnitten mellan dem och sådana tillämpliga protokoll som inte fastställs i denna föreskrift.

NR	TILL-LITS-NIVÅ	SAMMANDRAG ÖVER KRAVEN PÅ IDENTIFIERINGSTJÄNS-TEN	BESTÄMMELSER	STANDARD HÄNVIS-NING	OBSERVATIONER
20.	S, H	Leverantören av identifierings-tjänsten erbjuder minst ett gränssnitt enligt en allmänt an-vänd standard i förtroendenätet.	**SRF 169/2016 Statsrådets förordning om förtroendenätet för leverantörer av tjänster för stark autentisering** **1 § Förtroendenätets tekniska gränssnitt** De tekniska gränssnitt som avses i 12 a § 2 mom. i lagen om stark autentisering och elektroniska signaturer (617/2009), nedan autentiseringsla-gen, är 1) gränssnittet mellan leverantörer av identi-fieringsverktyg, 2) gränssnittet mellan en leverantör av iden-tifieringsverktyg och en leverantör av identifieringsförmedlingstjänster, 3) gränssnittet mellan en leverantör av iden-tifieringsförmedlingstjänster och en part som förlitar sig på identifieringstjänsterna. Leverantörer av identifieringstjänster som hör till förtroendenätet kan avtala om det gränssnitt som behövs för förmedlingen av debiteringen för en identifieringsuppgift som avses i 12 a § 3 mom. i autentiseringslagen eller om något annat gräns-snitt som behövs i förtroendenätets verksamhet. En leverantör av identifieringstjänster som hör till förtroendenätet ska i vartdera av de gränssnitt som avses i 1 mom. 1–2 punkten tillhandahålla minst ett tekniskt gränssnitt som baserar sig på en allmänt tillämpad standard.		**Tillämpning: Striktare krav i M72B punkt 14.1 ”gränssnitt minst enligt OpenID Connect eller SAML-protokollet”** Transport- och kommuni-kationsverket har utarbe-tat rekommendationsprofi-ler för SAML- och OpenID Connect-protokollen efter att ha hört förtroendenä-tets samarbetsgrupp. Rekommendation 212/2023 S (SAML) om förtroendenätets gräns-snitt Rekommendation 213/2023 S (OIDC) om förtroendenätets gräns-snitt Rekommendationerna finns på ämbetsverkets webbplats på

			M72B 14 Protokoll som används vid dataöverföring samt övriga krav **14.1 Protokoll som används vid dataöverföring** Leverantören av identifieringstjänsten ska för egen del möjliggöra sammankoppling av inledande identifieringar enligt 17 § i autentiseringslagen samt förmedling av identifieringar i förtroendenätet enligt 12 a § i autentiseringslagen åtminstone via gränssnitt enligt Open IDConnect- eller SAML-protokollet.		https://www.kyberturvallisuuskeskus.fi/sv/elektronisk-identifiering
21.	S, H	Leverantören av identifieringsverktyg tillhandahåller kravenliga uppgifter (attribut) vid identifiering av en **fysisk person**.	**M72B 12 Minimiuppsättning uppgifter som ska förmedlas i förtroendenätet** **12.1 Obligatoriska uppgifter** 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 som autentiserats av leverantören av identifieringsverktyget samt personens förnamn, efternamn och födelsedatum, […] 3) om identifieringsverktyget ligger på tillitsnivån väsentlig eller hög […]		Förmedlingstjänsten kan vid behov berika eller utarma uppgifterna som erhållits av leverantören av identifieringsverktyget (se M72B punkt 12.3). Leverantören av identifieringsverktyget ska i varje fall förmedla uppgifter enligt punkt 12.1 i M72B.
22.	S, H	Leverantören av identifieringsverktyg har en erforderlig **planerad beredskap** att förmedla optionella uppgifter vid identifiering av en **fysisk person**.	**M72B 12 Minimiuppsättning uppgifter som ska förmedlas i förtroendenätet** **12.2 Valfria uppgifter** Gränssnitten mellan leverantörer av identifieringsverktyg och leverantörer av tjänster för identifieringsförmedling ska ha tekniskt planerad beredskap att förmedla följande uppgifter: 1) information om huruvida 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,		MPS72 12.1 § motiveringar, s. 56: Beredskap att förmedla icke-obligatoriska attribut betyder att behandlingen av icke-obligatoriska attribut måste planeras i gränssnittet och identifieringssystemet så att leverantören av identifieringstjänster har en uppfattning om de tekniska åtgärder

			[…]		som är nödvändiga vid införandet. Icke-obligatoriska attribut behöver inte genomföras tekniskt i systemen. Vid teknisk konfigurering ska man dock beakta att icke-obligatoriska attribut i identifieringsmeddelanden inte ska störa identifieringstransaktioner även om man inte kommit överens om användningen av dem. I praktiken måste planen dokumenteras för tillsynsåtgärder.
23.	S, H	Leverantören av identifieringsverktyg tillhandahåller kravenliga uppgifter (attribut) vid identifiering av en **juridisk person**.	**M72B 12 Minimiuppsättning uppgifter som ska förmedlas i förtroendenätet** **12.1 Obligatoriska uppgifter** Följande uppgifter ska förmedlas via gränssnitten mellan leverantörer av identifieringsverktyg och leverantörer av tjänster för identifieringsförmedling: […] 2) vid identifiering av en juridisk person åtminstone den identifieringsuppgift som autentiserats av leverantören av identifieringsverktyget som identifierar den fysiska personen som företräder den juridiska personen, personens efternamn och förnamn samt den identifieringsuppgift som identifierar organisationen, 3) information om huruvida identifieringsverktyget ligger på tillitsnivån väsentlig eller hög, och […]		Endast om man börjar tillhandahålla stark autentisering av juridiska personer
24.	S, H	Leverantören av identifieringsverktyg har en erforderlig plane-	**M72B 12 Minimiuppsättning uppgifter som ska förmedlas i förtroendenätet** **12.2 Valfria uppgifter**		

		rad beredskap att förmedla optionella uppgifter vid identifiering av en **juridisk person**.	Gränssnitten mellan leverantörer av identifieringsverktyg och leverantörer av tjänster för identifieringsförmedling ska ha tekniskt planerad beredskap att förmedla följande uppgifter: 1) information om huruvida en identifieringstransaktion gäller en offentlig eller en privat tjänst för ärendehantering, 2) […] 3) vid identifiering av en juridisk person: a) nuvarande adress, b) momsregistreringsnummer, c) skatteregisteringsnummer, d) Den identifikator som avses i artikel 3.1 i Europaparlamentets och rådets direktiv 2009/101/EG, e) den identifieringskod för juridiska personer (LEI) som avses i kommissionens genomförandeförordning (EU) nr 1247/2012, f) det registrerings- och identitetsnummer för ekonomiska aktörer (EORI-nummer) som avses i kommissionens genomförandeförordning (EU) nr 1352/2013, och g) punktskattenummer som avses i artikel 2.12 i rådets förordning nr 389/2012.		

B 3 Tekniska krav på informationssäkerhet

CENTRALA BESTÄMMELSER

M72B 15 Bedömningskriterier för överensstämmelse
En bedömning enligt 29 § i autentiseringslagen måste omfatta alla de krav som ställs i lagen och i denna föreskrift som gäller
1) funktioner som påverkar tillhandahållandet av identifieringstjänsten (ett identifieringssystem)
d) tekniska åtgärder

Autentiseringslagen 8 § Krav på system för elektronisk identifiering

4) identifieringssystemet är säkert och tillförlitligt på ett sådant sätt att åtminstone de villkor uppfylls som gäller för tillitsnivån väsentlig enligt avsnitten ... 2.4.6 i bilagan till förordningen om tillitsnivåer vid elektronisk identifiering, med hänsyn till de informationssäkerhetsrisker som är förknippade med den teknik som används vid tidpunkten

LoA Bilaga 2.4.6 Tekniska kontroller (controls)
1) Proportionella tekniska kontroller ska finnas för att hantera riskerna för tjänsternas säkerhet, och för att skydda de behandlade uppgifternas sekretess, integritet och tillgänglighet.

M72B 5 Krav på informationssäkerhet i identifieringsmetoder
5.1 Identifieringssystemets skyddsförmåga
5.1.1
Identifieringssystemets datakommunikation och informationssystem samt användningen av dem ska planeras, förverkligas och kontinuerligt upprätthållas under hela deras livscykel så att identifieringstjänstens integritet och sekretess skyddas. Identifieringstjänsten ska ha skyddsförmåga åtminstone på tillitsnivån väsentlig eller hög mot hot och angreppspotential enligt punkt 2.3 i bilagan till förordningen om tillitsnivåer vid elektronisk identifiering, i enlighet med identifieringstjänstens tillitsnivå.

5.1.2
Krypteringskraven för datakommunikationsförbindelser mellan leverantörer av identifieringstjänster samt mellan identifieringstjänster och förlitande parter definieras i punkt 7. I identifieringssystemets övriga datakommunikationsförbindelser samt i krypteringen av informationssystem och information ska man till de delar det är tekniskt tillämpligt använda krypteringslösningar enligt punkt 7 i föreskriften, om inte skyddsförmågan bedömd som helhet förverkligas genom andra säkerhetsåtgärder.

5.2 Datakommunikationssäkerhet
I identifieringssystemets datakommunikation ska man planera, förverkliga och kontinuerligt upprätthålla
a) säkerhet i nätstrukturen,
b) indelning av datakommunikationsnätet i zoner,
c) filtreringsregler enligt principen om behovsenlig behörighet,
d) administration av filtrering och kontrollsystem,
e) säkra administrationsförbindelser, och
f) använda krypteringslösningar som rekommenderas internationellt eller nationellt.

5.3 Säkerhet i informationssystem
I identifieringssystemets informationssystem ska man planera, förverkliga och kontinuerligt upprätthålla
a) hantering av behörigheter enligt principen om behovsenlig behörighet,
b) individuell identifiering av systemanvändarna,
c) härdande av system,
d) ett skydd mot skadliga program,
e) förmågan och en process för att spåra säkerhetsrelaterade händelser,
f) förmågan att upptäcka avvikelser och en process för att åtgärda dem, och
g) använda krypteringslösningar som rekommenderas internationellt eller nationellt.

5.4 Säkerhet i användning
I driften av identifieringssystemet ska man planera, förverkliga och kontinuerligt upprätthålla
a) hantering av förändringar,
b) en behandlingsmiljö och förvaring för sekretessbelagt material som baserar sig på klassificeringen av informationen,
c) ett skydd av användning och administration på distans mot hot i distansanvändningsmiljön,
d) hantering av programutveckling och sårbarheter i programvara,
e) säkerhetskopiering, samt
f) använda krypteringslösningar som rekommenderas internationellt eller nationellt.

5.5 Administratörs- och distansförbindelser i identifieringssystemets produktionsnät
Ett produktionsnät och administrationsförbindelser samt distansanvändning och -administration enligt underpunkterna 5.2 e) och 5.4 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 bedömda som helhet på tillitsnivån hög.

B 3.1 Datakommunikationssäkerhet:

3.1 Datakommunikationssäkerhet					
NR	**TILL-LITS-NIVÅ**	**SAMMANDRAG ÖVER KRAVEN PÅ IDENTIFIERINGSTJÄNS-TEN**	**BESTÄMMELSER**	**STANDARD HÄNVIS-NING**	**OBSERVATIONER**
25.	S, H	Datakommunikationssäkerhet: **Datakommunikationsförbin-delser, administrationsförbin-delser, processer** för identifie-ringssystem (datakommunikation vid delprocesser för tillhandahål-lande, inklusive administration, av identifieringstjänster) och de-ras skyddspraxis har **identifie-rats, dokumenterats och ad-ministrerats**	**M72B 5.2 Datakommunikationssäkerhet** I identifieringssystemets datakommunikation ska man planera, förverkliga och kontinuerligt upp-rätthålla a) säkerhet i nätstrukturen, b) indelning av datakommunikationsnätet i zoner, c) filtreringsregler enligt principen om behov-senlig behörighet, d) administration av filtrering och kontrollsy-stem, e) säkra administrationsförbindelser, och f) använda krypteringslösningar som rekom-menderas internationellt eller nationellt.	A.8.1.1 Inven-tering av till-gångar A.13.1 Kom-munikations-säkerhet/Han-tering av nät-verkssäker-het:	Informationssäkerheten i datakommunikationen ska säkerställas i identifie-ringssystemets helhetsar-kitektur. Obs! Alla relevanta data-kommunikationsförbindel-ser till underleverantörer ska också säkerställas vid planeringen (inkl. infra-struktur, programvaror, drifttjänster, kortprodukt-ion osv.).

		Indelningen av ett identifieringssystems datakommunikationsförbindelser i zoner och filtreringsreglerna ska göras enligt principen om behovsenlig behörighet (least privilege) och principen om försvar på djupet (defence in depth).	**LoA Bilaga 2.4.6 Tekniska kontrolle**r (controls) 2. Elektroniska kommunikationskanaler som används för att utbyta personuppgifter eller känslig information skyddas mot avlyssning, manipulation och omspelning.	A.13.1.1 Säkerhetsåtgärder för nätverk A.13.1.3 Separation av nätverk	En beskrivning av arkitekturen ska bifogas anmälan/**inspektionsberättelsen**. Beskrivningen ska innehålla uppgifter om datakommunikationsförbindelserna mellan olika delar av identifieringssystemet och om deras skyddspraxis. Dokumentationen ska innehålla en tydlig beskrivning av nätområdena på olika skyddsnivåer och filtrerings- och övervakningssystemen mellan nätområdena.
26.	S, H	Datakommunikationssäkerhet: Identifieringssystemets **anordningar och system för datatrafik** har identifierats och dokumenterats.	**M72B 5.2 Datakommunikationssäkerhet** I identifieringssystemets datakommunikation ska man planera, förverkliga och kontinuerligt upprätthålla a) säkerhet i nätstrukturen	A.8.1.1 Inventering av tillgångar	
27.	S, H	Datakommunikationssäkerhet: **Produktionsnätet** ska vara **åtskilt** från underhålls- och hanteringsnätet. Underhålls- och hanteringsnätet ska vara åtskilt från det övriga kontorsnätet. En utvecklingsmiljö som har åtskilts från produktionen ska användas.	**M72B 5.2 Datakommunikationssäkerhet** I identifieringssystemets datakommunikation ska man planera, förverkliga och kontinuerligt upprätthålla a) säkerhet i nätstrukturen b) indelning av datakommunikationsnätet i zoner […] **5.5 Administratörs- och distansförbindelser i identifieringssystemets produktionsnät** Ett produktionsnät och administrationsförbindelser samt distansanvändning och -administration enligt underpunkterna 5.2 e) och 5.4 c) ovan ska genomföras så att informationssäkerhetshot som orsakas av organisationens övriga tjänster, som e-post eller webbsurfning, samt informationssäker-	A.12.1.4 Driftsäkerhet: Separation av utvecklings-, test- och driftmiljöer A.13.1.3 Separation av nätverk	Separationen kan göras logiskt eller fysiskt. Den nivå som krävs vid separation påverkas totalt sett av hur kritiskt ett nät är och vilka uppgifter som behandlas i nätet. Syftet med kravet är att minska de risker som via datakommunikationsförbindelser uppstår för sekretess, integritet och tillgänglighet i nät.

			hetshot 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) b) förhindrade som helhet på tillitsnivån hög.		
28.	S, H	Datakommunikationssäkerhet: Genom datakommunikationsförbindelser i identifieringssystem **säkerställs filtreringar** enligt principen om behovsenlig behörighet.	**M72B 5.2 Datakommunikationssäkerhet** I identifieringssystemets datakommunikation ska man planera, förverkliga och kontinuerligt upprätthålla […] c) filtreringsregler enligt principen om behovsenlig behörighet, d) administration av filtrering och kontrollsystem, […]	A.13.1.1–3 Kommunikationssäkerhet/Hantering av nätverkssäkerhet: A.13.1.1 Säkerhetsåtgärder för nätverk A.13.1.2 Säkerhet hos nätverkstjänster A.13.1.3 Separation av nätverk Se även åtkomsthantering	
29.	S, H	Datakommunikationssäkerhet: Produktionsnätets **förbindelser till det offentliga nätet** ska vara riskbaserade förbindelser som endast möjliggör tjänstens funktioner.	**M72B 5.2 Datakommunikationssäkerhet** I identifieringssystemets datakommunikation ska man planera, förverkliga och kontinuerligt upprätthålla a) säkerhet i nätstrukturen, b) […] c) filtreringsregler enligt principen om behovsenlig behörighet, d) administration av filtrering och kontrollsystem, e) säkra administrationsförbindelser, och f) […]	Se raden ovan	Alla andra förbindelser som inte är nödvändiga för verksamheten har uttryckligen förbjudits eller stängts.

