

Anvisning om bedömning av elektroniska identifieringstjänster

Transport- och kommunikationsverkets anvisning

211/2019 O

UTKAST 20.6.2019

Innehåll

1	Inledning	7
1.1	Syftet med anvisningen	7
1.2	Anvisningens ikraftträdande	9
1.3	Hänvisningar till standarder och bestämmelser samt förkortningar	11
1.4	Definitioner av identifieringstjänster	13
1.5	Tjänsteleverantörers allmänna tillförlitlighet ingår inte i kriterierna.....	14
2	Bedömning av en identifieringstjänst samt inspektionsberättelse	16
2.1	Inlämnande av inspektionsberättelsen som bilaga till anmälan.....	16
2.1.1	Anmälan om inledande av verksamhet	17
2.1.2	Anmälan om ändring av verksamhet	18
2.1.3	Periodisk bedömning	18
2.2	Delområden som ska bedömas i identifieringstjänster.....	20

2.3	Identifieringsmetod, identifieringssystem och underleverantörer	23
2.3.1	Definitioner	23
2.3.2	Bedömning	25
2.3.3	Inspektionsberättelse: Beskrivning av vilken del av identifieringsmetoden och/eller identifieringssystemet bedömningen omfattar	27
2.3.4	Inspektionsberättelse: Namn (alla) på den identifieringstjänst som är föremål för bedömning ...	28
2.3.5	Inspektionsberättelse: Beskrivning av identifieringsmetoden (identifieringsverktyget)	28
2.3.6	Inspektionsberättelse: beskrivning av identifieringssystemet (systemarkitekturen).	29
2.4	Uppgifter om bedömningsorganet	31
2.4.1	Inspektionsberättelse: Bedömningsorganets identifierings- och kontaktuppgifter	32
2.4.2	Inspektionsberättelse eller anmälan: Bedömningsorganets kompetens och oberoende.....	32
2.5	Genomförande av bedömningen.....	35
2.5.1	Inspektionsberättelse: Tidpunkt för bedömning och bedömningens längd enligt personarbetstiden35	
2.5.2	Inspektionsberättelse: Bedömningsmetoder	35
2.5.3	Uppgifter om den dokumentation som har använts vid bedömningen av överensställelsen. ...	36
2.6	Proportionalitet mellan bedömning och tillitsnivå respektive risker.....	37
2.7	Inspektionsberättelsens noggrannhet	41
2.8	Rapportering av avvikelser i inspektionsberättelsen	42

3	Delområden som ska bedömas	43
3.1	Identifieringsmetodens egenskaper och autentiseringsmekanism	44
3.2	Interoperabilitet	45
3.3	Tekniska krav på informationssäkerhet	46
3.4	Förmåga att observera avvikelser, hantering av avvikelser och störningsanmälningar.....	48
3.5	Lagring och behandling av uppgifter	49
3.6	Säkerhet i anläggningar	50
3.7	Tillräckliga och kvalificerade personalresurser.....	51
3.8	Ledning avseende informationssäkerhet.....	52
3.9	Styrkande och kontroll av identitet hos sökande av identifieringsverktyg (inledande identifiering)	53
3.10	Identifieringsverktygs, eller identifieringsmetoders, livscykel	58
4	BILAGA A: Minneslista om anvisningen om inspektionsberättelse	59
5	BILAGA B: Allmänna kriterier för bedömning av identifieringstjänster	62
5.1	Identifieringsmetodens egenskaper och autentiseringsmekanism	62

5.2	Interoperabilitet.....	79
5.3	Tekniska krav på informationssäkerhet	87
5.3.1	Datakommunikationssäkerhet	89
5.3.2	Säkerhet i informationssystem	99
5.3.3	Säkerhet i användning.....	107
5.4	Förmåga att observera avvikelser, hantering av avvikelser och störningsanmälningar.....	113
5.5	Lagring och behandling av uppgifter	124
5.6	Säkerhet i anläggningar	136
5.7	Tillräckliga och kvalificerade personalresurser.....	139
5.8	Ledning avseende informationssäkerhet.....	141
5.9	Styrkande och kontroll av identitet hos sökande av identifieringsverktyg (inledande identifiering)	148
5.10	Identifieringsverktygs, eller identifieringsmetoders, livscykel	161
6	BILAGA C Särskilda kriterier gällande lösningar för mobilidentifiering	172
6.1	Arkitektur, planer och modeller för hotbilder.....	172
6.2	Lagring av information samt dataskydd.....	174

6.3	Krypteringskrav	177
6.4	Identifiering, identifieringsmetodens egenskaper och sessionshantering.....	179
6.5	Datakommunikation	186
6.6	Interaktion mellan plattform och app.....	187
6.7	Programvarukodens säkerhet, kvalitet och utvecklingsmiljö.....	189
6.8	Säkerhetskontroller och skydd (EN: Resilience).....	191

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

Anvisning

211/2019 O
x.x.2019

8 (192)

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-förordning¹. 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 (214/2016 O). Bestämmelser om bedömning av överensstämmelse med kraven hos sådana system

¹ Europaparlamentets och rådets förordning (EU) nr 910/2014 av den 23 juli 2014 om elektronisk identifiering och betrodda tjänster för elektroniska transaktioner på den inre marknaden och om upphävande av direktiv 1999/93/EG.

Anvisning

211/2019 O
x.x.2019

9 (192)

för elektronisk identifiering som ska anmälas till EU ingår i eIDAS-förordningen och förordningen om tillitsnivåer vid elektronisk identifiering (LOA)².

1.2 Anvisningens ikraftträdande

Anvisningen 211/2019 O träder i kraft x.x.2019.

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> och <https://www.traficom.fi/sv/foreskrifter>

Version	Datum	Beskrivning/ändring	Författare
---------	-------	---------------------	------------

² Kommissionens genomförandeförordning (EU) 2015/1502 av den 8 september 2015 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 (Text av betydelse för EES).

Anvisning

211/2019 O
x.x.2019

10 (192)

211/2019 O	x.x.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 av identifieringstjänster	2.11.2016	De första publicerade versionerna	Kommunikationsverket, Cybersäkerhetscentret

215/2016 O Be- rättelser för be- dömning av iden- tifieringstjänster och betrodda tjänster			
---	--	--	--

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*).

Anvisning

211/2019 O
x.x.2019

12 (192)

- Kommissionens genomförandeförordning (EU) 2015/1502³ (nedan *LOA* eller *förordningen om tillitsnivåer*)
 - Hänvisningar i autentiseringslagen till förordningen om tillitsnivåer
 - LOA guidance, en inofficiell tillämpningsguide för förordningen om tillitsnivåer⁴
- Kommunikationsverkets föreskrift 72A/2018 M (nedan *M72*)
 - Genom föreskriften preciseras vissa krav som fastställs i autentiseringslagen

Hänvisningar till standarder⁵:

- ISO/IEC 27001:2013 Information security management

³ https://eur-lex.europa.eu/legal-content/SV/TXT/?uri=OJ%3AJOL_2015_235_R_0002 Kommissionens genomförandeförordning har utfärdats med stöd av EU:s så kallade eIDAS-förordning (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)

⁴ https://www.kyberturvallisuuskeskus.fi/sites/default/files/media/file/LOA_Guidance_Final_suomeksi.pdf

⁵ Följande dokument har också använts som bakgrundsmaterial vid beredningen av kriterierna: FIDO Security Reference: <https://fidoalliance.org/specs/fido-v2.0-id-20180227/fido-security-ref-v2.0-id-20180227.html>

- 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.1.1.3⁶

Förkortningar av tillitsnivåerna i tabellerna

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

1.4 Definitioner av identifieringstjänster

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

En leverantör av identifieringsverktyg tillhandahåller slutanvändare elektroniska identifieringsverktyg.

⁶ https://www.owasp.org/index.php/OWASP_Mobile_Security_Testing_Guide

Anvisning

211/2019 O
x.x.2019

14 (192)

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*.

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 § i föreskrift 72.

Anvisning

211/2019 O
x.x.2019

15 (192)

Uppgifter som ska lämnas till Transport- och kommunikationsverket tillsammans med anmälningar om inledande, upphörande eller ändring av verksamhet beskrivs närmare i anvisningen **214/2016 O Anmälningar om identifieringstjänster och betrodda tjänster**.

BESTÄMMELSER

M72: 16 § Utredning om att övriga krav är uppfyllda

Leverantören av en identifieringstjänst ska, antingen genom en egen skriftlig utredning eller genom en kvalitetsrevision enligt 15 §, visa att följande krav på tillförlitlighet hos leverantörer av identifieringstjänster och uppgifter om identifieringstjänsten är uppfyllda:

- 1) offentliggjorda meddelanden och användaruppgifter (t.ex. identifieringsprinciper, avtalsvillkor och prislistor)
- 2) en etablerad organisation
- 3) förmåga att ta skaderisker
- 4) tillräckliga ekonomiska resurser
- 5) ansvar för underleverantörer
- 6) en plan för verksamhetens upphörande.

2 Bedömning av en identifieringstjänst samt inspektionsberättelse

2.1 Inlämnande av inspektionsberättelsen som bilaga till anmälan

BESTÄMMELSER

Autentiseringslag (23.11.2018/1009): 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.

Autentiseringslag: 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.

Autentiseringslag: 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.

2.1.3 Periodisk bedömning

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

Anvisning

211/2019 O
x.x.2019

19 (192)

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 Transport- och kommunikationsverket har godkänt inspektionsberättelsen. Leverantören av identifieringstjänster ska lämna en ny inspektionsberättelse till ämbetsverket två år efter att den föregående inspektionsberättelsen godkänts om leverantören vill fortsätta att tillhandahålla tjänster för stark autentisering.

Revisionsberättelsen 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 godkänts.

Bestämmelserna om bedömningsskyldighet i autentiseringslagen trädde i kraft den 1 juli 2016. Enligt övergångsbestämmelsen skulle inspektionsberättelsen lämnas till Kommunikationsverket senast den 31 januari 2017. Ämbetsverket har offentliggjort en anvisningspromemoria om de nya bedömningar som gjordes 2019 (dnr 1003/620/2018 *Tolkningspromemoria 12/2018 Anvisning om bedömning av överensstämmelsen hos identifieringstjänster 2019*).

Minimiuppsättningen uppgifter i anmälningar om inledande eller ändring av verksamhet finns beskriven i Kommunikationsverkets anvisning 214/2016 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 72.

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 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)–1d) och 2g) gäller **tjänster för identifieringsförmedling**.

BESTÄMMELSER

Autentiseringslag: 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.

[...]

Autentiseringslag: 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,

[...]

M72: 15 § Kriterier för kvalitetsrevision

Kvalitetsrevisioner av identifieringstjänster ska omfatta krav på

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

- a) *ledning avseende informationssäkerhet*
- b) *registerföring*
- c) *anläggningar och personal*
- d) *tekniska åtgärder*

2) *identifieringsmetod, dvs. identifieringsverktyg*

- a) *ansökan och registrering*
- b) *styrkande och kontroll av den sökandes identitet*
- c) *identifieringsmetodens egenskaper och utformning*
- d) *utfärdande, leverans och aktivering*
- e) *upphävande, återkallelse och återaktivering*
- f) *förnyelse och ersättning*
- g) *autentiseringsmekanismer.*

Kvalitetsrevisionerna av de delområden som anges i 1 mom. ska bygga på kraven i autentiseringslagen och denna föreskrift, bestämmelser eller guider 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.

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

Autentiseringslag: 2 §

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

Jfr 8 § Krav på system för elektronisk identifiering i autentiseringslagen

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

eIDAS-förordning: artikel 3

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

Autentiseringslag: 13 §

[...]

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

2.3.2 Bedömning

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.

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.

Anvisning

211/2019 O
x.x.2019

26 (192)

Hänvisningarna till ISO/IEC 27001:2013 om underleverantörer har inte angetts separat i tabellen om bedömningskriterier. I en bedömning enligt ISO-standarderna av ledningen av informationssäkerheten behandlas underlevens överlag i punkten A.15.1 Informationssäkerhet i leverantörsrelationer (*Information security in supplier relationships*).

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?

Anvisning

211/2019 O
x.x.2019

27 (192)

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 relaterad till de ovannämnda.

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.

- 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

Autentiseringslag (29.6.2016/533): 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 18 § eller 19 § i M72).

Autentiseringslag (23.11.2018/1009): 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 och betrodda tjänster.

[...]

M72: 18 § Krav på utomstående organ för bedömning av identifieringstjänster

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 jämförbara bestämmelser, anvisningar eller standarder för allmän ledning avseende informationssäkerhet eller sektorspecifik reglering eller standardisering.

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 1 mom. gäller identifieringssystem.

M72: 19 § Krav på interna organ för kontroll av identifieringstjänster

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) ISACAs 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 jämförbara standarder för myndighetsreglering eller allmän hantering av oberoende intern kontroll.

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 1 mom. riktas till 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.

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.

2.6 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.

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.

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

Alla angrepp kan inte helt förhindras med de autentiseringsmekanismer som används vid autentiseringen, utan mekanismerna kan endast användas på en viss säkerhets- eller tillitsnivå. Ett vanligt sätt att mäta den skyddsgrad som olika mekanismer ger är att rangordna mekanismerna utgående från hur bra skydd de ger mot angripare med viss angreppspotential (dvs. angriparens kraft).

De termer som används för angreppspotential på de olika tillitsnivåerna är "förhöjd/grundläggande" (enhanced-basic), "måttlig" (moderate) och "hög" (high). Dessa termer 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". Texten i standarderna kan läsas fritt på www.commoncriteriaportal.org/cc (CCPART1-3 motsvarar standarden ISO/IEC 15408 och CEM standarden ISO/IEC 18045).

ISO/IEC 15408-1 defines "attack potential – measure of the effort to be expended in attacking a [mechanism], expressed in terms of an attacker's expertise, resources and motivation".

Annex B.4 of ISO/IEC 18045 / CEM contains Guidance on how to calculate the attack potential necessary to exploit a given weakness of an authentication mechanism.

För att de uppställda kraven i genomförandeförordningen ska kunna uppfyllas krävs det en bedömning av skyddskapaciteten mot potentiella angrepp.

Vid bedömningen bör hänsyn tas till relevanta hot. I ISO 29115 nämns följande: gissningar på och utanför nätet, kopiering av identifieringsuppgifter, nätfiske, tjuvlyssning, replay-angrepp, sessionskapning, man-i-mitten-attacker, stöld av identifieringsuppgifter, spoofing-angrepp och olaga identitetsanvändning.

Anvisning

211/2019 O
x.x.2019

40 (192)

Vid bedömningen av skyddskapaciteten finns det skäl att beakta hela autentiseringsmekanismen och även riskerna till följd av autentisering av innehavaren av medlet 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 riskhantering är att en organisation själv ska välja vilken risknivå organisationen anser vara godtagbar. Denna princip ändras genom kravet i avsnitt 2.4 eftersom en organisations kontroller enligt kravet ska stå i proportion till riskerna på en viss tillitsnivå.