			5.5 Administratörs- och distansförbindelser i identifieringssystemets produktionsnät Ett produktionsnät och administrationsförbindelser samt distansanvändning och -administration enligt underpunkterna 5.2 e) och 5.4 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) b) förhindrade som helhet på tillitsnivån hög.		
30.	S, H	Datakommunikationssäkerhet: Identifieringstjänsternas och de förlitande parternas **kryptografiska nyckelmaterial** eller **metadata** byts på ett säkert sätt.	**M72B 8 Verifiering av parterna i datakommunikationen** **8.1 Identifiering av parterna i en datakommunikationsförbindelse** När man upprättar en datakommunikationsförbindelse mellan identifieringstjänster eller mellan en identifieringstjänst och en förlitande part måste man autentisera äktheten och integriteten hos de certifikat som används för att kryptera datakommunikationen eller meddelandena samt deras innehavare. Autentiseringen ska basera sig på en kvalificerad elektronisk underskrift eller en kvalificerad elektronisk stämpel enligt eIDAS-förordningen eller direkt på ett bilateralt förfarande. Autentiseringen kan inte baseras endast på ett certifikat som det råder allmänt förtroende för. **8.2 Förnyande av certifikat och nycklar** De certifikat och nycklar som avses ovan i punkt 8.1 ska förnyas regelbundet. För att säkerställa äktheten och integriteten hos nya certifikat och nycklar ska förnyelsen göras antingen	A.10.1.2 Kryptering: Nyckelhantering	jfr jfr PSD2/RTS eIDAS art45 eller eSeal krav på certifikat för identifiering av part Mellan parterna har en process för att skapa ett säkert tillitsförhållande definierats och för att verifiera parterna och byta ut långvariga nycklar/hemligheter. Processer och rutiner för administration av krypteringsnycklar ska vara dokumenterade och på ett ändamålsenligt sätt införda. Processerna ska kräva åtminstone användning av kryptografiskt starka nycklar, säker utdelning av nycklar, säker förvaring av

			a) enligt det förfarande som beskrivs i punkt 8.1, b) genom att skicka de nya nycklarna via en datakommunikationsförbindelse vars integritet och sekretess har säkerställts genom att knyta parternas datakommunikation till certifikat eller nycklar som levererats enligt punkt 8.1, eller c) genom att underteckna den nya nyckeln med en nyckel som levererats enligt punkt 8.1 eller en sådan kedjad nyckel. **LoA Bilaga 2.4.6 Tekniska kontroller** 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. […] 5. Alla medel som innehåller personuppgifter eller kryptografiska eller andra känsliga uppgifter ska lagras, transporteras och bortskaffas på ett säkert sätt. **LoA Bilaga 2.4.6 Tekniska kontroller** Väsentlig: Känsligt krypteringstekniskt material, som används för att bevilja och autentisera metoder för elektronisk identifiering, är skyddade mot olovlig hantering. **LoA Bilaga 2.3.1 Autentiseringsmekanism** Väsentlig: 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		nycklar, regelbundet byte av nycklar, byte av gamla eller avslöjade nycklar och förhindrande av sådant nyckelbyte som saknar befogenheter. KATAKRI v.2015 (I12)

			som görs av en angripare med måttlig angrepps-potential (”moderate”) kan underminera autenti-seringsmekanismerna.		
31.	H	Datakommunikationssäkerhet: Identifieringstjänsternas och de förlitande parternas kryptogra-fiska nyckelmaterial eller meta-data byts på ett säkert sätt.	Jfr ovan samt **LoA Bilaga 2.3.1 Autentiserings-mekanism** Hög: Autentiseringsmekanismen genomför säker-hetskontroller för att verifiera medlet för elektro-nisk identifiering, varför det är högst osannolikt att exempelvis gissningar, tjuvlyssning, omspel-ning eller manipulation av kommunikation som görs av en angripare med stor angreppspotential (”high”) kan underminera autentiseringsmekan-ismerna.	A.10.1.2 Kryp-tering: Nyck-elhantering	
32.	S, H	Identifieringsmeddelandet mellan den som erbjuder identifierings-tjänsten (förmedlingstjänst eller förmedling av eget verktyg) och den förlitande parten ska verifie-ras,	**M72B 9.1.2** I datakommunikation mellan tjänsten för identifie-ringsförmedling och den förlitande part måste identifieringsmeddelanden autentiseras genom underskrift.		
33.	S, H	Man sörjer för integriteten och sekretessen hos identifierings-meddelandena.	**M72B 9.1.1** I datakommunikation mellan identifieringstjänster samt mellan en identifieringstjänst och en förli-tande part måste man trygga integriteten och sek-retessen hos identifieringsmeddelanden som inne-håller personuppgifter antingen a) genom att säkerställa datakommunikat-ionsförbindelsens integritet och sekretess genom att knyta parternas datakommuni-kation till certifikat eller nycklar som leve-rerats enligt punkt 8, eller b) genom att kryptera och underteckna med-delandena med nycklar som levererats en-ligt punkt 8. **LoA Bilaga 2.4.6 Tekniska kontroller** 1. Proportionella tekniska kontroller ska finnas för att hantera riskerna för tjänsternas säkerhet, och för att skydda de behandlade uppgifternas sekre-tess, integritet och tillgänglighet.		I punkt 8 beskrivs olika metoder med vilka ett till-räckligt datakommunikat-ionsskydd mellan parterna kan genomföras.

			2. Elektroniska kommunikationskanaler som används för att utbyta personuppgifter eller känslig information skyddas mot avlyssning, manipulation och omspelning.		
34.	S, H	Datakommunikationssäkerhet: Det gäller att säkerställa **administration av filtrering och kontrollsystem** i datakommunikationsförbindelser i identifieringssystem.	**M72B 5.2 Datakommunikationssäkerhet** I identifieringssystemets datakommunikation ska man planera, förverkliga och kontinuerligt upprätthålla […] d) administration av filtrering och kontrollsystem, e) säkra administrationsförbindelser, och […]	A.13.1 Kommunikationssäkerhet/Hantering av nätverkssäkerhet: A.13.1.1 Säkerhetsåtgärder för nätverk	
35.	S	Datakommunikationssystem/kontroll över datakommunikationen: Vid distansanvändning och distansadministration av ett identifieringssystem har informationssäkerhetshot som orsakas av e-post eller webbsurfning **bedömts och minimerats**. Detsamma gäller informationssäkerhetshot som har orsakats av en terminalenhet vid hantering av andra funktioner än de som är nödvändiga för hanteringen.	**M72B 5.2 Datakommunikationssäkerhet** I identifieringssystemets datakommunikation ska man planera, förverkliga och kontinuerligt upprätthålla […] d) administration av filtrering och kontrollsystem, e) säkra administrationsförbindelser, och […] **5.4 Säkerhet i användning** I driften av identifieringssystemet ska man planera, förverkliga och kontinuerligt upprätthålla […] c) ett skydd av användning och administration på distans mot hot i distansanvändningsmiljön, […] **5.5 Administratörs- och distansförbindelser i identifieringssystemets produktionsnät** Ett produktionsnät och administrationsförbindelser samt distansanvändning och -administration enligt underpunkterna 5.2 e) och 5.4 c) ovan ska ge-	A 6.2.2 Distansarbete A.9.4 Styrning av åtkomst till system och tillämpningar A.9.4.1 Begränsning av åtkomst till information A.9.4.4 Användning av privilegierade verktygsprogram A.13.1.3 Hantering av nätverkssäkerhet: Separation av nätverk	MPS72: Internet och kontorsnät anses vara nätverk som saknar förtroende, om inte kontorsnätet omfattas av bedömning av överensstämmelse. Överföringskanalen ska alltså vid fjärranvändning vara skyddad och de risker som kontorsnätet kan orsaka måste beaktas. Kraven på tillitsnivån väsentlig är normala och kan täckas genom att tillämpa kraven i t.ex. standarden ISO 27001.

			nomföras 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 […]		
36.	H	Datakommunikationssystem/kontroll över datakommunikationen: Vid distansanvändning och distansadministration av ett identifieringssystem (ett produktionsnät) har informationssäkerhetshot som orsakas av e-post eller webbsurfning **förhindrats**. Detsamma gäller informationssäkerhetshot som har orsakats av en terminalenhet vid hantering av andra funktioner än de som är nödvändiga för hanteringen.	**M72B 5.2 Datakommunikationssäkerhet** I identifieringssystemets datakommunikation ska man planera, förverkliga och kontinuerligt upprätthålla […] d) administration av filtrering och kontrollsystem, e) säkra administrationsförbindelser, och […] **5.4 Säkerhet i användning** I driften av identifieringssystemet ska man planera, förverkliga och kontinuerligt upprätthålla […] c) ett skydd av användning och administration på distans mot hot i distansanvändningsmiljön, […] **5.5 Administratörs- och distansförbindelser i identifieringssystemets produktionsnät** Ett produktionsnät och administrationsförbindelser samt distansanvändning och -administration enligt underpunkterna 5.2 e) och 5.4 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: […]	Se raden ovan	

			b) förhindrade bedömda som helhet på tillitsnivån hög. **MPS72B Tillämpningsguide:** På tillitsnivån hög kan kraven genomföras åtminstone så att arbetsstationer som är i fjärranvändning nekas åtkomst till organisationens övriga tjänster, såsom e-post, och att möjligheten att använda andra funktioner än de som är nödvändiga för användning av administrationsnätet tas bort från arbetsstationen. I praktiken betyder detta alltså att det behövs en separat arbetsstation för administration. Helhetsbedömningen på tillitsnivån hög betyder att om man använder en annan än en sådan härdad arbetsstation som beskrivs ovan, ska man i genomförandet beakta separering av produktionssystemet och övriga arrangemang med vilka informationssäkerhetshot kan hanteras. I princip förutsätter det en virtuell terminering eller en lösning som baserar sig på kvm-principen (keyboard, video, mouse; fjärrskrivbord). Det väsentliga är vad man gör med den terminalenheten som tar virtuell kontakt och därför är t.ex. en two-factor VPN-förbindelse till ett virtuellt skrivbord inte ensam en lösning. Det är inte heller tillräckligt att man använder antivirusprogram och webbproxy. Vid överföring av nödvändiga filer från en terminalenhet till en annan ska man också ta hänsyn till risk för skadliga program bl.a. genom att endast använda tillförlitliga källor och säkerställa informationssäkerheten (integriteten) med alla nödvändiga metoder.		

B 3.2 Säkerhet i informationssystem:

3.2 Säkerhet i informationssystem

NR	TILL-LITS-NIVÅ	SAMMANDRAG ÖVER KRAVEN PÅ IDENTIFIERINGSTJÄNS-TEN	BESTÄMMELSER	STANDARD HÄNVIS-NING	OBSERVATIONER
37.	S, H	Säkerhet i informationssystem: Informationssystemen och **pro-cesserna i ett identifierings-system** (de processer som an-vänder informationssystem vid tillhandahållande och admini-stration av identifieringstjänster) **har identifierats, dokumente-rats och administrerats.** Informationssystemen i ett iden-tifieringssystem har **klassifice-rats** med beaktande av den in-formation som behandlas i syste-men och de funktioner som sy-stemen möjliggör. I klassifice-ringen av system ska man be-akta hela livscykeln för den in-formation som skyddas. Den databehandlingsmiljö som används vid hanteringen har skilts åt från andra miljöer.	**M72B 5.3 Säkerhet i informationssystem** I identifieringssystemets informationssystem ska man planera, förverkliga och kontinuerligt upprätt-hålla a) hantering av behörigheter enligt principen om behovsenlig behörighet, b) individuell identifiering av systemanvän-darna, […]	A.8.1.1 Hante-ring av till-gångar, An-svar för till-gångar: In-ventering av tillgångar A.8.2.1 Hante-ring av till-gångar: Klass-ning av in-formation	Klassning: bl.a. en god-känd användning av ut-rustning, program och öv-rig egendom ska vara fast-ställd.
38.	S, H	Säkerhet i informationssystem: **Åtkomsträttigheterna** till ett identifieringssystem har definie-rats och dokumenterats. Åtkomsträttigheterna **bygger på** en klassificering av informations-system och enskilda perso-ners/användares arbetsuppgifter.	**M72B 5.3 Säkerhet i informationssystem** I identifieringssystemets informationssystem ska man planera, förverkliga och kontinuerligt upp-rätthålla a) hantering av behörigheter enligt principen om behovsenlig behörighet, b) individuell identifiering av systemanvän-darna, c) härdande av system, […]	A.9.1.1 Verk-samhetskrav för styrning av åtkomst: Reg-ler för styr-ning av åt-komst A.9.1.2 Till-gång till nät-verk och nät-verkstjänster	Åtkomsten till information och databehandlingsmil-jöer ska begränsas på ett systematiskt och doku-menterat sätt genom ad-ministration av åtkomst-rättigheter.

		Åtkomst ska endast beviljas utifrån arbetsuppgifter (principen om behovsenlig behörighet).		A.9.4.1 Styrning av åtkomst till system och tillämpningar: Begränsning av åtkomst till information	
39.	S, H	Säkerhet i informationssystem: **Användare** av informationssystem för ett identifieringssystem **identifieras** med en känd teknik/metod som anses vara säker.	**M72B 5.3 Säkerhet i informationssystem** I identifieringssystemets informationssystem ska man planera, förverkliga och kontinuerligt upprätthålla a) hantering av behörigheter enligt principen om behovsenlig behörighet, b) individuell identifiering av systemanvändarna, c) härdande av system, d) […] e) förmågan och en process för att spåra säkerhetsrelaterade händelser, f) […]	A.9.4.2 styrning av åtkomst till system och tillämpningar: Säkra inloggningsrutiner	T.ex. certifikat, 2FA i regel något annat än ett lösenord, men om lösenord ingår behövs det tillräckligt långa och individuella lösenord och användarnamn (ej gemensamma)
40.	S, H	Säkerhet i informationssystem: Åtkomsträttigheter övervakas och **hålls uppdaterade**.	**M72B 5.3 Säkerhet i informationssystem** I identifieringssystemets informationssystem ska man planera, förverkliga och kontinuerligt upprätthålla a) hantering av behörigheter enligt principen om behovsenlig behörighet, b) individuell identifiering av systemanvändarna, c) härdande av system, d) […] e) förmågan och en process för att spåra säkerhetsrelaterade händelser, f) förmågan att upptäcka avvikelser och en process för att åtgärda dem, och g) […]	A.9.2 Hantering av användaråtkomst A.9.2.1 Registrering och avregistrering av användare A.9.2.3 Hantering av privilegierade åtkomsträttigheter A.9.2.5 Granskning av användares	

				åtkomsträttig-heter A.9.2.6 Bort-tagning eller justering av åtkomsträttig-heter	
41.	S, H	Säkerhet i informationssystem: De anställdas **arbetsuppgifter och aktiviteter ska fastställas** så att en person inte genom sin verksamhet oavsiktligen eller av-siktligen kan orsaka allvarliga sä-kerhetsavvikelser (farliga arbets-kombinationer).	**M72B 5.3 Säkerhet i informationssystem** I identifieringssystemets informationssystem ska man planera, förverkliga och kontinuerligt upp-rätthålla a) hantering av behörigheter enligt principen om behovsenlig behörighet, b) individuell identifiering av systemanvän-darna, c) härdande av system, d) […] e) förmågan och en process för att spåra sä-kerhetsrelaterade händelser, f) förmågan att upptäcka avvikelser och en process för att åtgärda dem, och g) […]	A.6.1.2 Upp-delning av ar-betsuppgifter	Ett exempel är att risken för att oärliga eller oakt-samma anställda beviljar identifieringsmetoder i strid med de uppställda kraven kan förebyggas ge-nom fastställda arbetsupp-gifter eller kontroller som minskar risken för misstag och missbruk. Vid bedömningen ska hän-syn, i enlighet med tillits-nivån för identifieringsme-toden, tas till en måttlig eller hög angreppspot-ential på samma sätt som i övriga punkter.
42.	S, H	Säkerhet i informationssystem: **Härdande** av identifieringssy-stem ska säkerställas: ett förfa-ringssätt, på vilket system instal-leras systematiskt så att resulta-tet är en härdad installation, ska användas. I identifieringssystem används **endast** tjänster, funktioner, pro-cesser, utrustning och kompo-nenter som är **nödvändiga** för	**M72B 5.3 Säkerhet i informationssystem** I identifieringssystemets informationssystem ska man planera, förverkliga och kontinuerligt upp-rätthålla […] c) härdande av system, […]	A.12.5 Styr-ning av drift-system	Se även datakommunikat-ion Anvisningen 211/2016 in-nehöll följande kriterier som ingår som informativa kriterier i denna anvisning: En härdad installation in-nehåller endast sådana komponenter och tjänster samt användar- och pro-cessrättigheter som är nödvändiga för att uppfylla

		systemets funktion. Användningen av dessa har specificerats så att alla onödiga behörigheter och funktioner/element har tagits bort från installationen.			funktionskraven och säkerställa säkerheten. Endast sådana funktioner, utrustningar och tjänster som är relevanta med tanke på användningskraven och databehandlingen har tagits i bruk.
43.	S, H	Säkerhet i informationssystem: I identifieringssystem säkerställs det att skador och hot som orsakas av **skadliga program** observeras, förebyggs, förhindras och åtgärdas.	**M72B 5.3 Säkerhet i informationssystem** I identifieringssystemets informationssystem ska man planera, förverkliga och kontinuerligt upprätthålla […] d) ett skydd mot skadliga program, e) förmågan och en process för att spåra säkerhetsrelaterade händelser, f) förmågan att upptäcka avvikelser och en process för att åtgärda dem, och […]	A.12.2 Skydd mot skadlig kod A.12.6 Hantering av tekniska sårbarheter	Se även förmåga att observera avvikelser
44.	S, H	Säkerhet i informationssystem: I alla delar av ett identifieringssystem används **krypteringslösningar** som rekommenderas.	**M72B 5.3 Säkerhet i informationssystem** I identifieringssystemets informationssystem ska man planera, förverkliga och kontinuerligt upprätthålla […] g) använda krypteringslösningar som rekommenderas internationellt eller nationellt.	A.10.1 Regler för användning av kryptografiska säkerhetsåtgärder A.18.1.5 Reglering av kryptografiska säkerhetsåtgärder	I MPS72 nämns följande som källor: - SOGIS-MRA - NCSA-FI - NIST - Enisa - SANS Anvisning 211/2016 innefattade följande observationer som ingår som informativa observationer i denna anvisning: Processerna ska kräva åtminstone användning av kryptografiskt starka nycklar, säker utdelning av nycklar, säker förvaring av nycklar, regelbundet byte av nycklar, byte av gamla

					eller avslöjade nycklar och förhindrande av sådant nyckelbyte som saknar befogenheter. KATAKRI v.2015 (I12)
45.	S, H	Säkerhet i informationssystem: Kryptografiskt material är skyddat under materialets hela livscykel.	**LoA Bilaga 2.4.6 Tekniska kontroller** 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. Väsentlig: Känsligt krypteringstekniskt material, som används för att bevilja och autentisera metoder för elektronisk identifiering, är skyddade mot olovlig hantering. **M72B 5.3 Säkerhet i informationssystem** I identifieringssystemets informationssystem ska man planera, förverkliga och kontinuerligt upprätthålla a) hantering av behörigheter enligt principen om behovsenlig behörighet, b) individuell identifiering av systemanvändarna, c) härdande av system, […] g) använda krypteringslösningar som rekommenderas internationellt eller nationellt. **M72B 5.4 Säkerhet i användning** I driften av identifieringssystemet ska man planera, förverkliga och kontinuerligt upprätthålla […] b) en behandlingsmiljö och förvaring för sekretessbelagt material som baserar sig på klassificeringen av informationen, […]	A.8.2.1 Klassning av information A.10.1.1 Regler för användning av kryptografiska säkerhetsåtgärder A.10.1.2 Nyckelhantering	Anvisning 211/2016 innefattade följande observationer som ingår som informativa observationer i denna anvisning: Hemliga nycklar används endast av användare och processer med befogenheter. Processer och rutiner för administration av krypteringsnycklar ska vara dokumenterade och på ett ändamålsenligt sätt införda. Processerna ska kräva åtminstone användning av kryptografiskt starka nycklar, säker utdelning av nycklar, säker förvaring av nycklar, regelbundet byte av nycklar, byte av gamla eller avslöjade nycklar och förhindrande av sådant nyckelbyte som saknar befogenheter. KATAKRI v.2015 (I12)

			f) använda krypteringslösningar som rekommenderas internationellt eller nationellt.		

B 3.3 Säkerhet i användning

3.3 Säkerhet i användning					
NR	**TILL-LITS-NIVÅ**	**SAMMANDRAG ÖVER KRAVEN PÅ IDENTIFIERINGSTJÄNSTEN**	**BESTÄMMELSER**	**STANDARD HÄNVISNING**	**OBSERVATIONER**
46.	S, H	Säkerhet i användning: **Hanteringen av förändringar** i ett identifieringssystem är planerad och omsorgsfull.	**M72B 5.4 Säkerhet i användning** I driften av identifieringssystemet ska man planera, förverkliga och kontinuerligt upprätthålla a) hantering av förändringar, […]	A.12.1.2 Driftsäkerhet/Driftsrutiner och ansvar: Ändringshantering A.14.2.2 Anskaffning, utveckling och underhåll av system/Säkerhet i utvecklings- och supportprocesser: Rutiner för hantering av systemändringar A.14.2.3 Teknisk granskning av tillämpningar efter ändringar i driftsmiljö A.14.2.4 Restriktioner för ändringar av programpaket	Tydliga processer ska vara fastställda för hantering av förändringar. I testplanen för genomförandet av nya egenskaper eller ändringar ha även negativa testfall beaktats. Testningen baserar sig inte enbart på automatiska tester.