...

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. Avvikelseerna kan beskrivas per krav eller i en sammanfattning.

Avvikelser som har upptäckts i normala situationer har korrigerats innan inspektionsberättelsen har lämnats till Transport- och kommunikationsverket. Om några avvikelser lämnas kvar ska de på ett entydigt sätt framgå av inspektionsberättelsen. I så fall ska berättelsen innehålla uppgift om vilka mindre avvikelser eller

andra slags avvikelser har lämnats kvar i systemet och enligt vilket tidsschema och på vilket sätt avvikelserna kommer att korrigeras.

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 korrigerande av avvikelserna är tillräcklig eller leverantören vidtar kompenserande åtgärder. Vid behov kräver Transport- och kommunikationsverket korrigerande av upptäckta avvikelser.

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:

- Autentiseringslag: 8 a § Autentiseringsfaktorer som ska användas i identifieringsmetoden
- Bilagan till LOA: 2.2.1 Medel för elektronisk identifiering: egenskaper och utformning
- Autentiseringslag: 8 § Krav på system för elektronisk identifiering. 1 mom. 3 punkten
- Bilagan till LOA: 2.3.1 Autentiseringsmekanism
- Bilagan till LOA: 2.4.6 Tekniska kontroller (controls), punkt 2
- M72: 6 § Krav på informationssäkerhet i identifieringsmetoder
- M72: 7 § Krypteringskrav för identifieringssystem och gränssnitt
- M72: 8 § Krav på informationssäkerhet i gränssnitt mellan en leverantör av identifieringsverktyg och en leverantör av tjänster för förmedling av identifiering
- M72: 9 § Krav på informationssäkerhet i gränssnitt för ärendehanteringstjänster
- Bilagan till LOA: 1. Tillämpliga definitioner
- 2. **autentiseringsfaktor**: en faktor som bekräftas vara bunden till en person och som tillhör någon av följande kategorier [...]

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

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 7 § i M72 lämnas in utöver inspektionsberättelsen. Rapporten ska visa TLS- och krypteringsprofilerna för gränssnittet utåt.

3.2 Interoperabilitet

Kraven föreskrivs i följande bestämmelser:

- Autentiseringslag (29.3.2019/412): 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
- M72: 12 § Minimiuppsättning uppgifter som ska förmedlas i förtroendenätet
- M72: 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:

- Autentiseringslag: 8 § Krav på system för elektronisk identifiering, 1 mom. 4 punkten
- LOA: 2.3.1 Autentiseringsmekanism
- Bilagan till LOA: 2.4.6 Tekniska kontroller (controls), punkterna 1–3

- M72: 5 § Tekniska informationssäkerhetsåtgärder i identifieringssystem

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 informationssäkerhetsshot 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 datakommunikationsförbindelserna 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
- hårdande
- 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:

- Autentiseringslag: 8 § Krav på system för elektronisk identifiering, 1 mom. 4 punkten
- Bilagan till LOA: 2.4.6 Tekniska kontroller (controls), punkterna 1 och 4
- Autentiseringslag: 16 § Skyldighet för leverantörer av identifieringstjänster att anmäla hot och störningar som riktas mot verksamheten eller skyddet av uppgifter
- M72: 5 § Tekniska informationssäkerhetsåtgärder i identifieringssystem
- M72: 11 § Störningsanmälningar från leverantörer av identifieringstjänster 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:

- Autentiseringslag: 13 § Allmänna skyldigheter för leverantörer av identifieringstjänster
- Bilagan till LOA: 2.4.4 Registerföring, punkterna 1–2
- Autentiseringslag: 8 § Krav på system för elektronisk identifiering, 1 mom. 4 punkten
- Bilagan till LOA: 2.4.6 Tekniska kontroller (controls), punkt 1 (observera kravet på skydd av känsligt kryptografiskt material på tillitsnivåerna väsentlig och hög) och punkt 5
- M72: 5 § Tekniska informationssäkerhetsåtgärder i identifieringssystem
- M72: 7 § Krypteringskrav för identifieringssystem och gränssnitt
- Autentiseringslag: 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:

- Autentiseringslag: 8 § Krav på system för elektronisk identifiering, 1 mom. 4 punkten
- Bilagan till LOA: 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:

- Autentiseringslag: 13 § Allmänna skyldigheter för leverantörer av identifieringstjänster
- Bilagan till LOA: 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:

- Autentiseringslag: 8 § Krav på system för elektronisk identifiering, 1 mom. 5 punkten
- Bilagan till LOA: 2.4 Hantering och organisation, ingress
- Bilagan till LOA: 2.4.3 Ledning avseende informationssäkerhet
- Bilagan till LOA: 2.4.7 Efterlevnad och revision
- M72: 4 § Krav på ledning avseende informationssäkerheten hos leverantörer av identifieringstjänster
- Bilagan till LOA: 1. Tillämpliga definitioner
- 4. **ledningssystem för informationssäkerhet:** 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:

- Autentiseringslag: 8 § Krav på system för elektronisk identifiering, 1 mom. 1–2 punkten
- Autentiseringslag: 17 § Identifiering av en fysisk person som ansöker om ett identifieringsverktyg
- Bilagan till LOA: 2.1.2 Styrkande och kontroll av identitet (fysisk person)
- Autentiseringslag: 7 b § Information om giltighet för pass eller identitetskort
- M72: 6 § Krav på informationssäkerhet i identifieringsmetoder

Krav på styrkande och kontroll av identitet hos juridisk person

- Autentiseringslag: 7 a § Användning av uppgifter i företags- och organisationsregister

Anvisning

211/2019 O
x.x.2019

54 (192)

- Autentiseringslag: 17 a § Identifiering av en juridisk person som ansöker om ett identifieringsverktyg
- Bilagan till LOA: 2.1.3 Styrkande och kontroll av identitet (juridisk person)
- Bilagan till LOA: 2.1.4

Bilagan till LOA: 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

- Inledande identifiering utgår från att en person visar ett identitetsbevis som är godkänt i Finland
- Inledande identifiering med elektroniskt identifieringsverktyg
- Inledande identifiering utifrån en identifiering som sker för annat ändamål
- Inledande identifiering som utförs av polisen

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

Anvisning

211/2019 O
x.x.2019

55 (192)

- jämföra fotot på identitetsbeviset med personens ansikte. Det går även att jämföra signaturer – beviset kan ha en elektronisk signatur. 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 någon visar ett förfalskat identitetsbevis eller om att ett identitetsbevis visas av fel person. Hänsyn ska även tas till följande:
 - kontrollera säkerhetsdetaljerna i identitetsbevis
 - kontrollera att det foto eller den video som personen har överlämnat om sig själv är äkta.

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.

Anvisning

211/2019 O
x.x.2019

56 (192)

Jfr även LOA guidance:

Det ska också finnas variationer i de egenskapsbaserade autentiseringsfaktorerna mellan olika personer för att det ska vara möjligt att specificera 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 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 någon visar ett förfalskat identitetsbevis eller om att ett identitetsbevis visas av fel person.
- 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.
- Det är en öppen fråga på vilket sätt ett identitetsbevis äkthet kan kontrolleras om beviset inte är försett med chip. 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.

Anvisning

211/2019 O
x.x.2019

57 (192)

- 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 nästan alla pass 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. Egenskapen ska i något skede också införas i EU-identitetskort. Denna ytterligare autentisering är inte möjlig för US-pass.
- När kontrollen av att uppgifterna 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. Därför kan fotot inte avläsas på chipet och användas vid identifiering. I biometriska pass har fotot lagrats på chipet.
- 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.

Anvisning

211/2019 O
x.x.2019

58 (192)

- 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.
- 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.
- 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 överensstämelsen hos uppgifterna i identitetsbeviset och även kan observera personens beteende.

3.10 Identifieringsverktygs, eller identifieringsmetoders, livscykel

Kraven föreskrivs i följande bestämmelser:

- Ansökan och registrering: 7 § och 20 § i autentiseringslagen och 6 § i M72
- Utfärdande, leverans och aktivering: 20 § och 21 § i autentiseringslagen och 2.2.2 i LOA
- Upphävande, återkallelse och återaktivering: 25 § och 26 § i autentiseringslagen (2.2.3 i LOA)
- Förnyelse och ersättning: 22 § i autentiseringslagen och 2.2.4 i LOA

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 anvisningspromemoria⁸ som behandlar kontroll av identitet i anslutning till underhåll.

4 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)

⁸ Se Tolkningstilläggstagande dnr: Traficom/106/09.02.00/2019 (25.3.2019) Transport- och kommunikationsverkets tolkningspromemoria om användning av körkort vid styrande 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.kyberturvallisuuskeskus.fi/sv/elektronisk-identifiering>

- 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 (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)
11. Resultat av bedömning av olika delområden (3.1–3.10 i tillämpliga delar)

5 BILAGA B: Allmänna kriterier för bedömning av identifieringstjänster

5.1 Identifieringsmetodens egenskaper och autentiseringsmekanism

1 Identifieringsmetodens egenskaper och autentiseringsmekanism

M72: 15 § Kriterier för kvalitetsrevision

Kvalitetsrevisioner av identifieringstjänster ska omfatta krav på
2) identifieringsmetod, dvs. identifieringsverktyg
c) identifieringsmetodens egenskaper och utformning
g) autentiseringsmekanismer

NR	TILLITS- NIVÅ	SAMMANFATTNING AV KRAVEN PÅ IDENTIFIERINGSTJÄNSTER	BESTÄMMELSER	HÄNVIS- NING TILL STANDAR- DER	OBSERVATIONER
1.	S, H	Autentiseringsmetoden använder minst två autentiseringsfaktorer från olika kategorier.	Autentiseringslag: 8 a § Autentiseringsfaktorer som ska användas i identifieringsmetoden 1) en kunskapsbaserad autentiseringsfaktor som personen måste kunna visa att den har kunskap om,		

Commented [LA1]: Hänvisningar på svenska till översättningar ISO/IEC 27001:2017 och ISO/IEC 27002:2014.
Skulle de vara hellre på engelska?

Anvisning

211/2019 O
x.x.2019

63 (192)

			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. [...] Bilagan till LOA: 2.2.1 Medel för elektronisk identifiering: egenskaper och utformning Medlet för elektronisk identifiering använder minst två autentiseringsfaktorer från olika kategorier.		
2.	S, H	Autentiseringsfaktorerna är oberoende av varandra.	Bilagan till LOA: 2.2.1 Medel för elektronisk identifiering: egenskaper och utformning Medlet för elektronisk identifiering är utformat så att det kan antas att det endast används under ägarens kontroll eller innehav.		Vid identifieringsmetoder som används med mobilutrustning ska särskild uppmärksamhet fästas vid att autentiseringsfaktorerna är oberoende av varandra.
3.	S, H	Vid utformningen av en identifieringsmetod har hänsyn tagits till att olika autentiseringsfaktorer är utsatta för olika hot.	Bilagan till LOA: 2.2.1 Medel för elektronisk identifiering: egenskaper och utformning Medlet för elektronisk identifiering är utformat så att det kan antas att det endast används under ägarens kontroll eller innehav.		

Anvisning

211/2019 O
x.x.2019

64 (192)

4.	S, H	Personalen och underleverantörerna till en leverantör av identifieringstjänster får inte kännedom om hemliga uppgifter om identifieringsmetoden.	M72A: 6 § Krav på informationssäkerhet i identifieringsmetoder [...] Tjänsteleverantören ska säkerställa att hemliga uppgifter om identifieringsverktyget inte i någon situation röjs för dess personal. Tjänsteleverantören 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.
5.	S, H	Autentiseringsfaktorerna har bekräftats vara bundna till en person.	Bilagan till LOA: 1. Tillämpliga definitioner 2. autentiseringsfaktor: en faktor som bekräftas vara bunden till en person och som tillhör någon av följande kategorier [...] Bilagan till LOA: 2.2.1 Medel för elektronisk identifiering: egenskaper och utformning Medlet för elektronisk identifiering är utformat så att det kan antas att det endast används under ägarens kontroll eller innehav.		Till exempel bindning mellan en identifieringsapp och en person, personifiering av chipet, bindning mellan en person och en kodtabell eller enhet.
6.	S, H	Autentiseringsmekanismen är utformad så att varje identifieringstransaktion har ett specifikt elektroniskt bevis.	Autentiseringslag: 8 a § [...] I varje identifieringsmetod ska det i enlighet med avsnitt 2.3.1 i bilagan till förordningen om tillitnivåer vid		även tjänster för identifieringsförmedling

Anvisning

211/2019 O
x.x.2019

65 (192)

			elektronisk identifiering användas en sådan dynamisk autentisering som <u>ändras vid varje</u> ny autentisering mellan en person och det system som kontrollerar personens identitet.		
7.	S, H	Ett elektroniskt bevis på en identifierings-transaktion bygger på autentiseringsfaktorer som är bundna till en person.	Bilagan till LOA: 1. Tillämpliga definitioner 3. dynamisk autentisering: en elektronisk process som använder kryptering eller andra metoder för att på begäran skapa ett elektroniskt bevis för att en person har kontroll över eller är i besittning av identifieringsinformationen, och som ändras vid varje autentisering mellan personen och det system som kontrollerar personens identitet.		LOA guidance (utdrag) Det primära syftet med dynamisk autentisering är att minska till exempel faran eller risken för man-in-the-middle-attacker (Man-in-The-Middle attack) där kontrolluppgifter om en tidigare lagrad autentisering används på nytt. ... Det är bra att komma ihåg att dynamisk autentisering och en autentisering som bygger på flera faktorer inte är identiska begrepp. En autentisering som bygger på flera faktorer kräver inte att autentiseringen ska ske dynamiskt (till exempel en pinkod eller uppgifter om fingeravtryck). Därför kan en sådan autentisering vara mer utsatt

					för replay-angrepp än vad en dynamisk autentisering är. ... Om en persons privata nyckel är lagrad i distanstjänst (koncentrerad exempelvis på en HSM-enhet som leverantören av identifieringstjänster använder), ska den autentiseringsmetod som krävs för att använda den privata nyckeln även vara dynamisk.
8.	H	Användaren kan på ett tillförlitligt sätt skydda metoden (verktyget) och sina autentiseringsfaktorer mot användning av andra.	Bilagan till LOA: 2.2.1 Medel för elektronisk identifiering: egenskaper och utformning Medlet för elektronisk identifiering är utformat så att ägaren på tillförlitligt sätt kan skyddas mot användning av andra.		Exempel i LOA guidance: Med tillförlitligt skydd avses åtgärder för att skydda ett medel för elektronisk identifiering så 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 pinkod, i maskinella processer.