47.	S, H	Säkerhet i användning: Hanteringen av **programsårbarheter** i identifieringssystem är systematisk. I identifieringssystem säkerställs det att skador och hot som orsakas av **programsårbarheter** observeras, förebyggs, förhindras och åtgärdas.	**M72B 5.4 Säkerhet i användning** I driften av identifieringssystemet ska man planera, förverkliga och kontinuerligt upprätthålla […] d) hantering av programutveckling och sårbarheter i programvara, […]	A.12.5.1 Driftsäkerhet: Installation av program på driftsystem A.12.6.1 Driftsäkerhet: Hantering av tekniska sårbarheter A.14.2 Anskaffning, utveckling och underhåll av system/Säkerhet i utvecklings- och supportprocesser A.14.2.1 Regler för säker utveckling A.14.2.2 Rutiner för hantering av systemändringar A.14.2.3 Teknisk granskning av tilllämpningar efter ändringar i driftsmiljö A.14.2.4 Restriktioner för ändringar av programpaket A.14.2.5 Principer för utveckling av säkra system	Organisationen ska upprätthålla en databas eller en lista med alla identifieringssystemets olika programkomponenter. Organisationen ska ha en metod för att följa upp allmänna sårbarheter. Sårbara programkomponenter ska uppdateras till uppdaterade versioner. Program som används i identifieringssystem ska vara förenliga med principerna för säker programmering. Identifieringssystemets nya versioner ska testas även så att testfallen innehåller negativa testfall.

				A.14.2.6 Säker utvecklingsmiljö A.14.2.7 Outsourcad utveckling A.14.2.8 Säkerhetstestning A.14.2.9 Acceptanstestning av system	
48.	S, H	Säkerhet i användning: I driften av identifieringssystemet ska man planera, förverkliga och kontinuerligt upprätthålla: Hantering av programvaruutveckling	**M72B 5.4 Säkerhet i användning** I driften av identifieringssystemet ska man planera, förverkliga och kontinuerligt upprätthålla a) hantering av förändringar, […]; d) hantering av programutveckling och sårbarheter i programvara, […]	Se föregående	I hanteringen av programvaruutveckling ska man särskilt beakta leveranskedjans struktur och upprätthålla information om programvarans olika komponenter och följa upp deras uppdateringar. Säker programvaruutveckling Testning
49.	S, H	Säkerhet i användning: **Säkerhetskopieringen** i identifieringssystem görs systematiskt. Vid säkerhetskopiering tas hänsyn till klassificering av information (personuppgifter, kryptografisk information osv.), återställande av system och lagring av säkerhetskopior.	**M72B 5.4 Säkerhet i användning** I driften av identifieringssystemet ska man planera, förverkliga och kontinuerligt upprätthålla […] e) säkerhetskopiering, samt […]	A.12.3.1 Säkerhetskopiering av information	Anvisning 211/2016 innefattade följande observationer som ingår som informativa observationer i denna anvisning: Det fysiska stället för säkerhetskopior ska vara tillräckligt åtskilt från det egentliga systemet.

B 4 Förmåga att observera avvikelser, hantering av avvikelser och störningsanmälningar

CENTRALA BESTÄMMELSER

M72B 15 Bedömningskriterier för överensstämmelse
En bedömning enligt 29 § i autentiseringslagen måste omfatta alla de krav som ställs i lagen och i denna föreskrift som gäller
1) funktioner som påverkar tillhandahållandet av identifieringstjänsten (ett identifieringssystem)
d) tekniska åtgärder

Allmänna krav

Autentiseringslagen 8 § Krav på system för elektronisk identifiering
4) identifieringssystemet är säkert och tillförlitligt på ett sådant sätt att åtminstone de villkor uppfylls som gäller för tillitsnivån väsentlig enligt avsnitten ... 2.4.6 i bilagan till förordningen om tillitsnivåer vid elektronisk identifiering, med hänsyn till de informationssäkerhetsrisker som är förknippade med den teknik som används vid tidpunkten

LoA Bilaga 2.4.6 Tekniska kontroller (controls)
1. Proportionella tekniska kontroller ska finnas för att hantera riskerna för tjänsternas säkerhet, och för att skydda de behandlade uppgifternas sekretess, integritet och tillgänglighet.
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.

Autentiseringslagen 16 § Skyldighet för leverantörer av identifieringstjänster att anmäla 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 en anmälan enligt 1 mom. ska det redogöras för de åtgärder som olika aktörer har tillgång till för att avvärja hot eller störningar samt de beräknade kostnaderna för åtgärderna.
[…]

Kraven har specificerats i punkt 5 och 11 i M72B

NR	TILL-LITS-NIVÅ	SAMMANDRAG ÖVER KRAVEN PÅ IDENTIFIERINGSTJÄNS-TEN	BESTÄMMELSER	STANDARD HÄNVIS-NING	OBSERVATIONER

50.	S, H	Det finns **processer som har specificerats i förväg** och **förmåga** att observera avvikelser i identifieringssystemet. I specifikationerna tas hänsyn till hur viktiga/kritiska systemets datakommunikationsförbindelser och informationssystemens komponenter och processer är och till klassificeringen av dem samt till att incidenter som knyter till/påverkar säkerheten kan spåras även i efterhand. I identifieringssystem insamlas och lagras **loggdata** om systemets funktion samt om incidenter och avvikelser som påverkar/knyter till informationssäkerheten.	**M72B 5.2 Datakommunikationssäkerhet** I identifieringssystemets datakommunikation ska man planera, förverkliga och kontinuerligt upprätthålla […] d) administration av filtrering och kontrollsystem, […] **M72B 5.3 Säkerhet i informationssystem** I identifieringssystemets informationssystem ska man planera, förverkliga och kontinuerligt upprätthålla a) hantering av behörigheter enligt principen om behovsenlig behörighet, b) individuell identifiering av systemanvändarna, […] e) förmågan och en process för att spåra säkerhetsrelaterade händelser, f) förmågan att upptäcka avvikelser och en process för att åtgärda dem, och […]	A.12.4.1 Driftsäkerhet: Loggning av händelser A.12.4.2 Driftsäkerhet: Skydd av logginformation A.12.4.3 Driftsäkerhet: Administratörs- och operatörsloggar A.16.1 Hantering av informationssäkerhetsincidenter/Hantering av informationssäkerhetsincidenter och förbättringar A. 16.1.1 Ansvar och rutiner A.16.1.6 Att lära av informationssäkerhetsincidenter	Processerna inkluderar både automatiska och manuella metoder. Processerna är administrerade.
51.	S, H	**Loggdata om hantering** av identifieringssystem har specificerats och skilts åt från övriga loggdata. Deras integritet har säkerställts.	**M72B 5.2 Datakommunikationssäkerhet** I identifieringssystemets datakommunikation ska man planera, förverkliga och kontinuerligt upprätthålla […] d) administration av filtrering och kontrollsystem, e) säkra administrationsförbindelser, och	A.12.4.1 Driftsäkerhet: Loggning av händelser A.12.4.2 Driftsäkerhet: Skydd av	i loggdata lagras information om ändringar i identifieringssystemet

			[…] **M72B 5.3 Säkerhet i informationssystem** I identifieringssystemets informationssystem ska man planera, förverkliga och kontinuerligt upprätthålla a) hantering av behörigheter enligt principen om behovsenlig behörighet, b) individuell identifiering av systemanvändarna, […] e) förmågan och en process för att spåra säkerhetsrelaterade händelser, f) förmågan att upptäcka avvikelser och en process för att åtgärda dem, och […]	logginformation A12.1.4 Separation av utvecklings-, test- och driftmiljöer	
52.	S, H	Funktion, ändringar och loggdata om identifieringssystem **övervakas** för att observera avvikelser och säkerhetsöverträdelser. **Avvikelser och störningar** i identifieringssystem **behandlas och analyseras** och deras inverkan/allvarlighetsgrad klassificeras systematiskt.	**M72B 5.2 Datakommunikationssäkerhet** I identifieringssystemets datakommunikation ska man planera, förverkliga och kontinuerligt upprätthålla […] d) administration av filtrering och kontrollsystem, […] **M72B 5.3 Säkerhet i informationssystem** I identifieringssystemets informationssystem ska man planera, förverkliga och kontinuerligt upprätthålla […] e) förmågan och en process för att spåra säkerhetsrelaterade händelser, f) förmågan att upptäcka avvikelser och en process för att åtgärda dem, och […]	A.16.1 Hantering av informationssäkerhetsincidenter/Hantering av informationssäkerhetsincidenter och förbättringar: A.16.1.2 Rapportering av informationssäkerhetshändelser A.16.1.3 Rapportering av svagheter gällande informationssäkerhet A.16.1.4 Bedömning av och beslut om	Alla observationer ska behandlas och deras inverkan klassificeras enligt överenskomna metoder. Loggarna analyseras med automatiska processer/verktyg såsom SIEM.

				informations-säkerhetshän-delser	
53.		**Korrigeringsåtgärder** som avvikelser och störningar i identifieringssystem kräver är systematiska och effektiva. Planerna för verksamhetens kontinuitet innehåller förebyggande och korrigerande åtgärder för att minimera de effekter som betydande störningar i verksamheten eller exceptionella incidenter har.	**M72B 5.2 Datakommunikationssäkerhet** I identifieringssystemets datakommunikation ska man planera, förverkliga och kontinuerligt upprätthålla […] d) administration av filtrering och kontrollsystem, […] **M72B 5.3 Säkerhet i informationssystem** I identifieringssystemets informationssystem ska man planera, förverkliga och kontinuerligt upprätthålla […] e) förmågan och en process för att spåra säkerhetsrelaterade händelser, f) förmågan att upptäcka avvikelser och en process för att åtgärda dem, och […]	A.16.1 Hantering av informationssäkerhetsincidenter/Hantering av informationssäkerhetsincidenter och förbättringar: A.16.1.5 Hantering av informationssäkerhetsincidenter 7.5. Dokumenterad data 10.1 Avvikelser och åtgärder som korrigerar avvikelserna	Korrigerande åtgärder ska dokumenteras. Kraven på tillgänglighet (SLA) är en avtalsfråga, hänsyn ska tas till icke-diskriminering
54.	S, H	I processer för incidenthantering har hänsyn tagits till **skyldigheten att göra anmälan till andra leverantörer av identifieringstjänster som hör till förtroendenätet.**	**Autentiseringslagen 16 § Skyldighet för leverantörer av identifieringstjänster att anmäla 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 […] övriga avtalsparter i förtroendenätet. […]	A.16.1.2 Hantering av informationssäkerhetsincidenter/Hantering av informationssäkerhetsincidenter och förbättringar: Rapportering	Ansvaret för undantagssituationer och kommunikation med intressenter har fastställts.

			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. **Tillämpning:** Samarbetsgruppen för förtroendenätet har tagit fram gemensamma rutiner för ömsesidiga störningsanmälningar och anmälningströsklar.	av informationssäkerhetshändelser	
55.	S, H	I processer för incidenthantering har hänsyn tagits till **skyldigheten att göra anmälan till användare och förlitande parter.**	**Autentiseringslagen 16 § Skyldighet för leverantörer av identifieringstjänster att anmäla hot och störningar som riktas mot verksamheten eller skyddet av uppgifter** En leverantör av identifieringstjänster ska [...] utan ogrundat dröjsmål anmäla betydande hot och störningar som riktas mot tjänsternas funktion, informationssäkerheten eller användningen av en elektronisk identitet till de parter som förlitar sig på tjänsterna, till innehavarna av identifieringsverktyg, [...]. 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.	A.16.1.2 Hantering av informationssäkerhetsincidenter/Hantering av informationssäkerhetsincidenter och förbättringar: Rapportering av informationssäkerhetshändelser	Ansvaret för undantagssituationer och kommunikation med intressenter har fastställts. Med förlitande parter avses tjänster för ärendehantering.
56.	S, H	I processer för incidenthantering har hänsyn tagits till **skyldigheten att göra anmälan till Transport- och kommunikationsverket**.	**Autentiseringslagen 16 § Skyldighet för leverantörer av identifieringstjänster att anmäla 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 Transport- och kommunikationsverket. I anmälan ska det redogöras för de åtgärder som	A.6.1.3 Kontakt med myndigheter A.16.1.2 Hantering av informationssäkerhetsincidenter/Hantering av informationssä-	Det dokument som tillitsnätverket tillsammans definierats följs vad gäller överskridandet av anmälningströskeln. Ansvaret för undantagssituationer och kommunikation med intressenter har fastställts.

			olika aktörer har tillgång till för att avvärja hot eller störningar samt de beräknade kostnaderna för åtgärderna. **M72B 11 Anmälningar om störningar från leverantören av identifieringstjänsten till Transport- och kommunikationsverket.** **11.1 Betydande hot eller störningar** Till de betydande störningar i identifieringstjänster som ska anmälas till Transport- och kommunikationsverket enligt 16 § i autentiseringslagen hör händelser som anknyter till felaktigheter i eller missbruk av en elektronisk identitet eller ett hot mot eller en störning i informationssäkerheten, som äventyrar identifieringens integritet och tillförlitlighet. Även oförutsedda funktionsstörningar som har större än ringa negativa effekter för förtroendenätet räknas som betydande. **11.2 Uppgifter som ska anmälas** I en anmälan till Transport- och kommunikationsverket om ett betydande hot eller en betydande störning ska åtminstone följande uppgifter ingå: 1) identifieringsverktyget eller tjänsten för identifieringsförmedling som störningen eller hotet påverkar, 2) en beskrivning av störningen eller hotet och dess kända orsaker samt varaktighet, 3) en beskrivning av störningens eller hotets konsekvenser, inklusive konsekvenser för beviljandet av nya identifieringsverktyg samt för användare, förlitande parter, andra aktörer i förtroendenätet och gränsöverskridande användning, 4) en beskrivning av korrigerande åtgärder, och 5) en beskrivning av informationen om störningen eller hotet till förlitande parter, innehavare av identifieringsverktyg och förtroendenätet samt uppgift om anmälan till andra myndigheter.	kerhetsincidenter och förbättringar: Rapportering av informationssäkerhetshändelser	

			11.3 Anmälningsförfarande Anmälningar om betydande störningar eller hot ska göras elektroniskt via Transport- och kommunikationsverkets webbformulär, e-post eller säker e-post. Uppgifterna i anmälan kan kompletteras senare, om alla uppgifter inte är tillgängliga när man gör en första anmälan enligt 16 § i autentiseringslagen utan oskäligt dröjsmål. **Tillämpningsanvisning i MPS72 om tröskeln för att göra anmälan till Transport- och kommunikationsverket**, stycke 4.1.1., avsnitt 11.1: Avsnitt 11.1 i föreskriften innehåller allmänna bestämmelser om de faktorer som är relevanta med tanke på hur betydande en störning eller ett hot är, det vill säga anmälningströskeln. Sådana betydande störningar är bland annat - när ett identifieringsverktyg beviljas till fel person - sådana störningar i spärrlistors funktion, där en uppdaterad spärrlista inte är tillgänglig - intrång i en tjänsteleverantörs system - avslöjande av signeringsnycklar för certifikat hos en leverantör av identifieringsverktyg - allvarliga missbruk av identifieringsverktyg, till exempel fall i anslutning till sammankoppling av identifieringsverktyg - allvarliga interna missbruk. Tröskeln för när fel i eller missbruk av en elektronisk identitet anses vara betydande är mycket låg, och detsamma gäller exempelvis sårbarheter och fel som äventyrar riktigheten i identifieringsuppgiften. Däremot är tröskeln för att anmäla problem i tillgängligheten eller kvaliteten i princip högre och sådana problem är än mer betydande främst på grund av att problemet påverkar andra aktörer i förtroendenätet. Den här typen av problem är sådana långvariga störningssituationer i		

			ett identifieringsverktyg eller en identifieringsförmedlingstjänst som förhindrar förmedling av identifieringstjänster till ärendehanteringstjänster. Även en störning som under en längre tid förhindrar sammankoppling av inledande identifieringar är betydande.		

B 5 Lagring och behandling av uppgifter

CENTRALA BESTÄMMELSER

M72B 15 Bedömningskriterier för överensstämmelse
En bedömning enligt 29 § i autentiseringslagen måste omfatta alla de krav som ställs i lagen och i denna föreskrift som gäller
1) funktioner som påverkar tillhandahållandet av identifieringstjänsten (ett identifieringssystem)
b) förvaringen och behandlingen av uppgifter
d) tekniska åtgärder

Allmänna krav

Autentiseringslagen 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.
[…]
Leverantören av identifieringstjänster ska dessutom ansvara för skyddet av uppgifterna enligt 32 § i personuppgiftslagen och för en tillräcklig informationssäkerhet i fråga om sina tjänster.

LoA Bilaga, 2.4.4 Registerföring
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.

Autentiseringslagen 8 § Krav på system för elektronisk identifiering
4) identifieringssystemet är säkert och tillförlitligt på ett sådant sätt att åtminstone de villkor uppfylls som gäller för tillitsnivån väsentlig enligt avsnitten [...] 2.4.6 i bilagan till förordningen om tillitsnivåer vid elektronisk identifiering, med hänsyn till de informationssäkerhetsrisker som är förknippade med den teknik som används vid tidpunkten

LoA Bilaga 2.4.6 Tekniska kontroller (controls)

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

Väsentlig: Känsligt krypteringstekniskt material, som används för att bevilja och autentisera metoder för elektronisk identifiering, är skyddade mot olovlig hantering.