Anvisning

211/2019 O
x.x.2019

67 (192)

					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, punkt 1): ☐ 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 exempel genom att begränsa antalet försök, använda fördröjningsmekanismer och säkerställa en tillräcklig entropi.
--	--	--	--	--	--

9.	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.	Bilagan till LOA: 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 transaktio-	även tjänster för identifieringsförmedling
----	------	---	--	---	---

Anvisning

211/2019 O
x.x.2019

69 (192)

				ner i till- lämpnings- tjänster	
10.	S, H	Identifieringsuppgifter (personuppgifter) som lagras i identifieringstransaktioner skyddas.	Bilagan till LOA: 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. Jfr M72: 7–9 § krypteringskrav på meddelandenivå nedan		även tjänster för identifieringsförmedling Hänsyn ska tas till alla tekniska miljöer som deltar i identifieringstransaktioner och där identifieringsuppgifter lagras.
11.	S	Säkerhetskontroller som en autentiseringsmekanism genomför skyddar mot angripare med måttlig angreppspotential.	Autentiseringslag: 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. Bilagan till LOA: 2.3.1 Autentiseringsmekanism	Vid bedömningen bör hänsyn tas till relevanta hot. I ISO 29115 nämns följande: gissningar på och ut- anför nätet, kopiering	även tjänster för identifieringsförmedling I autentiseringsmekanismer ska hänsyn även tas till hot som föranleds av att fel ärendehanteringstjänst har lämnat en identifieringsbegäran eller kapat identifieringssessioner (phishing). se LOA guidance: beskrivning i avsnitt 2.3.1, s. 24–26, på

Anvisning

211/2019 O
x.x.2019

70 (192)

			Autentiseringsmekanismen genomför säkerhetskontroller för att verifiera medlet för elektronisk identifiering, varför det är högst osannolikt att exempelvis gissningar, tjuvlyssning, omspelning eller manipulation av kommunikation som görs av en angripare med måttlig angreppspotential kan underminera autentiseringsmekanismerna.	av identifieringsuppgifter, nät-fiske, tjuvlyssning, replay-angrepp, sessionskapning, man-i-mitten-attacker, stöld av identifieringsuppgifter, spoofing-angrepp och olaga identitetsanvändning.	https://www.kyberturvallisuuskeskus.fi/sites/default/files/media/file/LOA_Guidance_Final_suomeksi.pdf
--	--	--	--	--	--

Anvisning

211/2019 O
x.x.2019

71 (192)

				ISO/IEC 15408-1 defines "attack potential – measure of the effort to be expended in attacking a [mechanism], expressed in terms of an attacker's expertise, resources and motivation". Annex B.4 of ISO/IEC 18045 / CEM contains Guidance on	
--	--	--	--	--	--

Anvisning

211/2019 O
x.x.2019

72 (192)

				how to calculate the attack potential necessary to exploit a given weakness of an authentication mechanism	
12.	H	Säkerhetskontroller som en autentiseringsmekanism genomför skyddar mot angripare med hög angreppspotential.	Autentiseringslag: 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. Bilagan till LOA: 2.2.1 Medel för elektronisk identifiering: egenskaper och utformning	se ovan	även tjänster för identifieringsförmedling alla säkerhetsfaktorer för en autentiseringsmekanism i proportion till en hög angreppspotential

Anvisning

211/2019 O
x.x.2019

73 (192)

			Medlet för elektronisk identifiering skyddar mot kopiering och manipulering samt mot angripare med hög angreppskapacitet. Bilagan till LOA: 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 kan underminera autentiseringsmekanismerna.		
13.	S, H	I en autentiseringsmekanism följs obligatoriska krypteringskrav mellan en leverantör av identifieringsverktyg och en identifieringsförmedling.	Bilagan till LOA: 2.4.6 Tekniska kontroller (controls) 2. <u>Elektroniska kommunikationskanaler</u> som används för att utbyta personuppgifter eller känslig information <u>skyddas</u> mot avlyssning, manipulation och omspelning. M72: 7 § Krypteringskrav för identifieringssystem och gränssnitt <u>Trafiken i gränssnitten mellan leverantörer av identifieringstjänster och mellan leverantörer av identifieringstjänster och tjänster för ärendehantering ska krypteras.</u>	A.10.1.1 Regler för användning av kryptografiska säkerhetsåtgärder A.13.2.3 Informationsöverföring:	även tjänster för identifieringsförmedling

Anvisning

211/2019 O
x.x.2019

74 (192)

			Följande metoder ska användas vid kryptering, nyckelutbyte och i underskrifter i anslutning till kryptering: 1) Nyckelutbyte: DHE-metoder, eller ECDHE-metoder som använder elliptiska kurvor, ska användas vid nyckelutbyte. Den ändliga kroppen (<i>finite field</i>) som används i räkneoperationer ska utgöra minst 2 048 bitar i DHE-metoden och minst 224 bitar i ECDHE-metoden. 2) Underskrifter: Vid användning av RSA för elektronisk underskrift ska nyckeln utgöra minst 2 048 bitar. Vid användning av ECDSA-metoden för elliptisk kurva ska den ändliga kroppen nedan utgöra minst 224 bitar. 3) Symmetrisk kryptering: Krypteringsalgoritmen ska vara AES eller Serpent. Nyckeln ska utgöra minst 128 bitar. Krypteringsmoden ska vara CBC, GCM, XTS eller CTR. 4) Hashfunktioner: Hashfunktionen ska vara SHA-2, SHA-3 eller Whirlpool. Med SHA-2 avses funktionerna SHA224, SHA256, SHA384 och SHA512.	Elektronisk meddelandehantering	
--	--	--	---	---------------------------------	--

Anvisning

211/2019 O
x.x.2019

75 (192)

			<u>Krypteringsinställningarna ska tekniskt tvingas till miniminivåerna ovan</u> för att handskakningen inte ska resultera i inställningar som är sämre än miniminivåerna. Vid användning av protokollet TLS ska TLS-version 1.2 eller nyare användas. TLS-version 1.1 kan användas endast om användarens terminalutrustning inte stöder nyare versioner. <u>Integriteten och sekretessen för meddelanden med personuppgifter ska skyddas</u> förutom med kryptering som avses i 1 mom. också <u>på meddelandenivå</u> enligt 1 mom. 8 § Krav på informationssäkerhet i gränssnitt mellan en leverantör av identifieringsverktyg och en leverantör av tjänster för förmedling av identifiering Krypteringsmetoderna ska uppfylla kraven i 7 § 1–4 mom. Metadata eller motsvarande metoder som garanterar motsvarande informationssäkerhetsnivå ska användas vid identifiering av parter och förmedling av uppgifter som behövs vid identifiering.		
--	--	--	---	--	--

Anvisning

211/2019 O
x.x.2019

76 (192)

			Alla personuppgifter ska krypteras och undertecknas på meddelandenivå.		
14.	S, H	I en autentiseringsmekanism följs obligatoriska krypteringskrav mellan en identifieringstjänst och en tjänst för ärendehantering.	Bilagan till LOA: 2.4.6 Tekniska kontroller (controls) 2. Elektroniska kommunikationskanaler som används för att utbyta personuppgifter eller känslig information <u>skyddas</u> mot avlyssning, manipulation och omspelning. M72: 7 § (ovan) M72: 9 § Krav på informationssäkerhet i gränssnitt för ärendehanteringstjänster Gränssnitten mellan en leverantör av tjänster för identifieringsförmedling och en tjänst för ärendehantering ska uppfylla kraven i 7 § 1–4 mom. En leverantör av identifieringsverktyg och tjänster för identifieringsförmedling ska sörja för personuppgifternas sekretess och integritet i gränssnitt för ärendehantering och i användargränssnitt.	A.10.1.1 Regler för användning av kryptografiska säkerhetsåtgärder A.13.2.3 Informationsöverföring: Elektronisk meddelandehantering	Observera även tjänster för identifieringsförmedling
15.	S, H	I en autentiseringsmekanism följs obligatoriska krypteringskrav i användargränssnitt (webbläsare, mobil användning).	Bilagan till LOA: 2.4.6 Tekniska kontroller (controls)	A.10.1.1 Regler för användning	Observera även tjänster för identifieringsförmedling

Anvisning

211/2019 O
x.x.2019

77 (192)

			2. <u>Elektroniska kommunikationskanaler</u> som används för att utbyta personuppgifter eller känslig information <u>skyddas</u> mot avlyssning, manipulation och omspelning. M72: 7 § (ovan) M72: 9 § Krav på informationssäkerhet i gränssnitt för ärendehanteringstjänster Gränssnitten mellan en leverantör av tjänster för identifieringsförmedling och en tjänst för ärendehantering ska uppfylla kraven i 7 § 1–4 mom. En leverantör av identifieringsverktyg och tjänster för identifieringsförmedling ska sörja för <u>personuppgifternas sekretess och integritet i gränssnitt för ärendehantering och i användargränssnitt</u>.	av krypto-grafiska säkerhetsåtgärder A.13.2.3 Informati- onsöverföring: Elektronisk meddelan- dehantering	
16.	H	I en autentiseringsmekanism följs de skärpta krypteringskrav som fastställs i rekommendationen /krypteringskraven på tillitsnivån hög, när autentiseringsmekanismen används mellan tjänster för	MPS72 (14.5.2018): B 7.2 Rekommendation När det gäller kraven i 7 § 1 mom. rekommenderas att följande värden inom parentes tillämpas på tillitsnivån hög i identifieringssystem i stället för de värden som förutsätts:	A.10.1.1 Regler för användning av krypto-grafiska säkerhetsåtgärder	Observera även tjänster för identifieringsförmedling

Anvisning

211/2019 O
x.x.2019

78 (192)

	identifieringsförmedling och en identifieringsförmedling, mellan en identifieringstjänst och en ärendehanteringstjänst och i användargränssnitt (webbläsare, mobil användning).	1) Nyckelutbyte: DHE-metoder, eller ECDHE-metoder som använder elliptiska kurvor, ska användas vid nyckelutbyte. Den ändliga kroppen (<i>finite field</i>) som används i räkneoperationer ska utgöra minst 2 048 (<u>3 072 på tillitsnivån hög</u>) bitar i DHE-metoden och minst 224 (<u>256 på tillitsnivån hög</u>) bitar i ECDHE-metoden. DH-grupperna 14–21, 23, 24 och 26 (<u>15–21 på tillitsnivån hög</u>) enligt IANAs IKEv2-parametrar uppfyller kraven ovan. 2) Underskrifter: Vid användning av RSA för elektronisk underskrift ska nyckeln utgöra minst 2 048 (<u>3 072 på tillitsnivån hög</u>) bitar. Vid användning av ECDSA-metoden för elliptisk kurva ska den ändliga kroppen nedan utgöra minst 224 (<u>256 på tillitsnivån hög</u>) bitar. 3) Symmetrisk kryptering: Krypteringsalgoritmen ska vara AES eller Serpent (<u>på tillitsnivån hög AES eller Serpent</u>). Nyckeln ska utgöra minst 128 (<u>128 på tillitsnivån hög</u>) bitar. Krypteringsmoden ska vara CBC, GCM, XTS eller CTR. 4) Hashfunktioner: Hashfunktionen ska vara SHA-2, SHA-3 eller Whirlpool. Med SHA-2 avses funktionerna SHA224,	A.13.2.3 Informationsöverföring: Elektronisk meddelandehantering	
--	--	---	---	--

			SHA256, SHA384 och SHA512 (<i>SHA256, SHA384, SHA512 och SHA-3 på tillitsnivån hög</i>)		
--	--	--	---	--	--

5.2 Interoperabilitet

2 Interoperabilitet

RELEVANTA BESTÄMMELSER

Autentiseringslag: 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.

...

M72: 15 § Kriterier för kvalitetsrevision

Kvalitetsrevisioner av identifieringstjänster ska omfatta krav på
1) funktioner som påverkar tillhandahållandet av identifieringstjänsten (ett identifieringssystem)
d) tekniska åtgärder

Autentiseringslag: 12 a §

...

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.

...

M72: 12 § Minimiuppsättning uppgifter som ska förmedlas i förtroendenätet

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

- 1) vid identifiering av en fysisk person, åtminstone den identifieringsuppgift som identifierar personen, personens förnamn, efternamn och födelsedatum,
- 2) vid identifiering av en juridisk person, åtminstone den identifieringsuppgift som identifierar den fysiska personen som företräder den juridiska personen, personens efternamn och förnamn och den identifieringsuppgift som identifierar organisationen,
- 3) om identifieringsverktyget ligger på tillitsnivån väsentlig eller hög.

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

- 1) om en identifieringstransaktion gäller en offentlig eller en privat tjänst för ärendehantering,
- 2) vid identifiering av en fysisk person; förnamn och efternamn vid födseln, födelseort, nuvarande adress och kön,
- 3) vid identifiering av en juridisk person
 - a) nuvarande adress
 - b) momsregistreringsnummer
 - c) skatteregistreringsnummer

211/2019 O
x.x.2019

81 (192)

- d) den identifikator som avses i artikel 3.1 i Europaparlamentets och rådets direktiv 2009/101/EG⁹
- e) den identifieringskod för juridiska personer (ID) som avses i kommissionens genomförandeförordning (EU) nr 1247/2012¹⁰
- f) det registrerings- och identitetsnummer för ekonomiska aktörer (EORI-nummer) som avses i kommissionens genomförandeförordning (EU) nr 1352/2013¹¹
- g) punktskattenummer som avses i artikel 2.12 i rådets förordning nr 389/2012¹².

M72: 14 § Protokoll som används vid dataöverföring samt övriga krav

Leverantörer av identifieringsverktyg, leverantörer av tjänster för identifieringsförmedling och leverantörer av tjänster för ärendehantering 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.

M72: 25 § Ikraftträdande och övergångsbestämmelser

[...]

⁹ Europaparlamentets och rådets direktiv 2009/101/EG av den 16 september 2009 om samordning av de skyddsåtgärder som krävs i medlemsstaterna av de i artikel 48 andra stycket i fördraget avsedda bolagen i bolagsmännens och tredje mans intressen, i syfte att göra skyddsåtgärderna likvärdiga inom gemenskapen (EUT L 258, 1.10.2009, s. 11).

¹⁰ Kommissionens genomförandeförordning (EU) nr 1247/2012 av den 19 december 2012 om fastställande av tekniska genomförandestandarder för form och frekvens för rapportering om handel till transaktionsregister enligt Europaparlamentets och rådets förordning (EU) nr 648/2012 om OTC-derivat, centrala motparter och transaktionsregister (EUT L 352, 21.12.2012, s. 20).

¹¹ Kommissionens genomförandeförordning (EU) nr 1352/2013 av den 4 december 2013 om fastställande av de formulär som avses i Europaparlamentets och rådets förordning (EU) nr 608/2013 om tullens säkerställande av skyddet för immateriella rättigheter (EUT L 341, 18.12.2013, s. 10).

¹² Rådets förordning (EU) nr 389/2012 av den 2 maj 2012 om administrativt samarbete i fråga om punktskatter och om upphävande av förordning (EG) nr 2073/2004 (EUT L 121, 8.5.2012, s. 1).