NR	TILL-LITS-NIVÅ	SAMMANDRAG ÖVER KRAVEN PÅ IDENTIFIERINGSTJÄNS-TEN	BESTÄMMELSER	STANDARD HÄNVIS-NING	OBSERVATIONER
57.	S, H	**Hanteringen av information** avseende identifieringssystem och identifiering **är systematisk** och bygger på en **klassificering av information**.	**LoA Bilaga, 2.4.4 Registerföring** 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. **LoA Bilaga 2.4.6 Tekniska kontroller (controls)** 1. Proportionella tekniska kontroller ska finnas för att hantera riskerna för tjänsternas säkerhet, och för att skydda de behandlade uppgifternas sekretess, integritet och tillgänglighet. Väsentlig: Känsligt krypteringstekniskt material, som används för att bevilja och autentisera metoder för elektronisk identifiering, är skyddade mot olovlig hantering. **M72B 5.4 Säkerhet i användning** I driften av identifieringssystemet ska man planera, förverkliga och kontinuerligt upprätthålla […] 2. en behandlingsmiljö och förvaring för sekretessbelagt material som baserar sig på klassificeringen av informationen, […]	A.8.2.1 Hantering av tillgångar/Informationsklassning: Klassning av information A.18.1.4 Efterlevnad/Efterlevnad av juridiska och avtalsmässiga krav: Skydd av personlig integritet och personuppgifter	I klassificeringen beaktas bland annat kryptografisk information, information om identifieringstransaktioner, personuppgifter, affärshemligheter och information som påverkar säkerheten i systemen.
58.	S, H	Planeringen av informationshanteringen har beaktat informationens hela **livscykel**.	**LoA Bilaga, 2.4.4 Registerföring** 2. Lagra – i den mån det är tillåtet enligt nationell lag eller andra nationella administrativa bestämmelser – och skydda register så länge som de be-	A.8.1.1 Inventering av tillgångar	Hänsyn ska tas bland annat till spårning av säkerhetsincidenter och till behov föranledda av behand-

		Den **period** under vilken uppgifter lagras har fastställts.	hövs för granskning och undersökning av säkerhetsöverträdelser och för lagring, varefter registren ska förstöras på ett säkert sätt. **M72B 5.4 Säkerhet i användning** I driften av identifieringssystemet ska man planera, förverkliga och kontinuerligt upprätthålla […] b) en behandlingsmiljö och förvaring för sekretessbelagt material som baserar sig på klassificeringen av informationen, […]	A.18.1.4 Efterlevnad/Efterlevnad av juridiska och avtalsmässiga krav: Skydd av personlig integritet och personuppgifter	lingsgrunder som *motsvarar* grunder enligt 24 § i autentiseringslagen. Som detaljanvändningen av attributet ftn_chain_level i samband med inledande identifiering. Anvisning 211/2016 innefattade följande observationer som ingår som informativa observationer i denna anvisning: Med tanke på utredning i efterhand ska en tillräckligt lång tid fastställas för lagring av loggdata.
59.	S, H	**De särskilda lagringsskyldigheter som föreskrivs i 24 §** i autentiseringslagen har uppfyllts.	**Autentiseringslagen 24 § 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 certifikatet 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.	A.12.4.1 Driftsäkerhet: Loggning av händelser	*”...endast ger ut identifieringsverktyg”* betyder i bestämmelsen identifieringstjänster som liknar MDB:s certifikat och där den som beviljar identifieringsverktyget inte förmedlar identifieringsmeddelanden i identifieringstransaktioner

			De uppgifter som avses i 1 mom. 1 punkten ska lagras i fem år från identifieringstransaktionen. e 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 1 mom. 1 punkten och 4 mom. inte på tjänsteleverantören, 2) räknas den registreringstid på fem år som avses i 3 mom. från det att identifieringsverktyget upphörde att gälla.		
60.	S, H	Det särskilda kravet i **24 § i autentiseringslagen** på registrering av uppgifter om behandling av uppgifter som enligt lag ska lagras.	**Autentiseringslagen 24 § Registrering och användning av uppgifter om identifieringstransaktioner och identifieringsverktyg** […] 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	A.12.4.1 Driftsäkerhet: Loggning av händelser A.12.4.3 Administratörs- och operatörsloggar	Observera spårning av behandlingsuppgifter och säkring av loggdatas integritet.

			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. […]		
61.	S, H	**Tekniska åtgärder har vidtagits för att säkerställa integritet och sekretess för uppgifter som behandlas och lagras** i identifieringssystem.	**Autentiseringslagen 8 § Krav på system för elektronisk identifiering** […] 4) identifieringssystemet är säkert och tillförlitligt på ett sådant sätt att åtminstone de villkor uppfylls som gäller för tillitsnivån väsentlig enligt avsnitten ... 2.4.6 i bilagan till förordningen om tillitsnivåer vid elektronisk identifiering, med hänsyn till de informationssäkerhetsrisker som är förknippade med den teknik som används vid tidpunkten **LoA Bilaga 2.4.6 Tekniska kontrolle**r (controls) 1. Proportionella tekniska kontroller ska finnas för att hantera riskerna för tjänsternas säkerhet, och för att skydda de behandlade uppgifternas sekretess, integritet och tillgänglighet. Väsentlig: Känsligt krypteringstekniskt material, som används för att bevilja och autentisera metoder för elektronisk identifiering, är skyddade mot olovlig hantering. **M72B 5.4 Säkerhet i användning** I driften av identifieringssystemet ska man planera, förverkliga och kontinuerligt upprätthålla […] b) en behandlingsmiljö och förvaring för sekretessbelagt material som baserar sig på klassificeringen av informationen, […] e) säkerhetskopiering, samt f) använda krypteringslösningar som rekommenderas internationellt eller nationellt.	A.9.1.1 Regler för styrning av åtkomst A.9.1.2 Tillgång till nätverk och nätverkstjänster A.10.1.1 Regler för användning av kryptografiska säkerhetsåtgärder A.12.4.2 Driftsäkerhet: Skydd av logginformation	Kryptering av information och/eller åtkomsthantering Åtskillnad vid behov (jfr särskilt kryptografiskt material) Säkerhetskopiering/återställande Ett nyckelutbyte som har fastställts bland krypteringskraven i rekommendationen kan vara relevant mellan en identifieringstjänst och dess underleverantör, även om det inte är relevant vid diskkryptering Hantering och säkerställande av hemligheter som står som grund för tillitsförhållandet Vid förvaringen måste man beakta att den fysiska placeringen ska separeras från det egentliga systemet.

			M72B 7, Krypteringskrav på identifieringssystemets gränssnitt **7.1 Krypteringsmetoder för datakommunikationen** 7.1.1 Trafiken i gränssnitten mellan leverantörer av identifieringstjänster och mellan leverantörer av identifieringstjänster och förlitande parter ska krypteras. Följande metoder ska användas vid kryptering, vid nyckelutbyte, i certifikat 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) Underskrift eller asymmetrisk kryptering: Vid användning av RSA för elektronisk underskrift eller kryptering ska nyckeln utgöra minst 2 048 bitar. Vid användning av metoder för elliptisk kurva från ECDSA eller EdDSA ska storleken på den ändliga kroppen vara minst 224 bitar. 3) Symmetrisk kryptering: Krypteringsalgoritmen ska vara AES, Serpent eller ChaCha20. Nyckeln ska utgöra minst 128 bitar. Krypteringsläget ska vara CBC, CCM, GCM eller CTR. 4) Hashfunktioner: Hashfunktionen eller autentiseringskoden ska vara SHA-2, SHA-3, Whirlpool eller Poly1305. 7.1.2 Utöver de som nämns i punkt 7.1.1 kan man följa metoder och värden som har bedömts vara säkra för sådan användning som avses i underpunkterna 1–4 i de aktuella versionerna av följande dokument:		

			a) Anvisningen Kryptografiset vahvuusvaatimukset luottamuksellisuuden suojaamiseen – kansalliset turvallisuusluokat (Dnr 190/651/2015) av myndigheten för godkännande av krypteringsprodukter (Crypto Approval Authority) inom Transport- och kommunikationsverket, eller b) dokumentet SOG-IS Crypto Evaluation Scheme Agreed Cryptographic Mechanisms, utgivet av vissa certifieringsorgan i EU-medlemsstater eller i medlemsstater i EES-området (Senior Officers Group for Information Systems, Mutual Recognition Agreement SOGIS-MRA). 7.1.3 Krypteringsinställningarna ska tekniskt tvingas till miniminivåerna ovan för att handskakningen inte ska resultera i inställningar som är sämre än miniminivåerna. **7.2 Krypteringsprotokoll för datakommunikationen** Om man använder TLS-protokoll ska man använda minst version 1.2.		
62.	H	Vid behandling och lagring av uppgifter följs de krypteringskrav som fastställs i **rekommendationen**/krypteringskraven på tillitsnivån hög.	**MPS M72B punkt 4.7.1.3 (20.5.2022) rekommendation** För tillitsnivån hög i identifieringssystem rekommenderas det att man i stället för de värden som förutsätts för tillitsnivån väsentlig enligt 7.1 i föreskriften tillämpar följande värden inom parentes, **med vilka man uppnår en styrka på 128 bitar**: 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 (**4 096 på**	se ovan	Nyckelutbyte kan vara relevant mellan en identifieringstjänst och dess underleverantör.

			tillitsnivån hög) bitar i DHE-metoden och minst 224 (**256 på tillitsnivån hög**) bitar i ECDHE-metoden. DH-grupperna 14-21, 23, 24 och 26 (16-21 på tillitsnivån hög) enligt IANAs IKEv2-parametrar uppfyller kraven ovan. 2) Underskrift eller asymmetrisk kryptering: Vid användning av RSA för elektronisk underskrift eller kryptering ska nyckeln utgöra minst 2 048 (**3 072 på tillitsnivån hög**) bitar. Vid användning av ECDSA- eller EdDSA-metoden för elliptisk kurva ska den ändliga kroppen nedan utgöra minst 224 (**256 på tillitsnivån hög**) bitar. 3) Symmetrisk kryptering: Krypteringsalgoritmen ska vara AES, Serpent eller ChaCha20 (**på tillitsnivån hög AES eller Serpent**). Nyckeln ska utgöra minst 128 (**128 på tillitsnivån hög**) bitar. Krypteringsläget ska vara CBC, CCM, GCM eller CTR. 4) Hashfunktioner: Hashfunktionen eller autentiseringskoden ska vara SHA-2, SHA-3, Whirlpool eller Poly1305. Med SHA-2 avses funktionerna SHA224, SHA256, SHA384 och SHA512 (**på tillitsnivån hög SHA-3-256, SHA-3-384, SHA-3-512**)		
63.	S, H	Alla **medel** som innehåller personuppgifter eller kryptografiska eller andra känsliga uppgifter ska lagras, transporteras och bortskaffas på ett säkert sätt.	**LoA Bilaga 2.4.6 Tekniska kontrolle**r (controls) 5) Alla medel som innehåller personuppgifter eller kryptografiska eller andra känsliga uppgifter ska lagras, transporteras och bortskaffas på ett säkert sätt. **M72B 5.4 Säkerhet i användning** I driften av identifieringssystemet ska man planera, förverkliga och kontinuerligt upprätthålla	A.8.3 Hantering av tillgångar/Hantering av lagringsmedia A.11.2.6 Säkerhet för utrustning och	hantering, förstöring, överföring

			[…] b) en behandlingsmiljö och förvaring för sekretessbelagt material som baserar sig på klassificeringen av informationen, […]	tillgångar utanför organisationens lokaler A.11.2.7 Säker kassering eller återanvändning av utrustning	

B 6 Säkerhet i anläggningar

CENTRALA BESTÄMMELSER

M72B 15 Bedömningskriterier för överensstämmelse
En bedömning enligt 29 § i autentiseringslagen måste omfatta alla de krav som ställs i lagen och i denna föreskrift som gäller
1) funktioner som påverkar tillhandahållandet av identifieringstjänsten (ett identifieringssystem)
c) anläggningar och [...]

Autentiseringslagen 8 § Krav på system för elektronisk identifiering
4) identifieringssystemet är säkert och tillförlitligt på ett sådant sätt att […] de lokaler som används för tillhandahållandet av identifieringstjänsten är säkra på det sätt som anges i avsnitt 2.4.5 i bilagan till förordningen om tillitsnivåer

NR	TILL-LITS-NIVÅ	SAMMANDRAG ÖVER KRAVEN PÅ IDENTIFIERINGSTJÄNSTEN	BESTÄMMELSER	STANDARD HÄNVISNING	OBSERVATIONER
64.	S, H	**Säkerhet i anläggningar** Anläggningarna för identifieringssystem har indelats i säkerhetszoner med beaktande av hur sekretessbelagda och kritiska uppgifterna är.	**LoA Bilaga, 2.4.5 Anläggningar och personal** 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.	A.11.1 Fysisk och miljörelaterad säkerhet/Säkra områden: A.11.1.1 Fysiska säkerhetsavgränsningar	Alla anläggningar som används vid eller påverkar tillhandahållandet av identifieringstjänster, även underleverantörer Utgångspunkten är att det räcker med att uppfylla Katakri, om tillhandahållandet av identifieringssystemet sker i de aktuella anläggningarna. De övriga

					standardernas omfattning har inte utretts.
65.	S, H	Den utrustning som används vid tillhandahållandet av identifieringstjänster **är skyddade** mot intrång, skadegörelse, brand, värme, gaser, damm, vibrationer, vatten och avbrott i eldistributionen. Säkerhetszonerna har beaktats i styrkan i skyddet. I anläggningarna finns en ändamålsenlig **passerkontroll**/tillträdesövervakning som säkerställer att endast behöriga personer har tillträde till anläggningarna. Säkerhetssystem och utrustning som är avsedda för fysiskt skydd av information ska vara förenliga med allmänt tillämpade tekniska standarder eller minimikrav.	**LoA Bilaga, 2.4.5 Anläggningar och personal** 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.	A.11.1.2 fysiska tillträdesbegränsningar A.11.1.3 Säkerställande av kontor, rum och anläggningar A.11.1.4 Skydd mot yttre och miljörelaterade hot A.11.2.1 Placering av utrustning och skydd A.11.2.3 Kablagesäkerhet	
66.	S, H	Det gäller att kontrollera att det inte finns några **obehöriga** utrustningar eller förbindelser i säkerhetszonerna.	**LoA Bilaga, 2.4.5 Anläggningar och personal** 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.	A.11. Fysisk och miljörelaterad säkerhet	

B 7 Tillräckliga och kvalificerade personalresurser

CENTRALA BESTÄMMELSER **M72B 15.1 Funktioner som ska bedömas i identifieringssystemet och identifieringsmedlet** En bedömning enligt 29 § i autentiseringslagen måste omfatta alla de krav som ställs i lagen och i denna föreskrift som gäller 1) funktioner som påverkar tillhandahållandet av identifieringstjänsten (ett identifieringssystem) c) [...] och personal					
NR	**TILL-LITS-NIVÅ**	**SAMMANDRAG ÖVER KRAVEN PÅ IDENTIFIERINGSTJÄNS-TEN**	**BESTÄMMELSER**	**STANDARD HÄNVIS-NING**	**OBSERVATIONER**
67.	S, H	**Tillräcklig och kvalificerad personal** Produktionsorganisationen i identifieringstjänster ska ha tillräcklig sakkännedom och personalresurser för att kunna säkerställa informationssäkerheten och dataskyddet.	**Autentiseringslagen 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 [...] och 2.4.5 i bilagan till förordningen om tillitsnivåer vid elektronisk identifiering. **LoA Bilaga, 2.4.5 Anläggningar och personal** Krav i fråga om anläggningar och personal och underleverantörer, om tillämpligt, som åtar sig uppgifter som omfattas av denna förordning. Uppfyllandet av vart och ett av kraven ska stå i proportion till den risknivå som är knuten till den tillitsnivå som tillhandahålls. 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.	A.7.2.2 Personalsäkerhet/Under anställning: Medvetenhet, utbildning, fortbildning info säkerhet	Bedömning - personalresurserna är tillräckliga i proportion till verksamhetens karaktär (24/7/365) - tekniska övervakningsarrangemang beaktas, ej strikta krav på personalstyrkan eller jouren - kunskapen inom nödvändiga delområden (teknik, juridik bl.a. på grund av behandling av personuppgifter)

68.	S, H	Tjänster och verksamheter som har köpts för identifieringssystem har identifierats och dokumenterats. Underleverantörernas tillräckliga, kvalificerade personalresurser har säkerställts.	**Se raden ovan**	Se raden ovan A.15.1.1 Informationssäkerhetspolicy för leverantörsrelationer A.15.2.1 Övervakning och granskning av leverantörstjänster	Information om identifieringssystemets underleverantörer (kontorssystem, drifttjänster, programvaror, infrastruktur osv.) och, minst på en allmän nivå, en bedömning av underleverantörernas personalresurser.

B 8 Ledning avseende informationssäkerhet

CENTRALA BESTÄMMELSER

M72B 15.1 Funktioner som ska bedömas i identifieringssystemet och identifieringsmedlet
En bedömning enligt 29 § i autentiseringslagen måste omfatta alla de krav som ställs i lagen och i denna föreskrift som gäller
1) funktioner som påverkar tillhandahållandet av identifieringstjänsten (ett identifieringssystem)
   a) ledning avseende informationssäkerhet

M72B 4 Ledningssystem för informationssäkerhet hos leverantörer av identifieringstjänster
4.1 Standard för ledning av informationssäkerheten
Vid ledning avseende informationssäkerheten i identifieringssystem ska leverantörerna av identifieringstjänster följa standarden ISO/IEC 27001 eller någon annan allmänt känd motsvarande standard för ledning avseende informationssäkerhet. Ledningen avseende informationssäkerheten kan också bygga på en kombination av flera standarder.

4.2 Informationssäkerhetsledningens täckning
Ledningen avseende informationssäkerheten ska omfatta följande delområden som påverkar tillhandahållandet av en identifieringstjänst:
1) identifieringstjänsteleverantörens verksamhetsmiljö som en helhet,
2) styrning, organisering och administration av ledningen avseende informationssäkerheten,
3) hantering av informationssäkerhetsrisker vid tillhandahållande av en identifieringstjänst,
4) resurser för informationssäkerheten, kompetens, personalens medvetenhet om informationssäkerheten, kommunikation och dokumentation samt administration av dokumenterad information,
5) planering och styrning av tillhandahållandet av en identifieringstjänst för att informationssäkerhetskraven ska kunna uppfyllas, och
6) bedömning av effektivitet och funktion i ledningen avseende informationssäkerheten.

Autentiseringslagen 8 § Krav på system för elektronisk identifiering
Ett system för elektronisk identifiering ska uppfylla följande krav:

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 förordningen.

LoA Bilaga 2.4 Hantering och organisation
Alla deltagare som tillhandahåller en tjänst för elektronisk identifiering i ett gränsöverskridande sammanhang (nedan kallad en tillhandahållare av tjänster) ska i dokumenterad form ha praxis, policyer och strategier för ledning av informationssäkerhet vad avser risker samt andra erkända kontroller som ger styrningsorganen för system för elektronisk identifiering i respektive medlemsstat garantier att effektiva förfaranden föreligger. Alla krav/beståndsdelar i hela avsnitt 2.4 ska antas stå i proportion till riskerna på en viss nivå.

LoA Bilaga 1. Tillämpliga definitioner

4) med 'ledningssystem för informationssäkerhet' avses en uppsättning processer och förfaranden avsedda att hantera godtagbara risknivåer förknippade med informationssäkerhet.

LoA Bilaga 2.4.7 Efterlevnad och revision
Väsentlig: Förekomst av regelbundna oberoende interna eller externa revisioner, som är utformade så att de omfattar alla delar som är relevanta för tillhandahållandet av tjänster, för att garantera efterlevnaden av relevant policy.