Anvisning

211/2019 O
x.x.2019

82 (192)

Beredskap att förmedla uppgifter enligt föreskriftens 12 § 2 mom. ska vara tekniskt planerad i identifieringssystemet senast den 1 oktober 2018.					
NR	TILLITS- NIVÅ	SAMMANFATTNING AV KRAVEN PÅ IDENTIFIERINGSTJÄNSTER	BESTÄMMELSER	HÄNVIS- NING TILL STANDAR- DER	OBSERVATIONER
17.	S, H	En leverantör av identifieringstjänster som hör till förtroendenätet ska tillhandahålla minst ett gränssnitt som baserar sig på en allmänt tillämpad standard.	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 autentiseringslagen, är <u>1) gränssnittet mellan leverantörer av identifieringsverktyg.</u> <u>2) gränssnittet mellan en leverantör av identifieringsverktyg och en leverantör av tjänster för förmedling av identifiering.</u>		Tillämpning: Transport- och kommunikationsverket har utarbetat rekommendationsprofiler för protokollen SAML och Open IDConnect i samråd med samarbetsgruppen för förtroendenätet. 212/2018 S Finnish Trust Network SAML 2.0 Protocol Profile version 1.0 213/2018 S Finnish Trust Network OpenID Connect 1.0 Protocol Profile version 1.0 Rekommendationerna finns på Transport- och kommunikationsverkets webbplats på

Anvisning

211/2019 O
x.x.2019

83 (192)

			3) gränssnittet mellan en leverantör av tjänster för förmedling av identifiering 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 gränssnitt som behövs i förtroendenätets verksamhet. <u>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.</u>		https://www.kyberturvallisuuskeskus.fi/sv/elektronisk-identifiering
18.	S, H	Leverantören av identifieringsverktyg tillhandahåller kravenliga uppgifter (attribut) vid identifiering av en fysisk person .	M72: 12 § Minimiuppsättning uppgifter som ska förmedlas i förtroendenätet Följande uppgifter ska förmedlas via gränssnitten mellan leverantörer av identifieringsverktyg och leverantörer av tjänster för identifieringsförmedling:		

Anvisning

211/2019 O
x.x.2019

84 (192)

			1) vid identifiering av en fysisk person, åtminstone den identifieringsuppgift som identifierar personen, personens förnamn, efternamn och födelsedatum, ... 3) om identifieringsverktyget ligger på tillitsnivån väsentlig eller hög.		
19.	S, H	Leverantören av identifieringsverktyg har en erforderlig planerad beredskap att förmedla optionella uppgifter vid identifiering av en fysisk person .	M72: 12 § Minimiuppsättning uppgifter som ska förmedlas i förtroendenätet 2 mom. Gränssnitten mellan leverantörer av identifieringsverktyg och leverantörer av tjänster för identifieringsförmedling ska ha beredskap att förmedla följande uppgifter: 1) om en identifieringstransaktion gäller en offentlig eller en privat tjänst för ärendehantering, 2) vid identifiering av en fysisk person; förnamn och efternamn vid födseln, födelseort, nuvarande adress och kön ...		MPS 72: motivering till 12.1 §, s. 60: Beredskap att förmedla icke-obligatoriska attribut betyder att behandlingen av icke-obligatoriska attribut måste planeras i gränssnittet och identifieringssystemet så att leverantör av identifieringstjänster har en uppfattning om de tekniska åtgärder som är behövliga vid införandet. Icke-obligatoriska attribut behöver inte genomföras tekniskt i systemen. Vid teknisk konfigurerings ska man dock beakta

Anvisning

211/2019 O
x.x.2019

85 (192)

					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.
20.	S, H	Leverantören av identifieringsverktyg tillhandahåller kravenliga uppgifter (attribut) vid identifiering av en juridisk person .	M72: 12 § Minimiuppsättning uppgifter som ska förmedlas i förtroendenätet Följande uppgifter ska förmedlas via gränssnitten mellan leverantörer av identifieringsverktyg och leverantörer av tjänster för identifieringsförmedling: ... 2) vid identifiering av en juridisk person, åtminstone den identifieringsuppgift som identifierar den fysiska personen som företräder den juridiska personen, personens efternamn och förnamn och den identifieringsuppgift som identifierar organisationen,		endast om man börjar tillhandahålla stark autentisering av juridiska personer

Anvisning

211/2019 O
x.x.2019

86 (192)

			3) om identifieringsverktyget ligger på tillitsnivån väsentlig eller hög.		
21.	S, H	Leverantören av identifieringsverktyg har en erforderlig planerad beredskap att förmedla optionella uppgifter vid identifiering av en juridisk person .	M72: 12 § Minimiuppsättning uppgifter som ska förmedlas i förtroendenätet Gränssnitten mellan leverantörer av identifieringsverktyg och leverantörer av tjänster för identifieringsförmedling ska ha beredskap att förmedla följande uppgifter: 1) om en identifieringstransaktion gäller en offentlig eller en privat tjänst för ärendehantering, ... 3) vid identifiering av en juridisk person a) nuvarande adress b) momsregistreringsnummer c) skatteregistreringsnummer d) den identifikator som avses i artikel 3.1 i Europaparlamentets och rådets direktiv 2009/101/EG		

Anvisning

211/2019 O
x.x.2019

87 (192)

			e) den identifieringskod för juridiska personer (ID) 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 g) punktskattenummer som avses i artikel 2.12 i rådets förordning nr 389/2012.		
--	--	--	---	--	--

5.3 Tekniska krav på informationssäkerhet

3 Tekniska krav på informationssäkerhet

RELEVANTA BESTÄMMELSER

M72A: 15 § Kriterier för kvalitetsrevision

Kvalitetsrevisioner av identifieringstjänster ska omfatta krav på

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

d) tekniska åtgärder

Autentiseringslag: 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

Bilagan till LOA: 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.

M72: 5 § Tekniska informationssäkerhetsåtgärder i identifieringssystem

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

- 1) datakommunikationssäkerhet
 - a) säkerhet i nätstrukturen
 - b) indelning av datakommunikationsnätet i zoner
 - c) filtreringsregler enligt principen om behovsenlig behörighet
 - d) administration av filtrering och kontrollsystem under hela livscykeln
 - e) administrationsförbindelser
- 2) säkerhet i informationssystem
 - a) administration av åtkomsträttigheter
 - b) identifiering av användare av system
 - c) hårdande av system
 - d) skydd mot skadliga program
 - e) spårning av säkerhetshändelser
 - f) förmåga att observera avvikelser samt återhämtning
 - g) internationellt eller nationellt rekommenderade krypteringslösningar till andra delar än vad som föreskrivs i 7 §
- 3) säkerhet i användning

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

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

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

5.3.1 Datakommunikationssäkerhet

3.1 Datakommunikationssäkerhet					
nr	tillits-nivå	SAMMANFATTNING AV KRAVEN PÅ IDENTIFIERINGSTJÄNSTER	Bestämmelser	Hänvis-ning till	observationer

				standar- der	
22.	S, H	Datakommunikationssäkerhet: datakommunikationsförbindelser, administrationsförbindelser, processer för identifieringssystem (datakommunikation vid delprocesser för tillhandahållande, inklusive administration, av identifieringstjänster) och deras skyddspraxis har identifierats och dokumenterats Indelningen av ett identifieringssystemets datakommunikationsförbindelser i zoner och filtreringsreglerna ska göras enligt principen om behovsenlig behörighet (least privilege) och principen om försvar på djupet (defence in depth).	M72A: 5 § Tekniska informationssäkerhetsåtgärder i identifieringssystem Ett identifieringssystem ska planeras, genomföras och administreras med beaktande av följande faktorer: 4) datakommunikationssäkerhet a) säkerhet i nätstrukturen b) indelning av datakommunikationsnätet i zoner Bilagan till LOA: 2.4.6 Tekniska kontroller (controls) 2. <u>Elektroniska kommunikationskanaler</u> som används för att utbyta personuppgifter eller känslig information <u>skyddas</u> mot avlyssning, manipulation och omspelning.	A.8.1.1 Inventering av tillgångar A.13.1 Kommunikationssäkerhet/Hantering av nätverkssäkerhet: A.13.1.1 Säkerhetsåtgärder för nätverk	Informationssäkerheten i datakommunikationen ska säkerställas i identifieringssystemets helhetsarkitektur. Obs! Alla relevanta datakommunikationsförbindelser till underleverantörer ska också säkerställas vid planeringen (inkl. infrastruktur, programvaror, drifttjänster, kortproduktion osv.). 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-

				A.13.1.3 Separation av nätverk	och övervakningssystemen mellan nätområdena.
23.	S, H	Datakommunikationssäkerhet: Identifieringssystemets datakommunikationsutrustning (de tidigare kriterierna in- nefattade <i>Den egendom som används</i>) och datakommunikationssystem har identifierats och dokumenterats.	M72A: 5 § Tekniska informationssäkerhetsåtgärder i identifieringssystem Ett identifieringssystem ska planeras, genomföras och administreras med beaktande av följande faktorer: 1) datakommunikationssäkerhet a) säkerhet i nätstrukturen	A.8.1.1 In- ventering av till- gångar	
24.	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.	M72A: 5 § Tekniska informationssäkerhetsåtgärder i identifieringssystem Ett identifieringssystem ska planeras, genomföras och administreras med beaktande av följande faktorer: 1) datakommunikationssäkerhet a) säkerhet i nätstrukturen b) indelning av datakommunikationsnätet i zoner	A.12.1.4 Driftsäkerhet: Separation av utvecklings-, test- och driftmiljöer	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.

25.	S, H	Datakommunikationssäkerhet: Genom datakommunikationsförbindelser i identifieringssystem säkerställs filtreringar enligt principen om behövsenlig behörighet.	M72A: 5 § Tekniska informationssäkerhetsåtgärder i identifieringssystem Ett identifieringssystem ska planeras, genomföras och administreras med beaktande av följande faktorer: 1) datakommunikationssäkerhet c) filtreringsregler enligt principen om behövsenlig behörighet	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	
26.	S, H	Datakommunikationssäkerhet: Förbindelserna mellan ett produktionsnät och ett offentligt nät ska vara riskbaserade förbindelser som endast möjliggör tjänstens funktioner.	M72A: 5 § Tekniska informationssäkerhetsåtgärder i identifieringssystem Ett identifieringssystem ska planeras, genomföras och administreras med beaktande av följande faktorer: 1) datakommunikationssäkerhet a) säkerhet i nätstrukturen c) filtreringsregler enligt principen om behövsenlig behörighet	se raden ovan	Alla andra förbindelser som inte är nödvändiga för verksamheten har uttryckligen förbjudits eller stängts.
27.	S, H	Datakommunikationssäkerhet: Identifieringstjänsternas och de förlitande parternas kryptografiska nyckelmateri eller metadata byts på ett säkert sätt.	M72A: 8 § Krav på informationssäkerhet i gränssnitt mellan en leverantör av identifieringsverktyg och en leverantör av tjänster för förmedling av identifiering Metadata eller motsvarande metoder som garanterar motsvarande informationssäkerhetsnivå ska användas vid identifiering av parter och förmedling av uppgifter som behövs vid identifiering.betämning jfr M72A: 7–9 § Krypteringskrav på meddelandenivå	A.10.1.2 Kryptering: Nyckelhantering	jfr PSD2/RTS eIDAS art45 eller eSeal krav på certifikat för identifiering av part Borde det finnas en definition av nyckelhanteringspraxisen för de olika tillitsnivåerna? Det skulle kunna vara nödvändigt att av praktiska skäl planera det

Anvisning

211/2019 O
x.x.2019

94 (192)

			jfr LOA: 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 <u>sekretess</u>, integritet och tillgänglighet. 2. Elektroniska kommunikationskanaler som används för att utbyta personuppgifter eller känslig information skyddas mot avlyssning, manipulation och omspelning. jfr LOA: 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 förhöjd/grundläggande angreppspotential kan underminera autentiseringsmekanismerna.	första nyckelutbytet och förnyelserna på olika sätt, särskilt tillsammans med förlitande parter, men de ska ändå vara säkra. Anvisning 211/2016 innehöll följande informativa observationer: Policyn ska beakta skyddet av krypteringsnycklar under nycklarnas hela livscykel. 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 befohgenheter.
--	--	--	--	---

Anvisning

211/2019 O
x.x.2019

95 (192)

					KATAKRI 2015 (I12)
28.	H	Datakommunikationssäkerhet: Identifieringstjänsternas och de förlitande parternas kryptografiska nyckelmaterial eller metadata byts på ett säkert sätt.	jfr ovan och 2.3.1 Autentiseringsmekanism i LOA Autentiseringsmekanismen genomför säkerhetskontroller för att verifiera medlet för elektronisk identifiering, varför det är högst osannolikt att exempelvis gissningar, tjuvlyssning, omspelning eller manipulation av kommunikation som görs av en angripare med stor angreppspotential kan underminera autentiseringsmekanismerna.	A.10.1.2 Kryptering: Nyckelhantering	Borde det finnas en definition av nyckelhanteringspraxisen för de olika tillitsnivåerna? Det skulle kunna vara nödvändigt att av praktiska skäl planera det första nyckelutbytet och förnyelserna på olika sätt, särskilt tillsammans med förlitande parter, men de ska ändå vara säkra.
29.	S, H	Datakommunikationssäkerhet: Det gäller att säkerställa administration av filtrering och kontrollsystem i datakommunikationsförbindelser i identifieringssystem.	Ett identifieringssystem ska planeras, genomföras och administreras med beaktande av följande faktorer: 1) datakommunikationssäkerhet d) administration av filtrering och kontrollsystem under hela livscykeln	A.13.1 Kommunikationssäkerhet/Hantering av nätverksäkerhet:	

				A.13.1.1 Säkerhets- åtgärder för nätverk	
30.	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.	M72A: 5 § Tekniska informationssäkerhetsåtgärder i identifieringssystem Ett identifieringssystem ska planeras, genomföras och administreras med beaktande av följande faktorer: 1) datakommunikationssäkerhet e) administrationsförbindelser 3) säkerhet i användning c) distansanvändning och -administration Ett produktionsnät och administrationsförbindelser i 1) e) samt distansanvändning och -administration i 3) c) ovan ska genomföras så att informationssäkerhetshot som orsakas av organisationens övriga tjänster, som e-post eller webbsurfning, samt informationssäkerhetshot som orsakas av organisationens terminalenhet vid hantering av andra funktioner än de som är nödvändiga för hanteringen är a) speciellt bedömda och minimerade på tillitsnivån väsentlig.	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	MPS72: internet och kontorsnätet anses vara icke-betrodda nät, om inte kontorsnätet omfattas av bedömning av överensstämmelse. Överföringskanalen ska alltså i distansanvändning 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.

				A.13.1.3 Hantering av nät- verkssä- kerhet: Se- paration av nätverk	
31.	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.	M72A: 5 § Tekniska informationssäkerhetsåtgärder i identifieringssystem Ett identifieringssystem ska planeras, genomföras och administreras med beaktande av följande faktorer: 1) datakommunikationssäkerhet e) administrationsförbindelser 3) säkerhet i användning c) distansanvändning och -administration M72A: 5 § Tekniska informationssäkerhetsåtgärder i identifieringssystem Ett produktionsnät och <u>administrationsförbindelser</u> i 1) e) samt <u>distansanvändning och -administration</u> i 3) c) ovan ska genomföras så att informationssäkerhetshot som orsakas av organisationens övriga tjänster, som e-post eller	se raden ovan	

Anvisning

211/2019 O
x.x.2019

98 (192)

			webbsurfning, samt informationssäkerhetshot som orsakas av organisationens terminalenhet vid hantering av andra funktioner än de som är nödvändiga för hanteringen är ... b) förhindrade som helhet på tillitsnivån hög. Tillämpningsanvisning i MPS72: På tillitsnivån hög kan kraven i 2 mom. genomföras åtminstone så att det från arbetsstationer som är i distansanvändning förhindras åtkomst till organisationens övriga tjänster, som e-post, och att det från arbetsstationen tas bort möjligheten att använda andra funktioner än de som är nödvändiga för användning av hanteringsnätet. I praktiken betyder detta alltså att det behövs en separat arbetsstation för hantering. Helhetsbedömningen på tillitsnivån hög betyder att om man använder en annan än en sådan hårdad arbetsstation som beskrivs ovan, ska man i genomförandet beakta separering av produktions-systemet 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; distansskrivbord). 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 web-proxy. 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 behövliga metoder.		
--	--	--	--	--	--

5.3.2 Säkerhet i informationssystem

3.2 Säkerhet i informationssystem					
NR	TILLITS- NIVÅ	SAMMANFATTNING AV KRAVEN PÅ IDENTIFIERINGSTJÄNSTER	BESTÄMMELSER	HÄNVIS- NING TILL STANDAR- DER	OBSERVATIONER
32.	S, H	Säkerhet i informationssystem: Informationssystemen och processerna i ett identifieringssystem (de processer som använder informationssystem vid tillhandahållande och administration av identifieringstjänster) har identifierats och dokumenterats .	M72A: 5 § Tekniska informationssäkerhetsåtgärder i identifieringssystem Ett identifieringssystem ska planeras, genomföras och administreras med beaktande av följande faktorer: 2) säkerhet i informationssystem a) administration av åtkomsträttigheter b) identifiering av användare av system	A.8.1.1 Hantering av tillgångar, Ansvar för tillgångar: Inventering	Klassning: bl.a. en godkänd användning av utrustning, program och övrig egendom ska vara fastställd.

		Informationssystemen i ett identifieringssystem har klassificerats med beaktande av den information som behandlas i systemen och de funktioner som systemen möjliggör. Klassificeringen av system ska beakta hela livscykeln för den information som ska skyddas. Den databehandlingsmiljö som används vid hanteringen har skilts åt från andra miljöer.		av tillgångar A.8.2.1 Hantering av tillgångar: Klassning av information	
33.	S, H	Säkerhet i informationssystem: Åtkomsträttigheterna till ett identifieringssystem har definierats och dokumenterats. Åtkomsträttigheterna bygger på en klassificering av informationssystem och enskilda personers/användares arbetsuppgifter. Åtkomst ska endast beviljas utifrån arbetsuppgifter (principen om behovsenlig behörighet).	M72A: 5 § Tekniska informationssäkerhetsåtgärder i identifieringssystem Ett identifieringssystem ska planeras, genomföras och administreras med beaktande av följande faktorer: 2) säkerhet i informationssystem a) administration av åtkomsträttigheter b) identifiering av användare av system	A.9.1.1 Verksamhetskrav för styrning av åtkomst: Regler för styrning av åtkomst A.9.1.2 Tillgång till nätverk och	Åtkomsten till information och databehandlingsmiljöer ska begränsas på ett systematiskt och dokumenterat sätt genom administration av åtkomsträttigheter.

				nätverks- tjänster A.9.4.1 Styrning av åtkomst till system och tillämp- ningar: Be- gränsning av åtkomst till inform- ation	
34.	S, H	Säkerhet i informationssystem: Användare av informationssystem för ett identifieringssystem identifieras med en känd teknik/metod som anses vara säker.	M72A: 5 § Tekniska informationssäkerhetsåtgärder i identifieringssystem Ett identifieringssystem ska planeras, genomföras och ad- ministreras med beaktande av följande faktorer: 2) säkerhet i informationssystem a) administration av åtkomsträttigheter b) identifiering av användare av system	A.9.4.2 Styrning av åtkomst till system och tillämp- ningar: Säkra inlogg- ningsruti- ner	t.ex. certifikat, 2FA i regel något annat än ett lösenord, men om lösenord ingår behövs det tillräckligt långa och individuella lö- senord och användarnamn (ej ge- mensamma)

35.	S, H	Säkerhet i informationssystem: Åtkomsträttigheter övervakas och hålls uppdaterade.	M72A: 5 § Tekniska informationssäkerhetsåtgärder i identifieringssystem Ett identifieringssystem ska planeras, genomföras och administreras med beaktande av följande faktorer: 2) säkerhet i informationssystem a) administration av åtkomsträttigheter b) identifiering av användare av system	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 åtkomsträttigheter	
-----	------	--	--	--	--

				A.9.2.6 Borttagning eller justering av åtkomsträttigheter	
36.	S, H	Säkerhet i informationssystem: De anställdas arbetsuppgifter och aktiviteter ska fastställas så att en person inte genom sin verksamhet oavsiktligen eller avsiktligt kan orsaka allvarliga säkerhetsavvikelser (farliga kombinationer).	M72A: 5 § Tekniska informationssäkerhetsåtgärder i identifieringssystem Ett identifieringssystem ska planeras, genomföras och administreras med beaktande av följande faktorer: 2) säkerhet i informationssystem a) administration av åtkomsträttigheter b) identifiering av användare av system		Ett exempel är att risken för att oärliga eller oaktsamma anställda beviljar identifieringsmetoder i strid med de uppställda kraven kan förebyggas genom fastställda arbetsuppgifter eller kontroller som minskar risken för misstag och missbruk. Vid bedömningen ska hänsyn, i enlighet med tillitsnivån för identifieringsmetoden, tas till en måttlig eller hög angreppspotential på samma sätt som i övriga punkter.

37.	S, H	Säkerhet i informationssystem: Härdande av identifieringssystem ska säkerställas: ett förfaringssätt, på vilket system installeras systematiskt så att resultatet är en härdad installation, ska användas. I identifieringssystem används endast tjänster, funktioner, processer, utrustning och komponenter som är nödvändiga för systemets funktion. Användningen av dessa har specificerats så att alla onödiga behörigheter och funktioner/element har tagits bort från installationen.	M72A: 5 § Tekniska informationssäkerhetsåtgärder i identifieringssystem Ett identifieringssystem ska planeras, genomföras och administreras med beaktande av följande faktorer: 2) säkerhet i informationssystem c) härdande av system	A.12.5 Styrning av driftsystem	se även datakommunikation Anvisningen 211/2016 innehöll följande kriterier som ingår som informativa kriterier i denna anvisning: En härdad installation ska endast omfatta sådana komponenter och tjänster samt användarnas och processernas rättigheter som är nödvändiga för att uppfylla verksamhetskraven och säkerställa säkerheten. Endast sådana funktioner, utrustningar och tjänster som är relevanta med tanke på användningskraven och databehandlingen har tagits i bruk.
38.	S, H	Säkerhet i informationssystem: I identifieringssystem säkerställs det att skador och hot som orsakas av skadliga program observeras, förebyggs, förhindras och åtgärdas.	M72A: 5 § Tekniska informationssäkerhetsåtgärder i identifieringssystem Ett identifieringssystem ska planeras, genomföras och administreras med beaktande av följande faktorer: 2) säkerhet i informationssystem	A.12.2 Skydd mot skadlig kod A.12.6 Hantering	Se även förmåga att observera avvikelser

Anvisning

211/2019 O
x.x.2019

105 (192)

			d) skydd mot skadliga program	av tekniska sårbarheter	
39.	S, H	Säkerhet i informationssystem: I alla delar av ett identifieringssystem används krypteringslösningar som rekommenderas.	M72A: 5 § Tekniska informationssäkerhetsåtgärder i identifieringssystem Ett identifieringssystem ska planeras, genomföras och administreras med beaktande av följande faktorer: 2) säkerhet i informationssystem g) internationellt eller nationellt rekommenderade krypteringslösningar till andra delar än vad som föreskrivs i 7 § i M72	A.10.1 Regler för användning av kryptografiska säkerhetsåtgärder A.18.1.5 Reglering av kryptografiska säkerhetsåtgärder	Följande källor anges i MPS72: 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 befohender.

Anvisning

211/2019 O
x.x.2019

106 (192)

					(KATAKRI 2015 (I12))
40.	S, H	Säkerhet i informationssystem: Kryptografiskt material är skyddat under materialets hela livscykel.	LOA: 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. Känsligt kryptografiskt material, om sådant används för utfärdande av medel för elektronisk identifiering och autentisering, ska skyddas från manipulation. M72A: 5 § Tekniska informationssäkerhetsåtgärder i identifieringssystem Ett identifieringssystem ska planeras, genomföras och administreras med beaktande av följande faktorer: 2) säkerhet i informationssystem a) administration av åtkomsträttigheter b) identifiering av användare av system	A.8.2.1 Klassning av information A.10.1.1 Regler för användning av kryptografiska säkerhetsåtgärder A.10.1.2 Nyckelhantering	Anvisningen 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.

Anvisning

211/2019 O
x.x.2019

107 (192)

			g) internationellt eller nationellt rekommenderade krypteringslösningar till andra delar än vad som föreskrivs i 7 § 3) säkerhet i användning b) behandlingsmiljön för sekretessbelagt material		KATAKRI 2015 (I12)
--	--	--	---	--	--------------------

5.3.3 Säkerhet i användning

3.3 Säkerhet i användning					
NR	TILLITS-NIVÅ	SAMMANFATTNING AV KRAVEN PÅ IDENTIFIERINGSTJÄNSTER	BESTÄMMELSER	HÄNVISNING TILL STANDAR- DER	OBSERVATIONER
41.	S, H	Säkerhet i användning: Hanteringen av förändringar i ett identifieringssystem är planerad och omsorgsfull.	M72A: 5 § Tekniska informationssäkerhetsåtgärder i identifieringssystem Ett identifieringssystem ska planeras, genomföras och administreras med beaktande av följande faktorer: 3) säkerhet i användning a) hantering av förändringar	A.12.1.2 Driftsäkerhet/Driftsrutiner och ansvar:	Tydliga processer ska vara fastställda för hantering av förändringar.

Anvisning

211/2019 O
x.x.2019

108 (192)

				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	
42.	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.	M72A: 5 § Tekniska informationssäkerhetsåtgärder i identifieringssystem Ett identifieringssystem ska planeras, genomföras och administreras med beaktande av följande faktorer: 3) säkerhet i användning c) hantering av programsårbarheter	A.12.5.1 Driftsäkerhet: Installation av program på driftsystem A.12.6.1 Driftsäkerhet: Hantering av tekniska sårbarheter	Anvisningen 211/2016 innefattade följande observationer som ingår som informativa observationer i denna anvisning: Organisationen ska ha en metod för att följa upp allmänna sårbarheter. Program som används i identifieringssystem ska vara förenliga med principerna för säker programmering.

Anvisning

211/2019 O
x.x.2019

110 (192)

				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	
--	--	--	--	---	--

Anvisning

211/2019 O
x.x.2019

111 (192)

				granskning av tillämpningar efter ändringar i driftsmiljö A.14.2.4 Restriktioner för ändringar av programpaket A.14.2.5 Principer för utveckling av säkra system A.14.2.6 Säker utvecklingsmiljö	
--	--	--	--	--	--

Anvisning

211/2019 O
x.x.2019

112 (192)

				A.14.2.7 Outsourcad utveckling A.14.2.8 Säkerhets- testning A.14.2.9 Acceptans- testning av system	
43.	S, H	Säkerhet i användning: Säkerhetskopieringen i identifierings-system görs systematiskt. Vid säkerhetskopiering tas hänsyn till klassificering av information (personuppgifter, kryptografisk information osv.), återställande av system och lagring av säkerhetskopior.	M72A: 5 § Tekniska informationssäkerhetsåtgärder i identifieringssystem Ett identifieringssystem ska planeras, genomföras och administreras med beaktande av följande faktorer: 3) säkerhet i användning d) säkerhetskopiering	A.12.3.1 Säkerhets- kopiering av inform- ation	Anvisningen 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.

5.4 Förmåga att observera avvikelser, hantering av avvikelser och störningsanmälningar

4 Förmåga att observera avvikelser, hantering av avvikelser och störningsanmälningar

RELEVANTA BESTÄMMELSER

M72A: 15 § Kriterier för kvalitetsrevision

Kvalitetsrevisioner av identifieringstjänster ska omfatta krav på

- 1) funktioner som påverkar tillhandahållandet av identifieringstjänsten (ett identifieringssystem)
- d) tekniska åtgärder

Allmänna krav

Autentiseringslag: 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

Bilagan till LOA: 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.