NR	TILL-LITS-NIVÅ	SAMMANDRAG ÖVER KRAVEN PÅ IDENTIFIERINGSTJÄNS-TEN	BESTÄMMELSER	STANDARD HÄNVIS-NING	OBSERVATIONER
69.	S, H	Leverantörer av identifierings-tjänster har ett effektivt **led-ningssystem för informat-ionssäkerhet** för hantering och kontroll av informationssäker-hetsrisker i identifieringstjänster som tillhandahålls via identifie-ringssystem (inkl. organisato-riska och tekniska åtgärder).	**LoA Bilaga 2.4.3 Ledning avseende informat-ionssäkerhet** Det finns ett effektivt ledningssystem för inform-ationssäkerhet för hantering och kontroll av in-formationssäkerhetsrisker. Väsentlig: Ledningssystemet för informationssä-kerhet följer utprovade standarder eller principer för hantering och kontroll av informationssäker-hetsrisker.	5 ledarskap A.5 Informat-ionssäkerhets-policy	Kravet på ledning avse-ende informationssäkerhet har uppfyllts när ISO 27001 har tillämpats utan större avvikelser.
70.	S, H	Ett ledningssystem för informat-ionssäkerhet bygger på en eller flera allmänt kända standarder.	**M72B 4 Ledningssystem för informationssä-kerhet hos leverantörer av identifierings-tjänster** **4.1 Standard för ledning av informationssä-kerheten**		

			Vid ledning avseende informationssäkerheten i identifieringssystem ska leverantörerna av identifieringstjänster följa standarden ISO/IEC 27001 eller någon annan allmänt känd motsvarande standard för ledning avseende informationssäkerhet. Ledningen avseende informationssäkerheten kan också bygga på en kombination av flera standarder. **LoA Bilaga 2.4.3 Ledning avseende informationssäkerhet** Väsentlig: Ledningssystemet för informationssäkerhet följer utprovade standarder eller principer för hantering och kontroll av informationssäkerhetsrisker.		
71.	S, H	Ledningssystemet för informationssäkerhet omfattar de väsentliga interna och externa tekniska, juridiska och administrativa krav och behov som påverkar identifieringssystemet.	**M72B 4.2 Informationssäkerhetsledningens täckning** Ledningen avseende informationssäkerheten ska omfatta följande delområden som påverkar tillhandahållandet av en identifieringstjänst: 1) identifieringstjänsteleverantörens verksamhetsmiljö som en helhet, 2) styrning, organisering och administration av ledningen avseende informationssäkerheten, […]	4 organisationens omvärld	I en identifieringstjänst ska man bland annat följa aktuella lagar och förordningar, såsom autentiseringslagen, föreskriften M72 och den allmänna dataskyddsförordningen.
72.	S, H	Ett ledningssystem för informationssäkerhet omfattar styrning, organisering och administration av ledningen avseende informationssäkerheten. Det finns en aktuell **informationssäkerhetspolicy** som har godkänts av företagsledningen. Säkerhetsprinciperna och policyerna är heltäckande och ändamålsenliga i förhållande till organisationen och de objekt som ska skyddas.	**M72B 4.2 Informationssäkerhetsledningens täckning** Ledningen avseende informationssäkerheten ska omfatta följande delområden som påverkar tillhandahållandet av en identifieringstjänst: […] 2) styrning, organisering och administration av ledningen avseende informationssäkerheten, […] 4) resurser för informationssäkerheten, kompetens, personalens medvetenhet om informationssäkerheten, kommunikation	5 ledarskap 9.2 intern kvalitetsrevision 9.3 ledningens syn 10 förbättring av ledningssystem A.5.1.1 Informationssäkerhetspolicyer	

		Personalens och underleverantörernas ansvar i fråga om informationssäkerhet har beskrivits.	och dokumentation samt administration av dokumenterad information, […]	A.6.1.1 Roller och ansvar för informationssäkerhet A.15.1.1 Informationssäkerhetspolicy för leverantörsrelationer	
73.	S, H	Ledningssystemet för informationssäkerhet omfattar hantering av de informationssäkerhetsrisker som anknyter till tillhandahållandet av identifieringstjänsten. Riskhantering är en regelbunden, kontinuerlig och dokumenterad process. De identifierade riskerna klassificeras och prioriteras. Genom riskhanteringsprocessen identifieras risker som berör informationens konfidentialitet, integritet och tillgänglighet. Riskhanteringsprocessen och dess resultat används för att planera säkerhetsfunktioner för identifieringstjänsten/identifieringssystemet.	**M72B 4.2 Informationssäkerhetsledningens täckning** Ledningen avseende informationssäkerheten ska omfatta följande delområden som påverkar tillhandahållandet av en identifieringstjänst: […] 3) hantering av informationssäkerhetsrisker vid tillhandahållande av en identifieringstjänst, […]	6 Planering 8 Verksamhet	
74.	S, H	Systemet för hantering av informationssäkerheten omfattar resurstilldelning för informationssäkerhet, behörighetskrav, personalens medvetenhet om informationssäkerhet, kommunikation och dokumentation samt	**M72B 4.2 Informationssäkerhetsledningens täckning** Ledningen avseende informationssäkerheten ska omfatta följande delområden som påverkar tillhandahållandet av en identifieringstjänst: […]	7 Stödfunktioner	

		hantering av dokumenterad information. Alla som deltar i uppgifter i anknytning till elektronisk identifiering ska ha tillgång till och känna till de aktuella anvisningarna och rutinerna för informationssäkerhet. Säkerhetsutbildningen för personalen är regelbunden och dokumenteras. Utbildningens effektivitet följs upp.	4) resurser för informationssäkerheten, kompetens, personalens medvetenhet om informationssäkerheten, kommunikation och dokumentation samt administration av dokumenterad information, […]		
75.	S, H	I ledningssystemet för informationssäkerhet sköter man planeringen och styrningen av tillhandahållandet av identifieringstjänsten så att de informationssäkerhetskrav som ställs på identifieringstjänsten uppfylls.	**M72B 4.2 Informationssäkerhetsledningens täckning** Ledningen avseende informationssäkerheten ska omfatta följande delområden som påverkar tillhandahållandet av en identifieringstjänst: […] 5) planering och styrning av tillhandahållandet av en identifieringstjänst för att informationssäkerhetskraven ska kunna uppfyllas, och […]	8 verksamhet A.18.1.1 överensstämmelse/efterlevnad av krav i lagstiftningen och avtal: specificering av de lagstadgade och avtalsmässiga krav som ska tillämpas	Krav som har fastställts för identifieringstjänster Dataskyddsbestämmelser i tillämpliga delar Avtalsbestämmelser för förtroendenät i tillämpliga delar
76.	S, H	Ledningssystemet för informationssäkerhet omfattar regelbunden bedömning av effektiviteten och funktionen i ledningen av informationssäkerheten,	**M72B 4.2 Informationssäkerhetsledningens täckning** Ledningen avseende informationssäkerheten ska omfatta följande delområden som påverkar tillhandahållandet av en identifieringstjänst: […] 6) bedömning av effektivitet och funktion i ledningen avseende informationssäkerheten.	9.1 uppföljning, mätning, analys, bedömning	Hur stor effekt har ledningen avseende informationssäkerheten på de faktorer, processer och problem som inverkar på informationssäkerheten i identifieringssystem?

B 9 Styrkande och kontroll av identitet hos sökande av identifieringsverktyg (inledande identifiering)

CENTRALA BESTÄMMELSER

M72B 15.1 Funktioner som ska bedömas i identifieringssystemet och identifieringsmedlet
En bedömning enligt 29 § i autentiseringslagen måste omfatta alla de krav som ställs i lagen och i denna föreskrift som gäller
2) identifieringsmetod, dvs. identifieringsverktyg
b) styrkande och kontroll av den sökandes identitet

Autentiseringslagen 8 § Krav på system för elektronisk identifiering
Ett system för elektronisk identifiering ska uppfylla följande krav:

1) identifieringsmetoden grundar sig på 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,

[…]

Autentiseringslagen 17 § 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, i 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.

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. [...]

LoA Bilaga 2.1.2 Styrkande och kontroll av identitet (fysisk person)
LoA Bilaga 2.1.3 Styrkande och kontroll av identitet (juridisk person)
LoA Bilaga 2.1.4 Bindning mellan fysiska och juridiska personers medel för elektronisk identifiering

JURIDISKA PERSONER
Kraven på utfärdande av identifieringsverktyg till juridiska personer behandlas inte i detalj i samband med dessa kriterier. Om en leverantör av identifieringstjänster börjar tillhandahålla juridiska personer identifieringsverktyg för stark autentisering, ska bestämmelserna om detta beaktas i bedömningen.

Autentiseringslagen 17 a § Identifiering av en juridisk person som ansöker om ett identifieringsverktyg
Den identitet som uppgetts av en juridisk person ska kontrolleras med användning av företags- och organisationsregistren eller på ett sådant sätt att åtminstone de krav på styrkande och kontroll av juridiska personers identitet uppfylls som gäller för tillitsnivån väsentlig enligt avsnitt 2.1.3 i bilagan till förordningen om tillitsnivåer vid elektronisk identifiering.

Autentiseringslagen 7 a § Användning av uppgifter i företags- och organisationsregister
Leverantörer av identifieringsverktyg och certifikatutfärdare som tillhandahåller betrodda tjänster ska hämta och uppdatera de uppgifter som de behöver för tillhandahållandet av identifieringstjänster för juridiska personer med användning av företags- och organisationsregistren. Leverantörer av identifieringstjänster ska dessutom säkerställa att de uppgifter som de behöver för tillhandahållandet av identifieringstjänster är uppdaterade enligt uppgifterna i företags- och organisationsregistren.

DEFINITIONER

Autentiseringslagen 2 § Definitioner
7) inledande identifiering verifiering av identiteten hos den som ansöker om ett identifieringsverktyg, när verifieringen sker i samband med att verktyget skaffas,

LoA Bilaga 1. Tillämpliga definitioner
1. tillförlitlig källa: en källa oavsett form som är tillförlitlig när det gäller att tillhandahålla korrekta uppgifter, information och/eller bevis som kan användas för att styrka en identitet.

Standard: ETSI TS 119 461

NR	TILL-LITS-NIVÅ	SAMMANDRAG ÖVER KRAVEN PÅ IDENTIFIERINGSTJÄNS-TEN	BESTÄMMELSER	STANDARD HÄNVIS-NING	OBSERVATIONER
Metod 1: Inledande identifiering utgår från att en person visar ett identitetsbevis som är godkänt i Finland					
77.	S, H	Styrkandet av identitet bygger på identitetsbevis som är godkända enligt autentiseringslagen.	**Autentiseringslagen 17 § Identifiering av en fysisk person som ansöker om ett identifieringsverktyg** […]		Gäller vid användning av en inledande identifiering som bygger på identitetsbevis.

		När det gäller andra identitetsbevis utfärdade i stater som räknas upp i lagen har godkännandet definierats på ett tydligt sätt.	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, i 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. […]		
78.	S, H	Identitetsbeviset visas upp och dess äkthet granskas **på ort och ställe**. Personalen är förtrogen med äkthetsfaktorerna i identitetsbevisen och kan granska dem. Man säkerställer att identitetsbeviset tillhör den person som visar upp det.	**Autentiseringslagen 17 § 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. [...] **LoA Bilaga 2.1.2 Styrkande och kontroll av identitet (fysisk person)** Väsentlig: 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		Om det är frågan om identifiering på distans, se Kriterierna i punkt ”Metod 5”.

			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 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,		
79.	S	Identitetsbeviset visas upp och dess äkthet kontrolleras via **distansuppkoppling**. Personalen är förtrogen med äkthetsfaktorerna i identitetsbevisen och kan granska dem. Man säkerställer att identitetsbeviset tillhör den person som visar upp det. Tillförlitlighetskraven på distansuppkopplingen beaktar angreppspotentialen på tillitsnivån väsentlig.	**Autentiseringslagen 17 § 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. [...] **LoA Bilaga 2.1.2 Styrkande och kontroll av identitet (fysisk person)** Väsentlig: 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		Se 3.9 i denna anvisning

			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 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,		
80.	H	Identitetsbeviset visas upp och dess äkthet kontrolleras via distansuppkoppling. Personbevis äkthet kontrolleras utifrån en elektronisk signatur, framtagen av utfärdaren av beviset, på chipet. Kontroll sker av att identitetsbeviset tillhör den person som visar upp beviset. Kontrollen görs genom att personens egenskaper jämförs med de elektroniskt signerade uppgifterna i beviset.	**LoA Bilaga 2.1.2 Styrkande och kontroll av identitet (fysisk person)** Hög: 1.a) När en person har kontrollerats och befunnits inneha fotografiskt eller biometriskt identifieringsbevis som erkänns i den medlemsstat där ansökan om medlet för elektronisk identitet görs, och den bevisningen avser den påstådda identiteten, kontrolleras beviset för att fastställa om det är giltigt enligt en tillförlitlig källa. och Sökanden har identifierats som den påstådda identiteten genom jämförelse av en eller flera fysiska egenskaper hos personen med en tillförlitlig källa.		Se 3.9 i denna anvisning

		Tillförlitlighetskraven på distans-uppkoppling beaktar angrepps-potentialen på tillitsnivån hög.			
81.	S, H	Passets eller identitetskortets giltighet kontrolleras ur polisens informationssystem eller ur tillförlitliga internationella källor.	**LoA Bilaga 2.1.2 Styrkande och kontroll av identitet (fysisk person)** *Förfarandena 1 och 2, delkrav* 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, **Autentiseringslagen 7 b § Information om giltighet för pass eller identitetskort** Leverantörer av identifieringstjänster har trots sekretessbestämmelserna rätt att via ett gränssnitt eller annars i elektronisk form få information ur polisens informationssystem om giltighet för pass eller identitetskort som används vid inledande identifiering.		Ett icke-obligatoriskt krav som dock kan påverka riskbedömningen och ersättningsansvaret. I regel nödvändigt på tillitsnivån hög.
82.	S, H	Personers existens kontrolleras i befolkningsdatasystemet.	**Autentiseringslagen 7 § 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. […]		Gäller alla förfaranden för inledande identifiering.
Metod 2: Inledande identifiering med elektroniskt identifieringsverktyg					
83.	S	Styrkandet av identiteten baserar sig på starka elektroniska identifieringsverktyg som godkänns i autentiseringslagen.	**Autentiseringslagen 17 § Identifiering av en fysisk person som ansöker om ett identifieringsverktyg** Vid inledande identifiering ska identifieringen av en fysisk person göras personligen eller elektroniskt		Gäller vid användning av en inledande identifiering som bygger på stark autentisering.

			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. […] **LoA Bilaga 2.1.2 Styrkande och kontroll av identitet (fysisk person)** Väsentlig: 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.		Transport- och kommunikationsverkets register innehåller de identifieringsverktyg på tillitsnivån väsentlig som är godkända enligt autentiseringslagen.
84.	H	Styrkandet av identiteten baserar sig på starka elektroniska identifieringsverktyg som godkänns i autentiseringslagen. På tillitsnivån hög kan identifieringsverktyg utfärdas utifrån elektronisk identifiering enbart med medel som ska användas på tillitsnivån hög.	**LoA Bilaga 2.1.2 Styrkande och kontroll av identitet (fysisk person)** Hög: 3. Om medel för elektronisk identifiering utfärdas på grundval av ett giltigt anmält medel för elektronisk identifiering med tillitsnivån ”hög”, 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 ”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. och		Gäller vid användning av en inledande identifiering som bygger på stark autentisering. Transport- och kommunikationsverkets register innehåller de identifieringsverktyg på tillitsnivån hög som är godkända enligt autentiseringslagen.

			åtgärder vidtas för att styrka att resultaten av detta tidigare förfarande för utfärdande av ett anmält medel för elektronisk identifiering fortfarande är giltiga.		
Metod 3: Inledande identifiering utifrån en identifiering som sker för annat ändamål (”tidigare kundrelation”)					
85.	S, H	I styrkandet av identiteten litar man på ett förfarande med vilket identiteten styrkts och säkerställts tidigare för ett annat ändamål än för beviljandet av ett identifieringsverktyg för stark autentisering. Förfarandet kan basera sig på annan reglering än autentiseringslagen eller eIDAS-förordningen och det övervakas av en myndighet. Förfarandet erbjuder motsvarande säkerhet som ett förfarande som baserar sig på uppvisandet av ett identitetsbevis enligt regleringen av identifikationen eller ett elektroniskt identifikationssätt.	**Autentiseringslagen 17 § 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. […] **LoA Bilaga 2.1.2 Styrkande och kontroll av identitet (fysisk person)** Väsentlig: 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		Användningen av ett förfarande för inledande identifiering enligt den här punkten förutsätter en uttrycklig bekräftelse av Transport- och kommunikationsverket. Till anmälan om förfarandet ska en bedömning av överensstämmelsen med kraven bifogas. Det kan till exempel komma i fråga att använda 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.

			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.		
Metod 4: Inledande identifiering som utförs av polisen					
86.	S, H	Vid behov utförs den inledande identifieringen av polisen.	**Autentiseringslagen 17 § Identifiering av en fysisk person som ansöker om ett identifieringsverktyg** […] 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. […] **LoA Bilaga 2.1.2 Styrkande och kontroll av identitet (fysisk person)** Hög 2.Om den sökande inte lägger fram något erkänt fotografiskt eller biometriskt identifieringsbevis, ska samma förfaranden som används på nationell nivå i medlemsstaten av den enhet som ansvarar för registreringen för att erhålla sådant erkänt fotografiskt eller biometriskt identifieringsbevis tillämpas.		
Metod 5: Inledande identifiering med distansuppkoppling					
87.	S	Lösningen för inledande identifiering med distansuppkoppling ska basera sig på en riskbedömning (Level of Identity Proofing, LoIP)	**Autentiseringslagen 8 § Krav på system för 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 tidpunk-	ETSI TS 119 461 ISO/IEC TS 29003:2018	Angreppspotential (väsentlig/hög) och utredning av vilka definierade kriterier som ska uppfyllas för att beviljandeprocessen kan slutföras, leveranskedjans säkerhet om man använder en tjänsteleverantör, om grunden är granskningen av en bild

			ten samt att de lokaler som används för tillhandahållandet av identifieringstjänsten är säkra på det sätt som anges i avsnitt 2.4.5 i bilagan till 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. […] **M72B 6.1 Identifieringsmedlets egenskaper och skyddsförmåga** 6.1.1 Identifieringsmedlets autentiseringsfaktorer, autentiseringsmekanism och säkerhetsåtgärder ska planeras, genomföras och upprätthållas så att de skyddar identifieringsmedlets integritet och sekretess. Identifieringsmedlet ska ha skyddsförmåga åtminstone på tillitsnivån väsentlig eller hög mot hot och angreppspotential enligt punkt 2.3 i bilagan till förordningen om tillitsnivåer vid elektronisk identifiering, i enlighet med identifieringstjänstens tillitsnivå. Skyddsförmågan ska basera sig på en riskbedömning, där man separat bedömer hot mot autentiseringsfaktorer och -mekanismer som baserar sig på innehav, information och egenskaper samt säkerhetsåtgärder som skyddar mot hoten. **LoA Bilaga 2.4.3 Ledning avseende informationssäkerhet** Låg: Det finns ett effektivt ledningssystem för informationssäkerhet för hantering och kontroll av informationssäkerhetsrisker. Väsentlig:		(selfie) eller ett videomaterial, kriterier som ska uppfyllas för att man övergår från en automatisk process till en manuell process.