Autentiseringslag: 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 5 § och 11 § i M72

NR	TILLITS- NIVÅ	SAMMANFATTNING AV KRAVEN PÅ IDENTIFIERINGSTJÄNSTER	BESTÄMMELSER	HÄNVIS- NING TILL STANDAR- DER	OBSERVATIONER
44.	S, H	Det finns processer som har specificerats i förväg och förmåga att observera avvikelser i identifieringssystemet.	M72: 5 § Tekniska informationssäkerhetsåtgärder i identifieringssystem Ett identifieringssystem ska planeras, genomföras och administreras med beaktande av följande faktorer: 1) datakommunikationssäkerhet	A.12.4.1 Driftsäkerhet: Loggning av händelser	

		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.	d) administration av filtrering och kontrollsystem under hela livscykeln 2) säkerhet i informationssystem e) spårning av säkerhetshändelser f) förmåga att observera avvikelser samt återhämtning	A.12.4.2 Driftsäkerhet: Skydd av loginformation A.12.4.3 Driftsäkerhet: Administratörs- och operatörsloggar A.16.1 Hantering av informationssäkerhetsincidenter/Hantering av informationssäkerhetsincidenter	
--	--	---	--	---	--

Anvisning

211/2019 O
x.x.2019

116 (192)

				och förbättringar A. 16.1.1 Ansvar och rutiner A.16.1.6 Att lära av informationssäkerhetsincidenter	
45.	S, H	Loggdata om hantering av identifieringssystem har specificerats och skilts åt från övriga loggdata. Deras integritet har säkerställts.	Kraven på upprätthållande av informationssäkerhet i identifieringssystem föreskrivs i 8 § i autentiseringslagen och 2.4.6 i LOA. M72: 5 § Tekniska informationssäkerhetsåtgärder i identifieringssystem Ett identifieringssystem ska planeras, genomföras och administreras med beaktande av följande faktorer: 1) datakommunikationssäkerhet d) administration av filtrering och kontrollsystem under hela livscykeln	A.12.4.1 Driftsäkerhet: Loggning av händelser A.12.4.2 Driftsäkerhet: Skydd av logginformation	i loggdata lagras information om ändringar i identifieringssystemet

Anvisning

211/2019 O
x.x.2019

117 (192)

			2) säkerhet i informationssystem e) spårning av säkerhetshändelser f) förmåga att observera avvikelser samt återhämtning	A.12.1.4 Separation av utvecklings-, test- och driftmiljöer	
46.	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.	M72: 5 § Tekniska informationssäkerhetsåtgärder i identifieringssystem Ett identifieringssystem ska planeras, genomföras och administreras med beaktande av följande faktorer: 1) datakommunikationssäkerhet d) administration av filtrering och kontrollsystem under hela livscykeln 2) säkerhet i informationssystem f) förmåga att observera avvikelser samt återhämtning	A.16.1 Hantering av informationssäkerhetsincidenter/Hantering av informationssäkerhetsincidenter och förbättringar: A.16.1.2 Rapportering av in-	Anvisningen 211/2016 innefattade följande observationer som ingår som informativa observationer i denna anvisning: Alla observationer ska behandlas och deras inverkan klassificeras enligt överenskomna metoder.

				formations- säkerhets- händelser A.16.1.3 Rapporte- ring av svagheter gällande in- formations- säkerhet A.16.1.4 Bedömning av och be- slut om in- formations- säkerhets- händelser	
		Korrigeringsåtgärder som avvikelser och störningar i identifieringssystem kräver är systematiska och effektiva.	M72: 5 § Tekniska informationssäkerhetsåtgärder i identifieringssystem Ett identifieringssystem ska planeras, genomföras och administreras med beaktande av följande faktorer: 1) datakommunikationssäkerhet	A.16.1 Hantering av inform- ationssä- kerhetsin-	Kraven på tillgänglighet (SLA) är en avtalsfråga, hänsyn ska tas till icke-diskriminering

Anvisning

211/2019 O
x.x.2019

119 (192)

		Planerna för verksamhetens kontinuitet innehåller förebyggande och korrigerande åtgärder för att minimera de effekter som betydande störningar i verksamheten eller exceptionella incidenter har.	d) administration av filtrering och kontrollsystem under hela livscykeln 2) säkerhet i informationssystem f) förmåga att observera avvikelser samt återhämtning	ciden- ter/Hante- ring av in- formations- säkerhets- incidenter och förbätt- ringar: A.16.1.5 Hantering av inform- ationssä- kerhetsin- cidenter	
47.	S, H	I processer för incidenthantering har hän- syn tagits till skyldigheten att göra an- mälan till andra leverantörer av iden- tifieringstjänster som hör till förtro- endenätet.	Autentiseringslag: 16 § Skyldighet för leverantörer av identifieringstjänster att anmäla hot och stör- ningar som riktas mot verksamheten eller skyddet av uppgifter En leverantör av identifieringstjänster ska trots sekretess- bestämmelserna utan ogrundat dröjsmål <u>anmäla</u> bety- dande hot och störningar som riktas mot tjänsternas funkt- ion, informationssäkerheten eller användningen av en	A.16.1.2 Hantering av inform- ationssä- kerhetsin- cident- ter/Hante- ring av in- formations-	Ansvar för undantagssituationer och kommunikation med intres- senter har fastställts.

Anvisning

211/2019 O
x.x.2019

120 (192)

			elektronisk identitet till ... övriga avtalsparter i förtroendena- tätet. ... Leverantören av identifieringstjänster får trots sekretess- bestämmelserna <u>underrätta</u> alla medlemmar i förtroende- nätet om hot och störningar som avses i 1 mom. samt om tjänsteleverantörer som skäligen kan misstänkas för att ef- tersträva orättmätig ekonomisk vinning, lämna betydelse- full osann eller vilseledande information eller behandla per- sonuppgifter på ett olagligt sätt. Tillämpning: Samarbetsgruppen för förtroendenätet har tagit fram gemen- samma rutiner för ömsesidiga störningsanmälningar och anmäl- ningströsklar.	säkerhets- incidenter och förbätt- ringar: Rapporte- ring av in- formations- säkerhets- händelser	
48.	S, H	I processer för incidenthantering har hän- syn tagits till skyldigheten att göra an- mälan till användare och förlitande parter.	Autentiseringslag: 16 § Skyldighet för leverantörer av identifieringstjänster att anmäla hot och stör- ningar som riktas mot verksamheten eller skyddet av uppgifter En leverantör av identifieringstjänster ska ... utan ogrun- dat dröjsmål anmäla betydande hot och störningar som	A.16.1.2 Hantering av inform- ationssä- kerhetsin- ciden- ter/Hante- ring av in-	Ansvar för undantagssituationer och kommunikation med intres- senter har fastställts. Med förlitande parter avses tjäns- ter för ärendehantering.

Anvisning

211/2019 O
x.x.2019

121 (192)

			riktas mot tjänsternas funktion, informationssäkerheten eller användningen av en elektronisk identitet till de tjänsternas förlitande parter, 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.	formations- säkerhets- incidenter och förbättringar: Rapportering av informations- säkerhets- händelser	
49.	S, H	I processer för incidenthantering har hänsyn tagits till skyldigheten att göra anmälan till Transport- och kommunikationsverket.	Autentiseringslag: 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 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 informations- säkerhets- incidenter och förbättringar: Rapportering	Ansvaret för undantagssituationer och kommunikation med intressenter har fastställts.

Anvisning

211/2019 O
x.x.2019

122 (192)

			M72: 11 § Störningsanmälningar från leverantörer av identifieringstjänster till Kommunikationsverket Minst följande uppgifter ska lämnas i anmälningar om betydande hot och störningar som ska göras till Kommunikationsverket enligt 16 § i autentiseringslagen: 1) det identifieringsverktyg eller den förmedlingstjänst som störningen påverkar, 2) beskrivning av störningen och kända orsaker till störningen, 3) beskrivning av störningens konsekvenser, inklusive konsekvenser för beviljandet av nya identifieringsverktyg samt för användare, förlitande parter, andra aktörer i förtroendenätet och gränsöverskridande användning, 4) beskrivning av korrigeringsåtgärder, och 5) beskrivning av information om störningen till förlitande parter, innehavare av identifieringsverktyg, förtroendenätet och uppgift om anmälan till andra myndigheter.	ring av informations-säkerhets-händelser	
--	--	--	--	--	--

Anvisning

211/2019 O
x.x.2019

123 (192)

			Vid bedömning av hur betydande en störning är har störningen ännu större betydelse om den gäller fel i eller missbruk av en elektronisk identitet eller ett sådant hot eller en sådan störning i informationssäkerheten som äventyrar integriteten eller tillförlitligheten i identifieringen. En störning har också större betydelse om störningen påverkar förtroendenätet. Tillämpningsanvisning i MPS72 om tröskeln för att göra anmälan till Transport- och kommunikationsverket, motivering till 11 §: I 2 mom. i paragrafen finns allmänna bestämmelser om de faktorer som är relevanta med tanke på hur betydande en störning är, det vill säga anmälningströskeln. Sådana betydande störningar är bland annat - när ett identifieringsverktyg beviljas till fel person - sådana störningar i spärllisters funktion, där en uppdaterad spärllista inte är tillgänglig - intrång i en tjänsteleverantörs system - signeringsnycklar för certifikat hos en leverantör av identifieringsverktyg avslöjas - allvarliga missbruk av identifieringsverktyg, till exempel fall i anslutning till sammankoppling av identifieringsverktyg - allvarliga interna missbruk.		
--	--	--	---	--	--

			Tröskeln för när ett 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.		
--	--	--	--	--	--

5.5 Lagring och behandling av uppgifter

5 Lagring och behandling av uppgifter

M72A: 15 § Kriterier för kvalitetsrevision

Kvalitetsrevisioner av identifieringstjänster ska omfatta krav på

- 1) funktioner som påverkar tillhandahållandet av identifieringstjänsten (ett identifieringssystem)
- b) registerföring
- d) tekniska åtgärder

Allmänna krav

Autentiseringslag: 13 § Allmänna skyldigheter för leverantörer av identifieringstjänster

Hos leverantörer av identifieringstjänster ska lagringen av uppgifter som sammanhänger med identifieringen, personalen och de tjänster som köps av underleverantörer uppfylla åtminstone kraven för tillitsnivån väsentlig enligt avsnitten 2.4.4 och 2.4.5 i bilagan till förordningen om tillitsnivåer vid elektronisk identifiering.

[...]

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

Bilagan till LOA: 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.

Autentiseringslag: 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

Bilagan till LOA: 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.

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

Anvisning

211/2019 O
x.x.2019

126 (192)

NR	TILLITS- NIVÅ	SAMMANFATTNING AV KRAVEN PÅ IDENTIFIERINGSTJÄNSTER	BESTÄMMELSER	HÄNVIS- NING TILL STANDAR- DER	OBSERVATIONER
50.	S, H	Hanteringen av information avseende identifieringssystem och identifiering är systematisk och bygger på en klassificering av information .	Bilagan till LOA: 2.4.4 Registerföring 1. Registrera och lagra relevant information med hjälp av ett effektivt <u>registerhanteringssystem</u>, med beaktande av tillämplig lagstiftning och god praxis i fråga om skydd och lagring av personuppgifter. Bilagan till LOA: 2.4.6 Tekniska kontroller (controls) 1. Proportionella tekniska kontroller ska finnas för att hantera riskerna för tjänsternas säkerhet, och för att skydda <u>de behandlade uppgifternas sekretess, integritet och tillgänglighet</u>. Känsligt kryptografiskt material, om sådant används för utfärdande av medel för elektronisk identifiering och autentisering, ska skyddas från manipulation.	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	I klassificeringen beaktas bland annat kryptografisk information, information om identifieringstransaktioner, personuppgifter, affärshemligheter och information som påverkar säkerheten i systemen.

Anvisning

211/2019 O
x.x.2019

127 (192)

				integritet och personuppgifter	
51.	S, H	Planeringen av informationshanteringen har beaktat informationens hela livscykel . Den period under vilken uppgifter lagras har fastställts.	Bilagan till LOA: 2.4.4 Registerföring 2. <u>Lagra</u> – i den mån det är tillåtet enligt nationell lag eller andra nationella administrativa bestämmelser – och <u>skydda</u> register så länge som de behövs för granskning och undersökning av säkerhetsöverträdelser och för lagring, varefter registren ska förstöras på ett säkert sätt.	A.18.1.4 Efterlevnad/Efterlevnad av juridiska och avtalsmässiga krav: Skydd av personlig integritet och personuppgifter	Hänsyn ska tas bland annat till spårning av säkerhetsincidenter och till behov föranledda av behandlingsgrunder som <i>motsvarar</i> grunder enligt 24 § i autentiseringslagen. Anvisningen 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.
52.	S, H	De särskilda lagringsskyldigheter som föreskrivs i 24 § i autentiseringslagen har uppfyllts.	Autentiseringslag: 24 § Registrering och användning av uppgifter om identifieringstransaktioner och identifieringsverktyg Leverantörer av identifieringstjänster ska registrera	A.12.4.1 Driftsäkerhet: Loggning av händelser	"Om en tjänsteleverantör endast ger ut identifieringsverktyg" ... betyder i bestämmelsen identifieringstjänster som liknar BRC:s certifikat och där den som beviljar

Anvisning

211/2019 O
x.x.2019

128 (192)

			1) de uppgifter som behövs för att verifiera en enskild identifieringstransaktion eller elektronisk underskrift, 2) uppgifter om i 18 § avsedda hinder och begränsningar som gäller användningen av identifieringsverktyg, 3) i fråga om certifikat, uppgifter om innehållet i certifikat enligt 19 §. Leverantörer av identifieringsverktyg ska registrera behövliga uppgifter om den inledande identifiering av sökande som avses i 17 och 17 a § och om de handlingar eller den elektroniska identifiering som använts i den inledande identifieringen. De uppgifter som avses i 1 mom. 1 punkten ska lagras i fem år från identifieringstransaktionen. De övriga uppgifter som avses i 1 och 2 mom. ska lagras i fem år från det att ett fast kundförhållande har upphört. Personuppgifter som har uppkommit i samband med en identifieringstransaktion ska förstöras efter transaktionen, om det inte är nödvändigt att registrera dem för att verifiera en enskild identifieringstransaktion.		identifieringsverktyg inte förmedlar identifieringsmeddelanden i identifieringstransaktioner.
--	--	--	---	--	--

Anvisning

211/2019 O
x.x.2019

129 (192)

			Leverantören av identifieringstjänster får behandla registrerade uppgifter endast för att tillhandahålla och upprätthålla tjänsterna, fakturera, trygga sina rättigheter vid tvister och utreda missbruk samt på begäran av en tjänsteleverantör som använder identifieringstjänster eller en innehavare av ett identifieringsverktyg. Leverantören av identifieringstjänster ska registrera uppgifter om när och varför uppgifterna behandlats och vem som gjort det. Om en tjänsteleverantör endast ger ut identifieringsverktyg 1) tillämpas inte 1 mom. 1 punkten och 4 mom. på tjänsteleverantören, 2) räknas den registreringstid på fem år som avses i 3 mom. från det att identifieringsverktyget upphörde att gälla.		
53.	S, H	Det särskilda kravet i 24 § i autentiseringslagen på registrering av uppgifter om behandling av uppgifter som enligt lag ska lagras.	Bestämmelser om behandling vid identifieringstransaktioner och identifieringstjänster finns i 24 § i autentiseringslagen. Autentiseringslag: 24 § ...	A.12.4.1 Driftsäkerhet: Loggning av händelser	Observera spårning av behandlingsuppgifter och säkring av loggdatas integritet.

Anvisning

211/2019 O
x.x.2019

130 (192)

			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. <u>Leverantören av identifieringstjänster ska registrera uppgifter om när och varför uppgifterna behandlats och vem som gjort det.</u>	A.12.4.3 Administratörs- och operatörsloggar	
54.	S, H	Tekniska åtgärder har vidtagits för att säkerställa integritet och sekretess för uppgifter som behandlas och lagras i identifieringssystem.	Autentiseringslag: 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 Bilagan till LOA: 2.4.6 Tekniska kontroller (controls) 1. Proportionella tekniska kontroller ska finnas för att hantera riskerna för tjänsternas säkerhet, och för att skydda	A.9.1.1 Regler för styrning av åtkomst A.9.1.2 Tillgång till nätverk och nätverks-tjänster A.10.1.1 Regler för användning av krypto-	kryptering av uppgifter 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 diskryptering.

Anvisning

211/2019 O
x.x.2019

131 (192)

			de behandlade uppgifternas sekretess, integritet och tillgänglighet. Känsligt kryptografiskt material, om sådant används för utfärdande av medel för elektronisk identifiering och autentisering, ska skyddas från manipulation. M72: 5 § Tekniska informationssäkerhetsåtgärder i identifieringssystem Ett identifieringssystem ska planeras, genomföras och administreras med beaktande av följande faktorer: 3) säkerhet i användning b) behandlingsmiljön för sekretessbelagt material d) säkerhetskopiering M72: 7 § Krypteringskrav för identifieringssystem och gränssnitt [...] Följande metoder ska användas vid kryptering, nyckelutbyte och i underskrifter i anslutning till kryptering:	grafiska säkerhetsåtgärder A.12.4.2 Driftsäkerhet: Skydd av loginformation	
--	--	--	---	--	--

Anvisning

211/2019 O
x.x.2019

132 (192)

			1) Nyckelutbyte: DHE-metoder, eller ECDHE-metoder som använder elliptiska kurvor, ska användas vid nyckelutbyte. Den ändliga kroppen (finite field) som används i räkneoperationer ska utgöra minst 2 048 bitar i DHE-metoden och minst 224 bitar i ECDHE-metoden. 2) Underskrifter: Vid användning av RSA för elektronisk underskrift ska nyckeln utgöra minst 2 048 bitar. Vid användning av ECDSA-metoden för elliptisk kurva ska den ändliga kroppen nedan utgöra minst 224 bitar. 3) Symmetrisk kryptering: Krypteringsalgoritmen ska vara AES eller Serpent. Nyckeln ska utgöra minst 128 bitar. Krypteringsmoden ska vara CBC, GCM, XTS eller CTR. 4) Hashfunktioner: Hashfunktionen ska vara SHA-2, SHA-3 eller Whirlpool. Med SHA-2 avses funktionerna SHA224, SHA256, SHA384 och SHA512. [...] Man ska sörja för integriteten och sekretessen för uppgifter som lagras i identifieringssystem. Om skyddet av uppgifterna endast baserar sig på kryptering, tillämpas kraven på		
--	--	--	--	--	--

Anvisning

211/2019 O
x.x.2019

133 (192)

			underskrift, symmetrisk kryptering och hashfunktioner i 1 mom. ovan. Tillämpningsanvisning i MPS72: Om uppgifter som ska skyddas lagras i system så att deras sekretess och/eller integritet skyddas endast eller i huvudsak genom kryptografiska metoder, ska de metoder som fastställs i 1 mom. användas, <u>exklusive kraven vid nyckelutbyte. Dessa lämpar sig inte eftersom nyckelutbyte vanligen inte används vid diskryptering.</u> Alternativt är det möjligt att utnyttja exempelvis en noggrann åtkomsthantering.		
55.	H	Vid behandling och lagring av uppgifter följs de krypteringskrav som fastställs i rekommendationen /krypteringskraven på tillitsnivån hög.	MPS72: B 7.2 Rekommendation När det gäller kraven i 7 § 1 mom. rekommenderas att följande värden inom parentes tillämpas på tillitsnivån hög i identifieringssystem i stället för de värden som förutsätts: 1) Nyckelutbyte: DHE-metoder, eller ECDHE-metoder som använder elliptiska kurvor, ska användas vid nyckelutbyte. Den ändliga kroppen (<i>finite field</i>) som används i räkneoperationer ska utgöra minst 2 048 (3 072 på tillitsnivån hög) bitar i DHE-metoden och minst 224 (256 på tillitsnivån hög) bitar i ECDHE-metoden.	se ovan	Nyckelutbyte kan vara relevant mellan en identifieringstjänst och dess underleverantör.

Anvisning

211/2019 O
x.x.2019

134 (192)

			DH-grupperna 14-21, 23, 24 och 26 (15-21 på tillitsnivån hög) enligt IANAs IKEv2-parametrar uppfyller kraven ovan. 2) Underskrifter: Vid användning av RSA för elektronisk underskrift ska nyckeln utgöra minst 2 048 (3 072 på tillitsnivån hög) bitar. Vid användning av ECDSA-metoden för elliptisk kurva ska den ändliga kroppen nedan utgöra minst 224 (256 på tillitsnivån hög) bitar. 3) Symmetrisk kryptering: Krypteringsalgoritmen ska vara AES eller Serpent (på tillitsnivån hög AES eller Serpent). Nyckeln ska utgöra minst 128 (128 på tillitsnivån hög) bitar. Krypteringsmoden ska vara CBC, GCM, XTS eller CTR. 4) Hashfunktioner: Hashfunktionen ska vara SHA-2, SHA-3 eller Whirlpool. Med SHA-2 avses funktionerna SHA224, SHA256, SHA384 och SHA512 (SHA256, SHA384, SHA512 och SHA-3 på tillitsnivån hög)		
56.	S, H	Alla medel som innehåller personuppgifter eller kryptografiska eller andra känsliga	Bilagan till LOA: 2.4.6 Tekniska kontroller (controls)	A.8.3 Hantering av	hantering, förstöring, överföring

Anvisning

211/2019 O
x.x.2019

135 (192)

		uppgifter ska lagras, transporteras och bortskaffas på ett säkert sätt.	5) Alla <u>medel</u> som innehåller personuppgifter eller kryptografiska eller andra känsliga uppgifter ska lagras, transporteras och bortskaffas på ett säkert sätt.	tillgångar/Hantering av lagringsmedia A.11.2.6 Säkerhet för utrustning och tillgångar utanför organisationens lokaler A.11.2.7 Säker kassering eller återanvändning av utrustning	
--	--	---	---	--	--

5.6 Säkerhet i anläggningar

6. Säkerhet i anläggningar

M72A: 15 § Kriterier för kvalitetsrevision

Kvalitetsrevisioner av identifieringstjänster ska omfatta krav på

- 1) funktioner som påverkar tillhandahållandet av identifieringstjänsten (ett identifieringssystem)
- c) anläggningar och [...]

Autentiseringslag: 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 den förordningen

NR	TILLIT SNIVÅ	SAMMANFATTNING AV KRAVEN PÅ IDENTIFIERINGSTJÄNSTER	BESTÄMMELSER	HÄNVIS- NING TILL STANDAR- DER	OBSERVATIONER
57.	S, H	Säkerhet i anläggningar	Bilagan till LOA: 2.4.5 Anläggningar och personal	A.11.1 Fy- sisk och miljörelate-	Alla anläggningar som används vid eller påverkar tillhandahållandet av identifieringstjänster, även under- leverantörer

Anvisning

211/2019 O
x.x.2019

137 (192)

		Anläggningarna för identifieringssystem har indelats i säkerhetszoner med beaktande av hur sekretessbelagda och kritiska uppgifterna är.	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 <u>tillträde till utrymmen</u> där personliga, kryptografiska eller andra känsliga uppgifter finns eller behandlas, är begränsat till auktoriserad personal eller underleverantörer.	rad säkerhet/Säkra områden: A.11.1.1 Fysiska säkerhetsavgränsningar	Antaganden är att det räcker med att uppfylla Katakri, om tillhandahållandet av identifieringssystemet sker i de aktuella anläggningarna. De övriga standardernas omfattning har inte utretts.
58.	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	Bilagan till LOA: 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 <u>tillträde till utrymmen</u> 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	

Anvisning

211/2019 O
x.x.2019

138 (192)

		ska vara förenliga med allmänt tillämpade tekniska standarder eller minimikrav.		A.11.1.4 Skydd mot yttre och miljörelaterade hot A.11.2.1 Placering av utrustning och skydd A.11.2.3 Kablagesäkerhet	
59.	S, H	Det gäller att kontrollera att det inte finns några obehöriga utrustningar eller förbindelser i säkerhetszonerna.	Bilagan till LOA: 2.4.5 Anläggningar och personal 3. Anläggningar som används för att tillhandahålla tjänsten ska <u>kontinuerligt övervakas och skyddas</u> 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 <u>tillträde till utrymmen</u> där personliga,	A.11. Fysisk och miljörelaterad säkerhet	

			kryptografiska eller andra känsliga uppgifter finns eller behandlas, är begränsat till auktoriserad personal eller underleverantörer.		
--	--	--	---	--	--

5.7 Tillräckliga och kvalificerade personalresurser

7. Tillräckliga och kvalificerade personalresurser

M72A: 15 § Kriterier för kvalitetsrevision

Kvalitetsrevisioner av identifieringstjänster ska omfatta krav på

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

c) [...] och personal

NR	TILLITS- NIVÅ	SAMMANFATTNING AV KRAVEN PÅ IDENTIFIERINGSTJÄNSTER	BESTÄMMELSER	HÄNVIS- NING TILL STANDAR- DER	OBSERVATIONER
----	------------------	---	--------------	---	---------------

Anvisning

211/2019 O
x.x.2019

140 (192)

60.	S, H	Tillräcklig och kvalificerad personal Produktionsorganisationen i identifieringstjänster ska ha tillräcklig sakkännedom och personalresurser för att kunna säkerställa informationssäkerheten och dataskyddet.	Autentiseringslag: 13 § Allmänna skyldigheter för leverantörer av identifieringstjänster Hos leverantörer av identifieringstjänster ska ... 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. Bilagan till LOA: 2.4.5 Anläggningar och personal Kraven 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 <u>personal</u> och underleverantörer är <u>tillräckligt utbildade, kvalificerade och erfarna</u> i de färdigheter som krävs för att sköta sina roller. 2. <u>Tillräcklig personal</u> 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 – kunskap inom nödvändiga delområden (teknik, juridik bl.a. på grund av behandling av personuppgifter)
61.	S, H	Tjänster och verksamheter som har köpts för identifieringssystem har identifierats och dokumenterats.	se raden ovan	se raden ovan	Information om identifieringssystemets underleverantörer (kon-

		Underleverantörernas tillräckliga, kvalificerade personalresurser har säkerställts.		A.15.1.1 Informationssäkerhetsregler för leverantörsrelationer A.15.2.1 Övervakning och granskning av leverantörstjänster	torssystem, drifttjänster, programvaror, infrastruktur osv.) och, minst på en allmän nivå, en bedömning av underleverantörernas personalresurser.
--	--	---	--	---	---

5.8 Ledning avseende informationssäkerhet

8. Ledning avseende informationssäkerhet

M72A: 15 § Kriterier för kvalitetsrevision

Kvalitetsrevisioner av identifieringstjänster ska omfatta krav på
1) funktioner som påverkar tillhandahållandet av identifieringstjänsten (ett identifieringssystem)
a) ledning avseende informationssäkerhet

Autentiseringslag: 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 tillförlitlighet vid elektronisk identifiering och åtminstone de villkor uppfylls som gäller för tillförlitligheten väsentlig enligt avsnitten 2.4.3 och 2.4.7 i bilagan till den förordningen.

Bilagan till LOA: 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.

Bilagan till LOA: 1. Tillämpliga definitioner

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

Bilagan till LOA: 2.4.7 Efterlevnad och revision

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	TILLITS- NIVÅ	SAMMANFATTNING AV KRAVEN PÅ IDENTIFIERINGSTJÄNSTER	BESTÄMMELSER	HÄNVIS- NING TILL STANDAR- DER	OBSERVATIONER
62.	S, H	Leverantörer av identifieringstjänster har ett effektivt ledningssystem för informationssäkerhet för hantering och kontroll av informationssäkerhetsrisker i identifieringstjänster som tillhandahålls via identifieringssystem (inkl. organisatoriska och tekniska åtgärder).	Bilagan till LOA: 2.4.3 Ledning avseende informationssäkerhet Det finns ett effektivt ledningssystem för informationssäkerhet för hantering och kontroll av informationssäkerhetsrisker. Ledningssystemet för informationssäkerhet följer utprovade standarder eller principer för hantering och kontroll av informationssäkerhetsrisker.	A.5 Informationssäkerhetspolicy	Kravet på ledning avseende informationssäkerhet har uppfyllts när ISO 27001 har tillämpats utan större avvikelser.
63.	S, H	Ett ledningssystem för informationssäkerhet bygger på en eller flera allmänt kända standarder.	M72A: 4 § Krav på ledning avseende informationssäkerheten hos leverantörer av identifieringstjänster Vid ledning avseende informationssäkerheten i identifieringssystem ska leverantörerna av identifieringstjänster använda standard ISO/IEC 27001 eller någon annan allmänt känd motsvarande standard för ledning avseende in-		Motiveringen till 4 § i MPS72 innehåller en hänvisning till ISO27001.