			Ledningssystemet för informationssäkerhet följer utprovade standarder eller principer för hantering och kontroll av informationssäkerhetsrisker.		
88.	S	Information till kunden om villkor och förutsättningar	**Autentiseringslagen 20 § Beviljande av identifieringsverktyg** 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. […] **Autentiseringslagen 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. **LoA 2.1.1. Ansökan och registrering** 1. Säkerställ att sökanden har kännedom om villkor och förutsättningar för användningen av metoder för elektronisk identifiering. 2. Säkerställ att sökanden har kännedom om rekommenderade säkerhetsåtgärder för metoderna för elektronisk identifiering. […]		
89.	S	Godkända dokument för inledande identifiering och kontroll av deras giltighet	**Autentiseringslagen 17 § Identifiering av en fysisk person som ansöker om ett identifieringsverktyg** […]		För närvarande i praktiken pass, eventuellt även identitetskort. Giltighetstiden hos dokumentet för inledande identifiering ska

			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, i 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. […] **Autentiseringslagen 7 b § Information om giltighet för pass eller identitetskort** Leverantörer av identifieringstjänster har trots sekretessbestämmelserna rätt att via ett gränssnitt eller annars i elektronisk form få information ur polisens informationssystem om giltighet för pass eller identitetskort som används vid inledande identifiering. **LoA 2.1.2 Styrkande och kontroll av identitet (fysisk person)** Låg: 1. Personen kan antas inneha ett bevis som erkänns i den medlemsstat där ansökan om medlet för elektronisk identitet görs och som avser den påstådda identiteten, 2. Beviset kan antas vara äkta eller giltigt enligt en tillförlitlig källa, och det verkar vara giltigt. 3. Den tillförlitliga källan känner till att den anmälda identiteten är befintlig och man kan anta att personen som uppger identiteten har denna samma identitet. Väsentlig: Dessutom minst 1 st. från punkten väsentlig, t.ex.		kontrolleras mot polisens gränssnitt eller ett annat internationellt tillförlitligt gränssnitt (Interpol).

			1. 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,		
90.	S	Personers existens kontrolleras i befolkningsdatasystemet.	**Autentiseringslagen 7 § 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. […] **LoA 2.1.2 Styrkande och kontroll av identitet (fysisk person)** Låg: 3. Den tillförlitliga källan känner till att den anmälda identiteten är befintlig och man kan anta att personen som uppger identiteten har denna samma identitet.		Gäller alla förfaranden för inledande identifiering.
91.	S	En applikation och externa lösningar eller komponenter som utför inledande identifiering med distansuppkoppling ska utvärderas eller vara utvärderade	**Autentiseringslagen 29 § Bedömning av överensstämmelse hos en elektronisk identifieringstjänst** En leverantör av identifieringstjänster ska regelbundet låta ett sådant bedömningsorgan som	ETSI TS 119 461 ISO/IEC TS 29003:2018	En bedömning av ett bedömningsinstitut, FAR-värdet, vilken testdata FAR baserar sig på, motsvarig-

			nämns i 28 § bedöma om identifieringstjänsten uppfyller kraven på interoperabilitet, informationssäkerhet, dataskydd och annan tillförlitlighet enligt denna lag. […] **M72B 4.2 Informationssäkerhetsledningens täckning** Ledningen avseende informationssäkerheten ska omfatta följande delområden som påverkar tillhandahållandet av en identifieringstjänst: 1) identifieringstjänsteleverantörens verksamhetsmiljö som en helhet, 2) styrning, organisering och administration av ledningen avseende informationssäkerheten, 3) hantering av informationssäkerhetsrisker vid tillhandahållande av en identifieringstjänst, 4) resurser för informationssäkerheten, kompetens, personalens medvetenhet om informationssäkerheten, kommunikation och dokumentation samt administration av dokumenterad information, 5) planering och styrning av tillhandahållandet av en identifieringstjänst för att informationssäkerhetskraven ska kunna uppfyllas, och 6) bedömning av effektivitet och funktion i ledningen avseende informationssäkerheten. **M72B 15 Bedömningskriterier för överensstämmelse** **15.1 Funktioner som ska bedömas i identifieringssystemet och identifieringsmedlet** En bedömning enligt 29 § i autentiseringslagen måste omfatta alla de krav som ställs i lagen och i denna föreskrift som gäller	ISO/IEC 30107	het med angreppspotentialen (väsentlig/hög). PAD-prestanda (Presentation Attack Detection). FRR är inte väsentlig Tillämpningen ska även bedömas eller på annat sätt ska dess säkerhet verifieras på ett sätt som motsvarar Bilaga C eller med ett annat liknande förfarande

			1) funktioner som påverkar tillhandahållandet av identifieringstjänsten (ett identifieringssystem) a) ledning avseende informationssäkerhet b) förvaringen och behandlingen av uppgifter c) anläggningar och personal d) tekniska åtgärder, och […] 2) identifieringsmetod, dvs. identifieringsverktyg a) ansökan och registrering b) styrkande och kontroll av den sökandes identitet […] d) utfärdande, leverans och aktivering e) upphävande, återkallelse och återaktivering f) förnyelse och ersättning, och g) autentiseringsmekanismer. **LoA 2.1.2 Styrkande och kontroll av identitet (fysisk person)** Väsentlig: 1. 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,		

92.	S	Det uppvisade dokumentets äkthet och att uppgifterna inte ändrats. Aktiv och passiv verifiering av dokument som används för inledande identifiering, granskning av dokumentet via videoförbindelse (MRZ, visuella säkerhetsfaktorer)	**LoA bilaga 2.1.2 Styrkande och kontroll av identitet (fysisk person)** Låg: 2. Beviset kan antas vara äkta eller giltigt enligt en tillförlitlig källa, och det verkar vara giltigt. Väsentlig: 1. […] beviset kontrolleras för att fastställa att det är äkta, eller enligt en tillförlitlig källa existerar det och avser en verklig person, […]		Äktheten hos dokumentet för inledande identifiering (pass, identitetskort) och äktheten hos informationen som lagrats på chipet ska kontrolleras
93.	S	Den inledande identifieringen och personens verifiering med videouppkoppling sker i förhållande vars minimikrav har fastställts.	**LoA bilaga 2.1.2 Styrkande och kontroll av identitet (fysisk person)** Väsentlig: 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,		Den inledande identifieringen på distans kan utföras i en sådan situation eller under sådana förhållanden där man kan maximera verkställandet av automatiska säkerhetskontroller.
94.	S	Automatiska säkerhetskontroller analyserar biometriken hos den inledande identifieringen på distans. Säkerhetskontrollerna är slumpmässiga eller baserar sig på metoder som kan påvisa att kraven enligt förordningen om tillitsnivå uppfylls.	**LoA bilaga 2.1.2 Styrkande och kontroll av identitet (fysisk person)** Låg: 3. Den tillförlitliga källan känner till att den anmälda identiteten är befintlig och man kan anta att personen som uppger identiteten har denna samma identitet. Väsentlig:		Med verksamheten strävar man efter att förhindra t.ex. skapandet av på förhand förberedda videoinspelningar Observering av livligheten på olika sätt automatiserat, till exempel antingen från videomaterial eller genom att

			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,		observera biosignaler från ansiktsbilden.
95.	S	För den inledande identifieringen på distans har tekniska minimikrav ställts upp, om de underskrids kan den inledandeidentifieringen på distans inte genomföras	**LoA bilaga 2.1.2 Styrkande och kontroll av identitet (fysisk person)** Låg: 3. Den tillförlitliga källan känner till att den anmälda identiteten är befintlig och man kan anta att personen som uppger identiteten har denna samma identitet. Väsentlig: […] 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,		T.ex. minimikrav på anordningsnivå, obrutenhet och snabbhet i datakommunikationsförbindelsen, resolution, kamerans förmåga, förekomsten av artefakter, resilienskriterierna i Bilaga C
96.	S	Överföring av uppgifter, lagring	**LoA Bilaga, 2.4.4 Registerföring** 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.		Dataskydd särskilt om information överförs utanför EU-området. Lagring för senare granskning om t.ex. missbruk iakttas.

			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. **även M72B 7 Krypteringskrav på identifieringssystemets gränssnitt**		
97.	S	Programvarukomponenten som utför den inledande identifieringen på distans ska vara verifierad	**Autentiseringslagen 13 § Allmänna skyldigheter för leverantörer av identifieringstjänster** […] Leverantören av identifieringstjänster svarar för att tjänster och produkter som produceras av personer som leverantören anlitar är tillförlitliga och fungerar. **LoA Bilaga 2.4.6 Tekniska kontroller** 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. […] **M72B Bedömningskriterier för överensstämmelse med kraven** **15.1 Funktioner som ska bedömas i identifieringssystemet och identifieringsmedlet** En bedömning enligt 29 § i autentiseringslagen måste omfatta alla de krav som ställs i lagen och i denna föreskrift som gäller 1) funktioner som påverkar tillhandahållandet av identifieringstjänsten (ett identifieringssystem):		I praktiken attestering av mobilapplikationen och tilllämpningen för bakgrundssystemet

			a) ledningen avseende informations-säkerhet		
98.	S	Den inledande identifieringen på distans ska åtminstone delvis basera sig på automatiserade processer.	**LoA Bilaga 2.4.6 Tekniska kontroller** 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.		Enbart användningen av en tjänsteman vid den inledande identifieringen på distans är inte tillräcklig utan processen ska åtminstone delvis basera sig på en jämförelse gjord med dator för de ovan nämnda kriteriernas del
99.	S	Den personal som deltar i processen för identifiering på distans ska vara utbildad	**LoA bilaga 2.4.5 Anläggningar och personal** 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.		Om även en anställd deltar i beslutsfattandet i processen för inledande identifiering på distans ska den anställda utbildas på tillräcklig nivå i att utvärdera äktheten hos eventuellt videomaterial, äkthetsfaktorerna i dokumentet för inledande identifiering

B 10 Identifieringsverktygs, eller identifieringsmetoders, livscykel

CENTRALA BESTÄMMELSER

M72B 15.1 Funktioner som ska bedömas i identifieringssystemet och identifieringsmedlet
En bedömning enligt 29 § i autentiseringslagen måste omfatta alla de krav som ställs i lagen och i denna föreskrift som gäller
2) identifieringsmetod, dvs. identifieringsverktyg
a) ansökan och registreringen
b) […]
c) […]
d) utfärdandet, leveransen och aktiveringen
e) upphävande, återkallelse och återaktivering
f) förnyelse och ersättning
g) […]

NR	TILL-LITS-NIVÅ	SAMMANDRAG ÖVER KRAVEN PÅ IDENTIFIERINGSTJÄNS-TEN	BESTÄMMELSER	STANDARD HÄNVIS-NING	OBSERVATIONER
100.	S, H	Identifieringsverktyg kombineras inte med personer, dvs. personifieras före inledande identifiering. De som skapat identifieringsmetoden kopplas till innehavaren av identifieringsmetoden.	**M72B 6.3 Koppling av ett identifieringsverktyg till en person** 6.3.1 Identifieringsmedlets autentiseringsfaktorer ska kopplas till innehavaren av identifieringsverktyget i identifieringssystemet. 6.3.2 Identifieringsverktyg får inte kopplas med den sökande förrän en inledande identifiering av den sökande har gjorts, eller så ska det vid processen för beviljande av identifieringsverktyg på annat sätt säkerställas att identifieringsverktyget inte kan användas innan en inledande identifiering av sökanden enligt 17 § i autentiseringslagen har gjorts.		
101.	S, H	Personuppgifterna för fysiska personer kontrolleras i befolkningsdatasystemet vid utfärdande av ett identifieringsverktyg och regelbundet under verktygets giltighet.	**Autentiseringslagen 7 § 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. […] **Se M72B 12 Minimiuppsättning uppgifter som ska förmedlas i förtroendenätet** **LoA bilaga 2.1.2 Styrkande och kontroll av identitet (fysisk person)** Väsentlig:		Hur regelbundet kontrollerna ska göras har inte fastställts. God vedertagen praxis är en gång i veckan. Jfr (autentiseringslagen innehåller ingen hänvisning, tillämpas endast om metoden anmäls) **LoA 2.1.1 Ansökan och registrering** 3. Samla in de relevanta identitetsuppgifter som krävs för styrkande och kontroll av identitet.

			1. 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,		
102.	S, H	**Utfärdande, leverans och aktivering av identifieringsverktyg** Förfarandet för överlåtelse eller leverans av identifieringsverktyg säkerställer att verktyget inte obehörigt kommer i någon annans besittning.	**Autentiseringslagen 20 § Beviljande av identifieringsverktyg** 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. […] Jfr (autentiseringslagen innehåller ingen hänvisning till 2.1.1 i LOA, dvs. det tillämpas formellt endast om metoden anmäls) **LoA 2.1.1 Ansökan och registrering** 1. Säkerställ att sökanden har kännedom om villkor och förutsättningar för användningen av metoder för elektronisk identifiering. 2. Säkerställ att sökanden har kännedom om rekommenderade säkerhetsåtgärder för metoderna för elektronisk identifiering. **Autentiseringslagen 21 § Överlåtelse av identifieringsverktyg till sökande** Leverantören av ett identifieringsverktyg ska överlåta identifieringsverktyget till sökanden på det sätt som anges i avtalet. Leverantören ska säkerställa		Avtalsvillkor (bl.a. 15 § i autentiseringslagen) ingår i frågor som aktören själv ska ta reda på och som inte omfattas av kvalitetsrevision. 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. Se LoA guidance: Möjliga mekanismer är till exempel följande: - personlig leverans

			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. **LoA Bilaga 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.		- 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 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.
103.	H	**Utfärdande, leverans och aktivering av identifieringsverktyg** Förfarandet för överlåtelse eller leverans av identifieringsverktyg säkerställer att verktyget inte obehörigt kommer i någon annans besittning.	**LoA Bilaga 2.2.2 Utfärdande, leverans och aktivering** <u>Hög:</u> Aktiveringsprocessen kontrollerar att medlet för elektronisk identifiering endast levererades till ägaren som det tillhör.		I regel förutsätter aktiveringsprocessen användningen av en aktiveringskod. Särskilt bör man sörja för att aktiveringskoden inte kan hamna i besittning hos andra vid leveransprocessen samt att aktiveringskoden är engångsanvändbar och att den inte kan användas för återaktivering eller för att skapa en ny pin-kod. Om aktiveringen inte utförs inom en viss tid, föråldras aktiveringskoden. Syftet är att säkerställa att aktiveringskoder som inte använts eller som används på nytt inte kan användas för att anullera, alltså överskriva den verifikationsfaktor (PIN) som endast användaren känner till eller aktivera identifieringsmetoden utan att denne vet om detta. I autentiseringslagen finns ingen hänvisning till LoA punkt 2.2.3 ”Åtgärder ska föreligga för att förhindra att

					upphävande, återkallelse och/eller reaktivering sker på otillåtet sätt.” Att koden endast kan användas en gång är dock bra praxis, om man inte på annat sätt kan skydda identifieringsverktyget från olovlig reaktivering.
104.	S, H	**Upphävande, återkallelse och återaktivering av identifieringsverktyg** Leverantörer av identifieringsverktyg har en 24/7-spärrlista för användare och en spärrlista för förlitande parter eller möjlighet att tekniskt förhindra användning av ett identifieringsverktyg som enligt användarens anmälan har stulits.	**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. 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. 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. 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 kon-		Jfr (autentiseringslagen innehåller ingen hänvisning till 2.2.3 i LOA, dvs. det tillämpas formellt endast om metoden anmäls) **LoA Bilaga 2.2.3 Upphävande, återkallelse och återaktivering** 1. Det är möjligt att avbryta och/eller återkalla ett medel för elektronisk identifiering i god tid och på ett verksamt sätt. 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.

			trollera uppgifterna föreligger dock inte, om användning av identifieringsverktyget kan förhindras med hjälp av tekniska medel eller om verktyget kan spärras. […] **26 § 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.		

			LoA bilaga 2.2.3 Upphävande, återkallelse och återaktivering 1. Det är möjligt att avbryta och/eller återkalla ett medel för elektronisk identifiering i god tid och på ett verksamt sätt. 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.		
105.	S, H	**Förnyande och ersättning av identifieringsverktyg**	**Autentiseringslagen 22 § 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. **LoA Bilaga 2.2.4 Förnyelse och ersättning** 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. **LoA bilaga 2.2.1 Medel för elektronisk identifiering: egenskaper och utformning** Väsentlig: 2. Metoden för elektronisk identifiering är planerad så att den kan antas användas endast om den innehas av den person som den tillhör. **LoA Bilaga 2.2.2 Utfärdande, leverans och aktivering**		Paragraf 8 i autentiseringslagen och avsnitt 2.2.1 och 2.2.2 i LoA innehåller krav på kontroll av att ett identifieringsverktyg endast får användas av ägaren. Detta krav ska även uppfyllas i alla situationer där vissa eller alla autentiseringsfaktorer eller aktiveringskoder överlåts på nytt vid förnyelse/ersättning eller återaktivering Se Tolkningsställningstagande *dnr: Traficom/106/09.02.00/2019 (25.3.2019) Transport- och kommunikationsverkets tolkningspromemoria om 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.* Ställningstagandet finns på

			Väsentlig: Efter utfärdandet levereras medlet för elektronisk identifiering via en mekanism genom vilken det kan antas att medlet levereras endast till ägaren.		ämbetsverkets webbplats på https://www.kybertur-vallisuus-keskus.fi/sv/elektronisk-identifiering
106.	H	**Förnyande och ersättning av identifieringsverktyg**	**LoA Bilaga 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. Hög: Om förnyelse eller ersättning grundas på ett giltigt medel för elektronisk identifiering, kontrolleras identitetsuppgifterna mot en tillförlitlig källa. **LoA bilaga 2.2.1 Medel för elektronisk identifiering: egenskaper och utformning** Hög: 2. Metoden för elektronisk identifiering är planerad så att personen det tillhör kan skydda det på ett tillförlitligt sätt från användning av andra. **LoA Bilaga 2.2.2 Utfärdande, leverans och aktivering** Hög: Aktiveringsprocessen kontrollerar att medlet för elektronisk identifiering endast levererades till ägaren som det tillhör.		Paragraf 8 i autentiseringslagen och avsnitt 2.2.1 och 2.2.2 i LoA innehåller krav på kontroll av att ett identifieringsverktyg endast får användas av ägaren. Detta krav ska även uppfyllas i alla situationer där vissa eller alla autentiseringsfaktorer eller aktiveringskoder överlåts på nytt vid förnyelse/ersättning eller återaktivering

Anvisning om bedömning av elektroniska identifieringstjänster

Transport- och kommunikationsverkets anvisning

211/2023 O Bilaga C Mobilkriterier

BILAGA C: Särskilda kriterier gällande lösningar för mobilidentifiering

Allmänt

Kriterierna gällande mobilappar **kompletterar de allmänna kriterierna**, när en mobilapp är integrerad i identifieringsmetoden eller identifieringssystemet.

Kriterierna har tagits fram **främst för tillitsnivån väsentlig**. Hänvisningar till förordningen om tillitsnivåer (EU) 2015/1502 (LoA) är på tillitsnivån väsentlig, ifall annat inte nämns. I framtiden kan kriterierna uppdateras och tillitsnivån hög kan också beaktas, när vi har fått erfarenhet av tillämpningen i Finland och en gemensam europeisk praxis om tolkning av eIDAS-kraven.

Detta dokument är en anvisning. Den som utför bedömningen ska överväga hur bra applikationen motsvarar kriterierna i anvisningen. Risken som avvikelserna medför bedöms som en helhet. Operativsystemets och identifieringsapplikationens versioner ska följas upp och ändringarnas totala inverkan på överensstämmelse med kraven ska bedömas. Leverantören av identifieringstjänster ska försäkra sig om att den får tillräckligt med aktuell information av applikationsleverantören om de ändringar som leverantören gjort i utrustningen eller programvaran.

Känslig information ("sensitive" i OWASP-kriterierna) betyder i detta sammanhang till exempel personuppgifter, kryptografiskt material eller konfidentiella/sekretessbelagda uppgifter som hänför sig till identifierings- eller registreringstransaktioner.

Anvisningen är avsedd för att bedöma mobila identifieringsapplikationers informationssäkerhet. Sådana här applikationer har vanligtvis en stark förbindelse med beviljarens bakgrundssystem. Med hjälp av denna anvisning kan man även bedöma applikationer av plånbokstyp vars förbindelse med bakgrundssystemet har minimerats.

Med märkningen App/Wallet avses en identifieringsmetod, alltså en applikation eller en del av en applikation som körs på enheten, och som utför stark elektronisk identifiering.

Kriterierna baserar sig på OWASP:s engelska dokument Mobile AppSec Verification (OWASP Mobile Application Security Verification Standard, MASVS version 1.4.2) som har utvidgats och modifierats så att den motsvarar användningsfallen inom identifiering.

Testanvisningen, som motsvarar OWASP:s originala kriterier, finns också på OWASP:s webbplats. Publikationen omfattar detaljerade och heltäckande anvisningar för testning av de originala OWASP-kriterierna.

Alternativa kriterier:

- FIDO 3 & 3+ (https://fidoalliance.org/certification/authenticator-certification-levels/)

C 1 Arkitektur, planer och modeller för hotbiler

NR	TILLIT SNIVÅ	KRITERIUM	MOTIVERING	Tilläggsinformation/kommentarer
400.		Alla komponenter i en applikation/plånbok har identifierats och klassificerats och är nödvändiga.	LoA 2.4.6, punkt 1 8.1 § 4 punkten i autentiseringslagen	
401.		Säkerhetskontrollerna genomförs inte bara på kundens sida, utan alltid i båda distanspunkterna.	LoA 2.4.6, punkt 1 M72B, underpunkt 5.3.c	
402.		En arkitektur på hög nivå har definierats för själva applikationen/plånboken och alla anslutna externa tjänster, och informationssäkerheten har beaktats i arkitekturen.	LoA 2.4.6, punkt 1 8.1 § 4 punkten i autentiseringslagen	
403.		Känsliga uppgifter som behandlas i appen/plånboken har identifierats och klassificerats på ett tydligt sätt och deras skyddsåtgärder har dokumenterats.	LoA 2.4.4, punkt 1 LoA 2.4.6, punkt 1 och 3	
404.		Alla komponenter i appen/plånboken har definierats utifrån de affärsverksamhets- och/eller säkerhetsåtgärder som de erbjuder.	LoA 2.4.6, punkt 1 8.1 § 4 punkten i autentiseringslagen	
405.		Hotbilder för appen/plånboken och de externa tjänster som den använder samt potentiella motåtgärder har identifierats.	LoA 2.3.1, väsentlig, punkt 2 LoA 2.3.1, hög	Angreppspotentialerna måttlig (väsentlig) eller hög (hög) bedöms.
406.		Alla säkerhetskontroller har en centraliserad implementering.	LoA 2.4.6, punkt 1	
407.		Lokala säkerhetskontroller har genomförts enligt branschens bästa praxis och har validerats med dessa kriterier.	LoA 2.4.6, punkt 1 M72B, underpunkt 6.1.1	
408.		Det finns en noggrant definierad metod för att hantera krypteringsnycklar, och metoden bygger på en internationellt godkänd, aktuell standard.	LoA 2.4.6, punkt 3 LoA 2.4.6, väsentlig	
409.		Appen/plånboken anger det operativsystem, egenskaperna på enheterna och programvaruversionens nummer för (beviljaren av appen/plånbokens) server.	LoA 2.4.6, punkt 1 M72B, underpunkt 5.3.c	
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.	LoA 2.3.1, väsentlig	
411.		Appen/plånboken stöder inte versioner av mobiloperativsystemen vars support/säkerhetsuppdateringar har	8.1 § 4 punkten i autentiseringslagen	Appen/plånboken ska klara av en riskbedömningsprocess. Om riskbedömningen

		upphört hos erbjudarna av operativsystem och fungerar inte på dessa.	M72B, underpunkt 5.4.d LoA 2.4.6, punkt 4	kommer fram till resultatet att gamla operativsystem som inte längre tar emot informationssäkerhetsuppdateringar är lämpliga kan även operativsystem som inte stöds användas. Denna utredning ska bifogas till inspektionsrapporten.
412.		Det finns en mekanism för att tvinga uppdatering av appen/plånboken.	ITSA section 8.1.4 M72B, subsection 5.4.d	
413.		En föråldrad app/plånbok uppmanar användaren att uppdatera operativsystemet och/eller appen/plånboken för att transaktionen ska kunna genomföras eller då appen/plånboken öppnas.	(LoA 2.1.1, punkt 2)	Rekommenderad praxis / Best practise (BP). 2.1.1 i LoA ingår inte i autentiseringslagen.
414.		Informationssäker praxis används under programvaruutvecklingens hela livscykel	LoA 2.4.6, punkt 1 och 4 8.1 § 4 punkten i autentiseringslagen	

C 2 Lagring av information samt dataskydd

Känslig information ("sensitive" i OWASP-kriterierna) betyder i detta sammanhang till exempel personuppgifter, kryptografiskt material eller konfidentiella/sekretessbelagda uppgifter som hänför sig till identifierings- eller registreringstransaktioner.

NR	TILLIT SNIVÅ	KRITERIUM	MOTIVERING	Tilläggsinformation/kommentarer
415.		Säkerhetstjänster/säkerhetsfunktioner i plattformen utnyttjas i full skala när appen lagrar känsliga uppgifter.	LoA 2.4.6, punkt 1, punkt 3	
416.		Användaren informeras på ett tydligt sätt vilken nivå identifieringen kommer att ske på.	LoA 2.1.1, punkt 2	Rekommenderad praxis
417.		Känslig information lagras inte utanför app-/plånboksmiljöns eller plattformens funktion för lagring av hemligheter.	LoA 2.4.6, punkt 1 M72B, underpunkt 5.4.b	
418.		Känslig information lagras inte i appens loggdata.	LoA 2.4.6, punkt 1 M72B, underpunkt 5.4.b	
419.		Känslig information delas inte med externa parter, om det inte i förväg har definierats i arkitekturen.	LoA 2.4.6, punkt 1 M72B, underpunkt 5.4.b	
420.		Cacheminnet är inte tillgängligt i textinmatningsfält som kan innehålla känsliga uppgifter.	LoA 2.4.6, punkt 1 M72B, underpunkt 5.4.b	
421.		Känsliga uppgifter och hemligheter (lösenord, pinkoder) röjs inte i något skede via användargränssnittet.	LoA 2.4.6, punkt 1 M72B, underpunkt 5.4.b	

422.		Klippbord används inte i dataelement som kan innehålla känsliga uppgifter.	LoA 2.4.6, punkt 1 M72B, underpunkt 5.4.b	
423.		Känsliga uppgifter delas inte när IPC-mekanismer används.	LoA 2.4.6, punkt 1 M72B, underpunkt 5.4.	
424.		Hemligheter som används vid identifiering lagras eller överförs inte utanför det datalager som används i appen.	LoA 2.4.6, låg, punkt 3 LoA 2.4.6, väsentlig M72B, underpunkt 5.4.b	
425.		När appen/plånboken övergår i bakgrunden raderas de känsliga uppgifterna från alla komponenter i användargränssnittet.	LoA 2.4.6, punkt 1 M72B, underpunkt 5.4.b	
426.		Känsliga uppgifter lagras inte onödigt lång tid i appens/plånbokens minne, och när uppgifterna inte längre behövs raderas de från minnet.	LoA 2.4.6, punkt 1 M72B, underpunkt 5.4.b	
427.		Appen/plånboken rekommenderar att slutanvändaren tar i bruk enhetssäkerhet på miniminivå (skydd av telefon med pinkod eller en biometrisk mekanism för öppnande av telefon eller motsvarande).	LoA 2.1.1, punkt 2	Rekommenderad praxis
428.		Användaren informeras om bästa praxis som denne bör följa vid behandling av uppgifter som definierar identiteten.	LoA 2.1.1, punkt 2	Rekommenderad praxis
429.		Inga känsliga uppgifter bör sparas lokalt på mobilenheten. Uppgifterna bör däremot hämtas från servern vid behov och endast lagras i minnet.	LoA 2.4.6, punkt 1 M72B, underpunkt 5.4.b	
430.		Om känsliga uppgifter trots detta måste sparas lokalt ska de krypteras med en nyckel för datalager som baserar sig på enheten och som förutsätter användningen av en eller flera verifikationsfaktorer.	LoA 2.4.6, punkt 1 M72B, underpunkt 5.4.b	Principen är att minimera lagringen av känsliga uppgifter. En applikation av plånbokstyp sparar känsliga uppgifter, så detta kriterium bör tillämpas på appar av plånbokstyp.
431.		Appen/plånboken ska tas (verifikationsfaktorn) ur bruk efter fem misslyckade verifikationsförsök.	M72B, underpunkt 6.1.2	En fortsatt användning av appen förutsätter att en normal process för bevil-jande/aktivering följs.
432.		Om mängden återförsök inte kan kommuniceras till servern ska räknaren för nya försök som finns lokalt i appen/plånboken vara ändamålsenligt skyddad.	LoA 2.3.1, väsentlig, punkt 2 M72B, underpunkt 5.3.e–f	

C 3 Krypteringskrav

NR	TILLITSNIVÅ	KRITERIUM	MOTIVERING	Tilläggsinformation/kommentarer

433.		Appen/plånboken använder inte enbart symmetriska krypteringsmetoder och hårdkodade nycklar som krypteringsmetod.	M72B, underpunkt 5.3.g, M72B, punkt 7	
434.		Appen/plånboken använder krypteringsprimitiv som lämpar sig för olika användningstillfällen och som konstaterats vara bra.	M72B, underpunkt 5.3.g	
435.		Appen/plånboken använder vare sig krypteringsprotokoll eller algoritmer som är föråldrade eller som har konstaterats vara dåliga.	M72B, underpunkt 5.3.g M72B, punkt 7	
436.		Krypteringsprimitiven har konfigurerats enligt bästa praxis och kraven i bestämmelser (om sådana finns).	LoA 2.4.6, punkt 2 M72B, underpunkt 7.1.	
437.		Appen/plånboken använder inte samma krypteringsnycklar på nytt för andra ändamål.	LoA 2.4.6, punkt 1 8.1 § 4 punkten i autentiseringslagen	
438.		Den använda slumptalsgeneratorn är tillräckligt säker och högkvalitativ.	LoA 2.4.6, punkt 1 8.1 § 4 punkten i autentiseringslagen	
439.		En signaturräknare används av appen/plånboken, dvs. servern kan eventuellt upptäcka försök att klona appen.	LoA 2.3.1, väsentlig, punkt 2 LoA 2.3.1, hög	
440.		Appen/plånboken innehåller eller använder inga hårdkodade användarnamn eller lösenord.	LoA 2.4.6, punkt 1 LoA 2.3.1, punkt 2 M72B, punkt 6	Användarnamn under utvecklingsfasen (om sådana finns) ska rengöras från versioner som går till produktion. Inga hårdkodade användarnamn/hemligheter som ger tjänsteleverantören tillgång till appen. Eventuella aktiverings- och PUK-koder är engångsanvändbara och giltiga i en på förhand bestämd tid.
441.		Om appen har innehållit krypteringsprotokoll, identifikatorer och certifikat som varit svagare när appen utvecklats, har dessa lämnats bort från den version som ska användas inom produktionen.	LoA 2.4.6, punkt 1 och 3 LoA 2.4.6, hög M72B, underpunkt 5.3.g M72B, punkt 7	

C 4 Identifiering, identifieringsmetodens egenskaper och sessionshantering

I detta avsnitt används i tillämpliga delar standarden OWASP och avsnitt 4. Dessutom har ett antal kriterier förtecknats särskilt för identifieringsmetodens egenskaper.

NR	TILLIT SNIVÅ	KRITERIUM	MOTIVERING	Tilläggsinformation/kommentarer
442.		När appen/plånboken specificeras i registreringsskedet säkerställs det att appen binds till ägaren av identifieringsverktyget.	LoA 1 (definitioner), punkt 2 LoA 2.2.1, väsentlig, punkt 2	
443.		De hemligheter som genomför identifieringen är skyddade mot missbruk och endast tillgängliga på ett på förhand fastställt säkert sätt.	LoA 2.4.6, punkt 3 LoA 2.4.6, väsentlig M72B, underpunkt 6.4.2	T.ex. en privat nyckel.
444.		Hemligheter/autentiseringsnycklar är individuella.	M72B, underpunkt 5.3.g	
445.		De asymmetriska hemligheter som genomför identifieringen skapas i terminalutrustningen (nyckelpar, någon annan hemlig nyckel eller hemlighet).	M72B, underpunkt 5.3.g M72B, underpunkt 5.4.b	jfr RTS
446.		Om de hemligheter som genomför identifieringen skapas utanför enheten, levereras de till den använda enheten på ett säkert sätt.	LoA 2.4.6, punkt 2 LoA 2.4.6, väsentlig M72B, underpunkt 5.4.b	jfr RTS
447.		Om de hemligheter som genomför identifieringen skapas utanför enheten och levereras på ett säkert sätt till den enhet som använder dem, skapas förbindelsen mellan hemligheten och PID (personen/innehavaren) med enheten och endast vid registreringen.	LoA 2.3.1, punkt 2 LoA 2.2.1, väsentlig, punkt 2 M72B, underpunkt 6.3.	
448.		Identifieringen får inte enbart bygga på en delad hemlighet.	LoA 2.2.1, väsentlig, punkt 2	
449.		Vid formatering av en app binds hemligheterna till terminalutrustningen så att de inte kan användas i en annan enhet genom kopiering eller överföras till en annan enhet så att hemligheterna kan användas på enheten.	LoA 2.2.1, väsentlig, punkt 2 M72B, underpunkt 6.4.2	
450.		Appen/plånboken genomför enhetsbindningen utifrån enhetens fingeravtryck som skapats enligt flera unika egenskaper i enheten.	LoA 2.3.1, låg, punkt 3, väsentlig, punkt 2 M72B, underpunkt 6.1.	Appen/plånboken ska ta i bruk metoder/mekanismer för att binda enheten eller en mekanism som motsvarar enhetsbindningen. Detta kan dock vara problematiskt både för iOS- och Android-plattformerna då enhetens fingeravtrycksegenskaper används.
451.		Appen/plånboken får inte i något skede permanent spara identifikationsuppgifter/användarnamn (lösenord, PIN-koder, användarnamn osv.).	LoA 2.2.1, väsentlig, punkt 2 LoA 2.2.1, hög, punkt 2 LoA 2.3.1, väsentlig, punkt 2 LoA 2.3.1, hög, punkt 2 LoA 2.4.6, punkt 3	

452.		Appen/plånboken möjliggör pseudonymiserad identifiering.	M72B, underpunkt 12.3 (GDPR artikel 32)	Gäller appar av plånbokstyp eller skydd av identitet.
453.		Om appen/plånboken kan spara attribut som hämtats av tredje part eller som skapats av användaren, sparar appen/plånboken dem på ett säkert sätt.	LoA 2.4.6, punkt 1–2 M72B, underpunkt 6.1 och 9.1.1	Gäller appar av plånbokstyp.
454.		Om appen/plånboken möjliggör tillägg av attribut från tredje part så hämtas de med säker praxis och framställning.	LoA 2.4.6, punkt 1–2 M72B, underpunkt 6.1 och 9.1.1	Gäller appar av plånbokstyp.
455.		En app/plånbok som sparar attribut lokalt säkerställer hemligheten hos attributen och deras integritet med säkerhetselement.	LoA 2.4.6, punkt 1–2	Antingen i själva säkerhetselementet eller genom att använda en nyckel som säkerhetselementet skyddar.
456.		Om man med hjälp av appen/plånboken visar attribut direkt till förlitande part, genomför appen/plånboken både överföringen och framställningen med säker praxis, ett sätt som tryggar identiteten och i ett säkert format.	LoA 2.4.6, punkt 1–2 M72B, underpunkt 6.1 och 9.1.1	Gäller appar av plånbokstyp.
457.		Om appen/plånboken tillåter användaren att uppvisa attribut direkt till den förlitande parten ska appen/plånboken i en säker källa verifiera att den förlitande parten har rätt att ta emot dessa attribut.	[eIDAS2] LoA 2.4.6, låg, punkt 3	Gäller appar av plånbokstyp.
458.		Om appen/plånboken upptäcker att den förlitande parten begär information som den inte har rätt till varnar appen tydligt slutanvändaren om att attribut utanför den förlitande partens rättigheter delas.	[eIDAS2] LoA 2.4.6, låg, punkt 3	Gäller appar av plånbokstyp.
459.		Om appen/plånboken skickar meddelanden till servern där valideringen av meddelandena i bakänden leder till identifiering, ska meddelandena skickas på ett säkert sätt genom att använda aktuella och godkända krypteringssätt (t.ex. Mutual/2-way TLS 1.2 eller senare version).	LoA 2.4.6, punkt 2 M72B, underpunkt 5.3.g M72B, underpunkt 7.1.1, underpunkterna 1–4	
460.		Om personuppgifter byts mellan appen/plånboken och servern, skyddas uppgifterna även genom kryptering på meddelandenivå.	LoA 2.4.6, punkt 2 LoA 2.4.6, väsentlig M72B, underpunkt 5.3.g	
461.		Om appen/plånboken bygger på en metod baserad på engångslösenord eller den innehåller en komponent som bygger på en sådan metod, ska lösningar som har	M72B, underpunkt 5.3.g	

		konstaterats vara bra och som bygger på standarder användas vid skapandet av engångslösenord (OTP).		
462.		För lagring av hemligheter som används vid identifiering används om möjligt tjänster som tillhandahålls av plattformen i en terminalbaserad säker miljö.	M72B, underpunkt 5.3.c M72B, underpunkt 5.4.b	Säkerhetselement (SE, secure element), pålitlig drivmiljö (TEE, trusted execution environment) osv. Appen/plånboken ska basera sig på en riskbedömning. Om riskbedömningen visar att säkerhetselementet inte behöver användas kan man för att spara hemligheten/hemligheterna även använda andra lösningar. Grunderna till avvikelsen ska lämnas in tillsammans med inspektionsberättelsen (som en del av riskbedömningen).
463.		Information om felaktiga indata skickas till servern varje gång. Servern följer upp mängden felaktiga indata och appen låser sig automatiskt efter X felaktiga indata. Om internetuppkoppling saknas och meddelandena inte kan skickas till servern på ett säkert sätt, följer appen själv samma logik. (PSD2: regeln om fem fel)	LoA 2.4.6, punkt 1 M72B, underpunkt 5.3.f	jfr RTS och SCA
464.		Mellan appen/plånboken och servern används tekniker som kan förhindra replay-angrepp och nonce vid: Bounded Probability of a Birthday Collision.	LoA 2.3.1, väsentlig, punkt 2 LoA 2.3.1, hög	
465.		Vid användning av sessionsidentifikatorer används slumpmässiga sessionsidentifikatorer.	LoA 2.3.1, väsentlig, punkt 2 LoA 2.3.1, hög	
466.		(Programvara/OAuth) Vid lösningar med token-baserad teknik säkerställs att token har signerats med en godkänd säker algoritm.	LoA 2.4.6, punkt 2 M72B, underpunkt 7.1.1, underpunkt 2	
467.		En sessions eller tokens giltighetstid fastställs i bakänden.	LoA 2.4.6, punkt 1 och 4	
468.		I (identifierings)bakänden fastställs behörighetspolicyer utifrån vilka beviljas åtkomst till målappen/tjänsten.	LoA 2.4.6, punkt 1 och 4	
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 använda-	LoA 2.2.1, väsentlig, punkt 1	T.ex. Apple iOS, biometri För en stark identifieringsmetod behövs inte alla tre faktorer utan det räcker med två, om man kan verifiera att faktorerna är oberoende av varandra och att de är

		ren kan specificeras på ett tillförlitligt sätt (t.ex. terminalutrustning = administration, pinkod för hemlighet = information och fingeravtryck = egenskap).		bundna till innehavaren av identifieringsverktyget.
470.		Om en biometrisk autentiseringsfaktor används och registrerade personer inte kan skiljas åt på grund av plattformens egenskaper, ska användaren ges tydliga instruktioner i att ta bort de övriga personernas biometriska identifikatorer/hemligheter som tillhör de övriga användarna av enheten.	LoA 2.2.1, väsentlig, punkt 1 LoA 2.1.1, punkt 2 LoA 1 (definitioner), punkt 2	LoA 2.1.1. Ingår inte i autentiseringslagen; upptäckts vara god praxis.
471.		Om appen/plånboken tillåter specificering av nya kompletterande autentiseringsfaktorer eller byte av autentiseringsfaktorer, skickas denna information även till bakänden. Byte och tillägg kräver alltid identifiering åtminstone på samma nivå som den nivå som den nya kombinationen möjliggör. Kombinationerna ska dokumenteras och bedömas som enskilda helheter.	LoA 1 (definitioner), punkt 2 LoA 2.2.1, väsentlig, punkt 2 LoA 2.2.4, väsentlig	Autentiseringsfaktorernas oberoende ska säkerställas. Det innebär till exempel byte av autentiseringsfaktor i en kategori eller tillägg av en ny autentiseringsfaktor i en kategori, varvid det används autentiseringsfaktorer från tre kategorier. Syftet är att ge användaren möjlighet att välja verifieringsfaktorer men samtidigt att säkerställa att identifieringstjänsten hela tiden kan sörja för deras säkerhet.
472.		Vid flerfaktorsautentisering (multi-factor, strong authentication) används en faktor som utgår från användarens uppgift (lösenord, pinkod) eller egenskap (fingeravtryck, ansikte, iris) för att öppna den hemlighet som själva begäran om identifiering besvaras med.	LoA 1 (definitioner), punkt 3 LoA 2.2.1, väsentlig, punkt 2 LoA 2.3.1, väsentlig, punkt 2	
473.		Vid genomförande av en biometrisk autentiseringsfaktor används endast gränssnitt som tillhandahålls av plattformen.	LoA 2.4.6, punkt 1 M72B, underpunkt 5.3.c	Särskilt användningsfall: Att läsa chipset på passet/identitetskortet med NFC. Även i detta fall ska man använda gränssnitt som tillhandahålls av plattformen.
474.		Vid utnyttjande av en biometrisk faktor överförs själva biometriska inspelningen (fingeravtrycket, ansiktsfotot, den skannade bilden på irisen) inte från appen/plånboken någon annanstans i identifieringstransaktionen.	LoA 2.2.1, väsentlig, punkt 2 LoA 2.3.1, väsentlig, punkt 2	
475.		Känsliga uppgifter eller personuppgifter som används i registreringsskedet kan endast med säkra metoder överföras till bakänden för bedömning.	LoA 2.4.6, punkt 2	
476.		Användaren ska ha möjlighet att tillfälligt spärra en hemlighet i a) en enhet, b) flera enheter eller c) alla enheter på en gång.	LoA 2.2.3, väsentlig, punkt 1	

477.		För att en tillfälligt spärrad hemlighet ska kunna öppnas krävs det alltid identifiering på minst samma nivå som den nivå som används när appen/plånboken tas i bruk.	LoA 2.2.3, väsentlig, punkt 3	
478.		Användaren ska ha möjlighet att på ett säkert sätt inaktivera identifieringsappen och hemligheten i a) en enhet, b) flera enheter eller c) alla enheter.	LoA 2.2.3, väsentlig, punkt 1 och 2	
479.		Det ska vara möjligt att tillfälligt spärra och inaktivera hemligheter i enskilda enheter även i bakänden.	LoA 2.2.3, väsentlig, punkt 1 och 2	
480.		Identifieringen binds till önskad transaktion eller webbläsarsession, det vill säga identifieringsappen visar på ett tydligt sätt information om vad som sker.	LoA 2.3.1, väsentlig, punkt 2	T.ex. RTS, dynamisk länkning. (EU) 2018/389. I PSD2-regelverket uppställs mera detaljerade krav på dynamisk länkning. Dessa krav ska iakttas då man vill använda identifieringsappen för både allmän identifiering och identifiering vid betalning.
481.		Identifieringsappen/plånboken genomför även så kallad binding message där användaren får möjlighet att på ett begripligt sätt länka identifieringen i mobilenheten exempelvis med en webbläsarsession.	LoA 2.3.1, väsentlig, punkt 2, M72B, underpunkt 6.2.1	Det används ett sådant språk som hjälper användaren förstå vilken session meddelandet gäller.
482.		Identifieringsappen/plånboken visar alltid namnet på den tjänst/app där användaren identifierar sig med attributet sp_name. Den här informationen ska finnas synlig för användaren i ett lättförståeligt format.	M72B, underpunkt 6.2.2	Språket ska vara tydligt så att det inte misstas som ett meddelande som gäller sessionen.
483.		Om identifieringsappens svar bygger på en asymmetrisk signatur, används principen WYSIWYS, dvs. den information som visas för användaren är också information som ska signeras.	LoA 2.3.1, väsentlig, punkt 2	
484.		Appen/plånboken styr användaren att välja starka pinkoder.	LoA 2.1.1, väsentlig, punkt 2 M72B, underpunkt 5.3.g	LoA 2.1.1, ingår inte i autentiseringslagen; upptäckts vara god praxis.
485.		Appen/plånboken godtar inte pinkoder som kan gissas lätt och inte heller andra hemligheter som bygger på användarens minne.	LoA 2.3.1, väsentlig, punkt 2 LoA 2.4.6, punkt 1	T.ex. svaga PIN-koder eller PIN-koder som är enkla att gissa, såsom 000000, 123456, 999999 osv. godkänns inte.
486.		Användarens indata, till exempel pinkoder, valideras på ett säkert sätt.	LoA 2.3.1, väsentlig, punkt 2 M72B, underpunkt 5.4.b	

487.		Om appen/plånboken utnyttjar terminalutrustningens säkerhetsegenskaper på hårdvarunivå, exempelvis TEE/SE eller motsvarande, meddelar appen den använda komponenten på hårdvarunivå och eventuell övrig information till (tillhandahållarens) server i anslutning till formateringen så att servern kan upptäcka sårbarheter i det använda systemet på hårdvarunivå och svara på dessa (även i fortsättningen).	LoA 2.4.6, punkt 1 och 4 M72B, underpunkt 5.4.d	CVE-2018-11976 → Servern ges möjlighet att reagera på kända sårbarheter i komponenter på hårdvarunivå.
488.		Om bakgrundssystemet eller den förlitande parten upptäcker en falsk app/plånbok stoppas framskridandet av identifieringen. Verifieringen av appen/plånboken ska alltså ske i själva appen och verifieringen ska vid behov valideras innan identifieringsbegäran framskrider.	LoA 2.4.6, punkt 1 och 3 LoA 2.3.1, väsentlig, punkt 1	ANMÄRKNING: tillägg 19.05.2023.
489.		Appen/plånboken och/eller bakgrundssystemet säkerställer att det på en gång inte kan finnas flera aktiva begäran om identifiering, alltså den tidigare begäran ska slopas/stängas innan en ny begäran inleds.	LoA 2.3.1, väsentlig, punkt 2	

C 5 Datakommunikation

NR	TILLITSNIVÅ	KRITERIUM	MOTIVERING	Tilläggsinformation/kommentarer
490.		Nättrafiken mellan appen/plånboken och servern är skyddad med internationellt eller nationellt rekommenderade protokoll, och de skyddade kanalerna används i appen/plånboken på ett enhetligt sätt.	LoA 2.4.6, punkt 2 M72B, underpunkt 5.3.g	Några krypteringskrav har inte fastställts för *interna* förbindelser i identifieringssystem. Utgångspunkten kan dock anses vara de krypteringsprotokoll för datakommunikation *mellan leverantörer* som avses i punkt 7 i M72B.
491.		Appen/plånboken kontrollerar inställningarna/konfigurationen i krypteringsprotokollet TLS (eller motsvarande) och säkerställer att de följer god praxis.	LoA 2.4.6, punkt 2 M72B, underpunkt 5.3.g, 7.1.3 och 7.2	Några krypteringskrav har inte fastställts för *interna* förbindelser i identifieringssystem. Utgångspunkten kan dock anses vara de krypteringsprotokoll för datakommunikation *mellan leverantörer* som avses i punkt 7 i M72B.
492.		Appen/plånboken låser terminalens certifikat eller offentliga nyckel och bildar inte en anslutning till terminaler med annat certifikat eller annan nyckel även om	LoA 2.4.6, punkt 2	

		det är undertecknat av en pålitlig certifikatutfärdare (Certificate Authority).		
493.		I kritiska funktioner, såsom formatering och skapande av hemligheter för enskilda användare, använder appen/plånboken inte osäkra kommunikationskanaler (till exempel e-post, sms).	LoA 1 (definitioner), punkt 2 LoA 2.2.1, väsentlig, punkt 2	I praktiken ska personifieringen i appen bygga på stark elektronisk autentisering.
494.		Appen/plånboken använder endast uppdaterade programbibliotek för att genomföra förbindelserna och informationssäkerheten.	LoA 2.4.6, punkt 1 och 4	

C 6 Interaktion mellan plattform och app

NR	TILLIT SNIVÅ	KRITERIUM	MOTIVERING	Tilläggsinformation/kommentarer
495.		Appen/plånboken begär endast de behörigheter som den behöver av terminalutrustningen.	LoA 2.4.6, punkt 1 M72B, underpunkt 5.3.c	
496.		All indata som kommer från externa källor kontrolleras och renas.	LoA 2.4.6, punkt 4 M72B, underpunkt 5.3.c	
497.		Vid användning av ett separat URL-schema eller IPC-mekanismer överförs information inte utanför appen/plånboken.	LoA 2.4.6, punkt 2 M72B, underpunkt 5.3.c	
498.		Om det är nödvändigt att visa information via webbläsaren (t.ex. val av metoder i identifieringsservern) i appen/plånboken används i första hand operativsystemets trygga egenskaper (se bästa praxis för närvarande för varje leverantör av operativsystemen). WebView används endast om det inte finns något tryggare alternativ. I använda komponenter används endast nödvändiga protokoll och de övriga spärras eller det säkerställs att dessa inte är tillgängliga.	LoA 2.4.6, punkt 1 M72B, underpunkt 5.3.c	
499.		Utgångspunkten är att JavaScript inte är tillgängligt i webbläsarkomponenterna.	LoA 2.4.6, punkt 1 M72B, underpunkt 5.3.c	
500.		Om det används komponenter som genomför webbläsarfunktionen tillåter deras konfiguration endast https-anslutning.	LoA 2.4.6, punkt 1 M72B, underpunkt 7.1–2 och 9.3	
501.		De ursprungliga metoderna har förhindrats om programversionen av plattformen har konstaterats vara sårbar.	LoA 2.4.6, punkt 1 M72B, underpunkt 5.3) och 5.4.d	I fråga om JavaScript kan till exempel genomförandet av en äldre version av operativsystemet Android vara oskyddat.

502.		Om de ursprungliga metoderna i appen/plånboken är öppna för webbläsarkomponenter, säkerställs det att endast JavaScript som ingår i applikationspaketet får aktiveras.	LoA 2.4.6, punkt 1 M72B, underpunkt 5.3.c	
503.		Webbläsarkomponenternas åtkomst till lokala resurser är förbjuden/förhindrad.	LoA 2.4.6, punkt 1 M72B, underpunkt 5.3.c)	
504.		Vid serialisering av objekt används skyddade API.	LoA 2.4.6, punkt 1 och 3 LoA 2.4.6, väsentlig M72B, underpunkt 5.3.c	
505.		Appen/plånboken skyddar sig själv mot attacker som baserar sig på ett fönster som döljer andra (overlay attack).	LoA 2.4.6, punkt 1	Riskhanteringsmetoderna för attacker av overlay-typ beror på den plattform som används och de möjligheter denna erbjuder. T.ex. kan risken från och med Android API-version 9 redan delvis hanteras. Appen/plånboken utnyttjar i fullo de säkerhetskontroller som plattformen erbjuder.
506.		Webbläsarkomponentens cacheminne, datalager och laddade resurser raderas innan webbläsarkomponenten förstörs.	LoA 2.4.6, punkt 1 och 3 M72B, underpunkt 5.4.b	
507.		Säkerställs att appen/plånboken förhindrar användningen av tredje parters tangentbord vid inmatning av känslig information.	LoA 2.4.6, punkt 1–2	Undantag är t.ex. de fall där användningen av tredje parters tangentbord är en förutsättning för användningen av identifieringsappen. Dessa ska separat identifieras och dokumenteras.

C 7 Programvarukodens säkerhet, kvalitet och utvecklingsmiljö

NR	TILLIT SNIVÅ	KRITERIUM	MOTIVERING	Tilläggsinformation/kommentarer
508.		Appen/plånboken har signerats och levererats med ett giltigt och tillförlitligt certifikat och den privata nyckeln har skyddats på ändamålsenligt sätt.	LoA 2.4.6, punkt 1	
509.		Appen/plånboken har tagits fram i release mode, det vill säga så att till exempel felsökning är svårare.	LoA 2.4.6, punkt 1 M72B, underpunkt 5.3.c	
510.		Vid utvecklingen av appen/plånboken används enbart god informationssäkerhetspraxis för programutveckling/kodning.	LoA 2.4.6, punkt 1 M72B, underpunkt 5.3.c	All JavaScript som används ska exempelvis kodas och renas i syfte att minska XSS-angreppsrisken.

511.		Symbolerna för felsökning har tagits bort från det binära talsystemet.	LoA 2.4.6, punkt 1 M72B, underpunkt 5.3.c	
512.		Felsökningskoden och felsökningsmeddelandena har tagits bort.	LoA 2.4.6, punkt 1 M72B, underpunkt 5.3	
513.		Inställningar under testning eller utveckling, insamling av loggar (verbose logging) och konfigurationer har raderats från den publicerade versionen.	LoA 2.4.6, punkt 1 och 4 M72B, underpunkt 5.3.c och 5.4.d	
514.		Samtliga tredje parts komponenter som används av appen/plånboken har identifierats och de kontrolleras regelbundet för kända sårbarheter.	LoA 2.4.6, punkt 4 M72B, underpunkt 5.4.d	
515.		Appen/plånboken upptäcker avvikelser och behandlar dem på ett ändamålsenligt sätt.	LoA 2.4.6, punkt 4 M72B, underpunkt 5.3.f och 5.4.d	
516.		Appen/plånboken eller servern minimerar informationen i felmeddelanden.	LoA 2.4.6, punkt 1 M72B, underpunkt 5.3.c	
517.		Utgångspunkten är att felbehandlingen vid säkerhetskontroller förhindrar åtkomst i felsituationer.	LoA 2.4.6, punkt 1 M72B, underpunkt 5.3.c	
518.		Minnet reserveras, används och frigörs på ett säkert sätt.	LoA 2.4.6, punkt 1 M72B, underpunkt 5.3.c	
519.		De informationssäkerhetsegenskaper som tillhandahålls av plattformen/utvecklingsmiljön är tillgängliga.	LoA 2.4.6, punkt 1 M72B, underpunkt 5.3.c	

C 8 Säkerhetskontroller och skydd (EN Resilience)

NR	TILLIT SNIVÅ	KRITERIUM	MOTIVERING	Tilläggsinformation/kommentarer
520.		Appen/plånboken använder flera skyddsmekanismer som presenteras i detta avsnitt.	LoA 2.4.6, punkt 1	Programvarans kapacitet att skydda mot angrepp ska bedömas som helhet.
521.		Appen/plånboken har fler än en funktion som försöker upptäcka enheter som används av tredje part eller är rotade.	LoA 2.4.6, punkt 4 M72B, underpunkt 5.3.f	
522.		Iakttagelsemekanismerna skapar olika slags reaktioner, bl.a. fördröjda och dolda reaktioner.	LoA 2.4.6, punkt 4 M72B, underpunkt 5.3.f och 6.1	
523.		Appen/plånboken skickar ett meddelande till genomförandet i bakänden när den har upptäckt en enhetsplattform som har rotats till en drivmiljö eller som används av tredje part, eller kan själv fastställa vad som	LoA 2.4.6, punkt 4 M72B, underpunkt 5.3.f	

		ska göras när miljön är rotad eller används av tredje part.		
524.		Appen/plånboken försöker förhindra försök till felsökning och reagerar om den upptäcker att en lösning som används för felsökning har anslutits till appen. Detta ska täcka all tillgänglig praxis för att korrigera fel.	LoA 2.4.6, punkt 1 M72B, underpunkt 5.3.c	
525.		Appen/plånboken upptäcker och reagerar om filer eller kritiska data/filer i appens drivmiljö (sandlåda) förändras under nedladdningen.	LoA 2.4.6, punkt 4 M72B, underpunkt 5.3.f	
526.		Appen/plånboken upptäcker och reagerar på allmänt tillämpade verktyg som försöker utreda källkoden för appen (reverse engineering).	LoA 2.4.6, punkt 4 M72B, underpunkt 5.3.f	
527.		Appen/plånboken upptäcker och reagerar om den används i en emulator.	LoA 2.4.6, punkt 4 M72B, underpunkt 5.3.f	
528.		Appen/plånboken upptäcker och reagerar på ett ändamålsenligt sätt när den har upptäckt förändringar/manipulation i minnesutrymmet.	LoA 2.4.6, punkt 4 M72B, underpunkt 5.3.f	
529.		Lösningar som är viktiga/relevanta för appen/plånboken är i tillämpliga delar krypterade på informationssystemnivå. Sådana lösningar kan inte dekrypteras genom analyser.	LoA 2.4.6, punkt 1 och 3 LoA 2.4.6, väsentlig M72B, underpunkt 5.3.c och 5.4.b	
530.		Kryptering på applikationsnivå av nyttolasten tillämpas.	LoA 2.4.6, punkt 1–4 M72B, underpunkt 5.3.g	

Källor

Kriterier som denna anvisning baserar sig på:

Autentiseringslagen – lagen om stark autentisering och betrodda elektroniska tjänster (617/2009)

LoA – Kommissionens genomförandebeslut (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

M72B – Föreskrift om elektroniska identifieringstjänster och betrodda elektroniska tjänster (M72B/2022) https://www.kybertur-vallisuuskeskus.fi/sv/var-verksamhet/reglering-och-tillsyn/elektronisk-identifiering

OWASP - OWASP Mobile Application Security Verification Standard, MASVS version 1.4.2