Anvisning

211/2019 O
x.x.2019

144 (192)

			formationssäkerhet. Ledningen avseende informationssäkerheten kan också bygga på en kombination av flera standarder.		
64.	S, H	Ett ledningssystem för informationssäkerhet omfattar relevanta interna och externa tekniska, rättsliga och administrativa krav och behov som påverkar identifieringssystemet.	M72A: 4 § Krav på ledning avseende informationssäkerheten hos leverantörer av identifieringstjänster Ledningen avseende informationssäkerheten ska omfatta följande delområden som påverkar tillhandahållandet av en identifieringstjänst: 1) identifieringstjänstleverantörens omvärld som en helhet	4 organisationens omvärld	Identifieringstjänsterna ska bland annat iaktta aktuella lagar och bestämmelser, såsom autentiseringslagen, föreskrift 72 och den allmänna dataskyddsförordningen.
65.	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 säkerhetspolicyerna är omfattande och ändamålsenliga för organisationen och de objekt som ska skyddas.	M72A: 4 § Krav på ledning avseende informationssäkerheten hos leverantörer av identifieringstjänster Ledningen avseende informationssäkerheten ska omfatta följande delområden som påverkar tillhandahållandet av en identifieringstjänst: 2) styrning, organisering och administration av ledningen avseende informationssäkerheten	5 ledarskap 9.2 intern kvalitetsrevision 9.3 ledningens syn	

		Personalens och underleverantörernas ansvarsområden inom informationssäkerheten har beskrivits.		10 förbättring av ledningssystem A.5.1.1 Informations-säkerhets-policy A.6.1.1 Informations-säkerhets-roller och ansvar A.15.1.1 Informat-ionssäker-hetsregler för leve-rantörsre-lationer	
--	--	---	--	--	--

66.	S, H	Ett ledningssystem för informationssäkerhet omfattar hantering av informationssäkerhetsrisker vid tillhandahållande av identifieringstjänster. Riskhanteringen är en regelbunden, kontinuerlig och dokumenterad process. Identifierade risker klassificeras och prioriteras. Riskhanteringsprocessen identifierar riskerna för informationens sekretess, integritet och tillgänglighet. Riskhanteringsprocessen och dess resultat utnyttjas vid planering av säkerhetsåtgärder för identifieringstjänster/identifieringssystem.	Ledningen avseende informationssäkerheten ska omfatta följande delområden som påverkar tillhandahållandet av en identifieringstjänst: 3) hantering av informationssäkerhetsrisker vid tillhandahållande av en identifieringstjänst	Hänvisning i MPS72: 6 planering	riskminskning är också en del av informationssäkerhetsåtgärderna ovan
67.	S, H	Ett ledningssystem för informationssäkerhet omfattar resurser för informationssäkerheten, kompetenskrav, personalens medvetenhet om informationssä-	Ledningen avseende informationssäkerheten ska omfatta följande delområden som påverkar tillhandahållandet av en identifieringstjänst:	MPS72: 7 stöd-funktioner	

		kerheten, kommunikation och dokumentation samt administration av dokumenterad information. Uppdaterade informationssäkerhetsanvisningar och förfaranden är tillgängliga och kända för alla som deltar i uppgifterna med elektronisk identifiering. Säkerhetsutbildningen för personal är regelbunden och dokumenterad. Effektiviteten i utbildningen följs upp.	4) resurser för informationssäkerheten, kompetens, personalens medvetenhet om informationssäkerheten, kommunikation och dokumentation samt administration av dokumenterad information		
68.	S, H	I ett ledningssystem för informationssäkerhet säkerställs planering och styrning av tillhandahållandet av en identifieringstjänst så att de informationssäkerhetskrav som har fastställts för identifieringstjänster uppfylls.	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	MPS72: 8 funktion A.18.1.1 Efterlevnad/Efterlevnad av juridiska och avtalsmässiga krav: Identifiering av gällande	krav som har fastställts för identifieringstjänster dataskyddsbestämmelser i tillämpliga delar avtalsbestämmelser för förtroendet i tillämpliga delar

				lagstiftning och avtalsmässiga krav	
69.	S, H	Ett ledningssystem för informationssäkerhet omfattar regelbundna bedömningar av effektivitet och funktion i ledningen avseende informationssäkerheten.	Ledningen avseende informationssäkerheten ska omfatta följande delområden som påverkar tillhandahållandet av en identifieringstjänst: 6) bedömning av effektivitet och funktion i ledningen avseende informationssäkerheten.	MPS72: 9.1 uppföljning, mätning, analys och bedömning	Hur stor effekt har ledningen avseende informationssäkerheten på de faktorer, processer och problem som inverkar på informationssäkerheten i identifieringssystem?

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

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

M72A: 15 § Kriterier för kvalitetsrevision

Kvalitetsrevisioner av identifieringstjänster ska omfatta krav på

- 2) identifieringsmetod, dvs. identifieringsverktyg
- b) styrkande och kontroll av den sökandes identitet

Autentiseringslag: 8 § Krav på system för elektronisk identifiering

Ett system för elektronisk identifiering ska uppfylla följande krav:

- 1) identifieringsmetoden grundar sig på en identifiering enligt 17 och 17 a § så att uppgifterna om den kan kontrolleras i efterskott i enlighet med 24 §,
- 2) identifieringsmetoden medger entydig identifiering av innehavaren av identifieringsverktyget så att åtminstone de villkor uppfylls som gäller för tillitsnivån väsentlig enligt avsnitten 2.1.2, 2.1.3 och 2.1.4 i bilagan till kommissionens genomförandeförordning (EU) 2015/1502 om fastställande av tekniska minimispecifikationer och förfaranden för tillitsnivåer för medel för elektronisk identifiering i enlighet med artikel 8.3 i Europaparlamentets och rådets förordning (EU) nr 910/2014 om elektronisk identifiering och betrodda tjänster för elektroniska transaktioner på den inre marknaden, *nedan förordningen om tillitsnivåer vid elektronisk identifiering* [...]

Autentiseringslag: 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.[...]

Bilagan till LOA: 2.1.2 Styrkande och kontroll av identitet (fysisk person)

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.

Autentiseringslag: 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.

Autentiseringslag: 7 a § Identifiering av en juridisk person som ansöker om ett identifieringsverktyg

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.

Bilagan till LOA: 2.1.3 Styrkande och kontroll av identitet (juridisk person)

Bilagan till LOA: 2.1.4 Bindning mellan fysiska och juridiska personers medel för elektronisk identifiering

DEFINITIONER					
Autentiseringslag: 2 § Definitioner					
7) <i>inledande identifiering</i> verifiering av identiteten hos den som ansöker om ett identifieringsverktyg, när verifieringen sker i samband med att verktyget skaffas					
Bilagan till LOA: 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.					
NR	TILLITS- NIVÅ	SAMMANFATTNING AV KRAVEN PÅ IDENTIFIERINGSTJÄNSTER	BESTÄMMELSE	STAN- DARD	OBSERVATIONER
Metod 1: Inledande identifiering utgår från att en person visar ett identitetsbevis som är godkänt i Finland					
70.	S, H	Styrkandet av identitet bygger på identitetsbevis som är godkända enligt autentiseringslagen. När det gäller andra identitetsbevis utfärdade i stater som räknas upp i lagen har godkännandet definierats på ett tydligt sätt.	Autentiseringslag: 17 § Dokument som godkänns vid inledande identifiering, när identifieringen endast sker utifrån en identitetshandling som utfärdats av en myndighet, är ett giltigt pass eller identitetskort som har utfärdats av en myndighet i en medlemsstat inom Europeiska ekonomiska samarbetsområdet. En leverantör av identifieringsverktyg som så önskar kan också vid kontrollen av identiteten använda ett		Gäller vid användning av en inledande identifiering som bygger på identitetsbevis.

Anvisning

211/2019 O
x.x.2019

152 (192)

			giltigt pass som har utfärdats av en myndighet i någon annan stat.		
71.	S, H	Identitetsbeviset visas upp och dess äkthet kontrolleras på ort och ställe. Personalen känner till säkerhetsdetaljerna i identitetsbevis och kan kontrollera dem. Kontroll sker av att identitetsbeviset tillhör den person som visar upp beviset.	Autentiseringslag: 17 § Identifiering av en fysisk person som ansöker om ett identifieringsverktyg Vid inledande identifiering ska identifieringen av en fysisk person göras <u>personligen</u> 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 <u>en identitetshandling som utfärdats av en myndighet</u> eller ett sådant identifieringsverktyg för stark autentisering som avses i denna lag. Bilagan till LOA: 2.1.2 1. Kontroll har <u>skett av att personen innehar ett bevis som erkänns i den medlemsstat</u> där ansökan om medlet för elektronisk identitet görs <u>och som avser den påstådda identiteten</u>, och <u>beviset kontrolleras för att fastställa att det är äkta</u>, eller enligt en tillförlitlig källa existerar det och avser en verklig person,		

Anvisning

211/2019 O
x.x.2019

153 (192)

			och åtgärder har vidtagits för att minimera risken att personens identitet inte är den påstådda identiteten, varvid det tas hänsyn till exempelvis risken för att beviset har förlorats, stulits, upphävts, återkallats eller löpt ut, eller 2. <u>en identitetshandling uppvisas under ett registreringsförfarande</u> 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,		
72.	S	Identitetsbeviset visas upp och dess äkthet kontrolleras via distansuppkoppling . Personalen känner till säkerhetsdetaljerna i identitetsbevis och kan kontrollera dem.	Autentiseringslag: 17 § Identifiering av en fysisk person som ansöker om ett identifieringsverktyg Vid inledande identifiering ska identifieringen av en fysisk person göras personligen eller <u>elektroniskt</u> 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		se 3.9 i denna anvisning

Anvisning

211/2019 O
x.x.2019

154 (192)

		Kontroll sker av att identitetsbeviset tillhör den person som visar upp beviset. Tillförlitlighetskraven på distansuppkoppling beaktar angreppspotentialen på tillitsnivån väsentlig.	persons identitet kan grunda sig på <u>en identitetshandling som utfärdats av en myndighet</u> eller ett sådant identifieringsverktyg för stark autentisering som avses i denna lag. Bilagan till LOA: 2.1.2 1. Kontroll har <u>skett av att personen innehar ett bevis som erkänns i den medlemsstat</u> där ansökan om medlet för elektronisk identitet görs <u>och som avser den påstådda identiteten,</u> och <u>beviset kontrolleras för att fastställa att det är äkta,</u> eller enligt en tillförlitlig källa existerar det och avser en verklig person, och åtgärder har vidtagits för att minimera risken att persons identitet inte är den påstådda identiteten, varvid det tas hänsyn till exempelvis risken för att beviset har förlorats, stulits, upphävts, återkallats eller löpt ut, eller 2. <u>en identitetshandling uppvisas under ett registreringsförfarande</u> i den medlemsstat där handlingen utfärdades, och handlingen tycks avse den person som uppvisar den,		
--	--	---	--	--	--

Anvisning

211/2019 O
x.x.2019

155 (192)

			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,		
73.	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. Tillförlitlighetskraven på distansuppkoppling beaktar angreppspotentialen på tillitsnivån hög.	Bilagan till LOA: 2.1.2 Hög 1. Nivå väsentlig, samt ett av de alternativ som anges i leden a–c måste vara uppfyllt: a) När en person har kontrollerats och befunnits innehå fotografiskt eller <u>biometriskt identifieringsbevis som erkänns i den medlemsstat där ansökan om medlet för elektronisk identitet görs</u>, 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

Anvisning

211/2019 O
x.x.2019

156 (192)

74.	S, H	Pass eller identitetskorts giltighet kontrolleras ur polisens informationssystem eller ur tillförlitliga internationella källor.	Bilagan till LOA: 2.1.2 Styrkande och kontroll av identitet (fysisk person) Förfarandena 1 och 2, delkrav och åtgärder har vidtagits för att minimera risken att persons identitet inte är den påstådda identiteten, varvid det tas hänsyn till <u>exempelvis risken för att beviset har förlorats, stulits, upphävts, återkallats eller löpt ut,</u> Autentiseringslag: 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.

Anvisning

211/2019 O
x.x.2019

157 (192)

75.	S, H	Personers existens kontrolleras i befolkningsdatasystemet.	Autentiseringslag: 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				
76.	S	Kontrollen av en persons identitet grundar sig på sådana identifieringsverktyg för stark autentisering som är godkända enligt autentiseringslagen.	Autentiseringslag: 17 § Identifiering av en fysisk person som ansöker om ett identifieringsverktyg Vid inledande identifiering ska identifieringen av en fysisk person göras personligen <u>eller elektroniskt</u> 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	Gäller vid användning av en inledande identifiering som bygger på stark autentisering. Transport- och kommunikationsverkets register innehåller de identifieringsverktyg på tillitsnivån väsentlig som är godkända enligt autentiseringslagen.

Anvisning

211/2019 O
x.x.2019

158 (192)

			som utfärdats av en myndighet <u>eller ett sådant identifieringsverktyg för stark autentisering som avses i denna lag.</u> Bilagan till LOA: 2.1.2 4. Om medel för elektronisk identifiering utfärdas <u>på grundval av ett giltigt anmält medel för elektronisk identifiering</u> 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.		
77.	H	Kontrollen av en persons identitet grundar sig på sådana identifieringsverktyg för stark autentisering som är godkända enligt autentiseringslagen. På tillitsnivån hög kan identifieringsverktyg utfärdas utifrån elektronisk identifiering enbart med medel som ska användas på tillitsnivån hög.	Bilagan till LOA: 2.1.2 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 or-		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.

Anvisning

211/2019 O
x.x.2019

159 (192)

			gan för bedömning av överensstämmelse som avses i artikel 2.13 i förordning (EG) nr 765/2008 eller av ett likvärdigt organ, och 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")					
78.	S, H	Kontrollen av identiteten förlitar sig på ett förfarande där identiteten tidigare har styrkts och kontrollerats i annat syfte än för beviljande av ett identifieringsverktyg för stark autentisering. Förfarandet bygger på andra bestämmelser än autentiseringslagen och eIDAS och övervakas av en myndighet. Förfarandet ger en tillit som är likvärdig det förfarande enligt identifieringsbestämme-	Autentiseringslag: 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. <u>Kontrollen av identiteten kan dessutom grunda sig på ett förfarande som en offentlig eller privat aktör tidigare och i</u>		Användning av det förfarande för inledande identifiering som avses i denna punkt kräver en uttrycklig bekräftelse från Transport- och kommunikationsverket. En bedömning av överensstämmelsen ska bifogas anmälan om förfarande.

Anvisning

211/2019 O
x.x.2019

160 (192)

		ser som utgår från uppvisande av identitetsbevis eller från identifiering med elektronisk identifieringsmetod.	<u>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.</u> Bilagan till LOA: 2.1.2 Styrkande och kontroll av identitet (fysisk person) 3. Om förfaranden som tidigare använts av ett offentligt eller privat företag i samma medlemsstat <u>för andra ändamål</u> än utfärdandet av medel för elektronisk identifiering ger en tillit som är likvärdig de <u>förfaranden</u> som anges i avsnitt 2.1.2 för tillitsnivån väsentlig, behöver den enhet som ansvarar för registreringen inte upprepa de tidigare förfarandena, förutsatt att en sådan likvärdig tillit bekräftas av ett sådant organ för bedömning av överensstämmelse som anges i artikel 2.13 i Europaparlamentets och rådets förordning (EG) nr 765/2008 ⁽¹⁾ eller av ett likvärdigt organ.		
Metod 4: Inledande identifiering som utförs av polisen					

Anvisning

211/2019 O
x.x.2019

161 (192)

79.	S, H	Vid behov utförs den inledande identifieringen av polisen.	Autentiseringslag: 17 § 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. Bilagan till LOA: 2.1.2 Hög 3. 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 er-hålla sådant erkänt fotografiskt eller biometriskt identifieringsbevis tillämpas.		
-----	------	--	--	--	--

5.10 Identifieringsverktygs, eller identifieringsmetoders, livscykel

10. Identifieringsverktygs, eller identifieringsmetoders, livscykel

M72A: 15 § Kriterier för kvalitetsrevision

Anvisning

211/2019 O
x.x.2019

162 (192)

Kvalitetsrevisioner av identifieringstjänster ska omfatta krav på 2) identifieringsmetod, dvs. identifieringsverktyg a) ansökan och registrering b) [...] c) [...] d) utfärdande, leverans och aktivering e) upphävande, återkallelse och återaktivering f) förnyelse och ersättning g) [...]					
NR	TILLITS-NIVÅ	SAMMANFATTNING AV KRAVEN PÅ IDENTIFIERINGSTJÄNSTER	BESTÄMMELSER	STANDARD	OBSERVATIONER
80.	S, H	Identifieringsverktyg kombineras inte med personer, dvs. personifieras före inledande identifiering.	M72A: 6 § Krav på informationssäkerhet i identifieringsmetoder Identifieringsverktyg får inte kombineras med den sökande förrän en inledande identifiering av den sökande har gjorts, eller så ska det vid processen för beviljande av identifieringsverktyg annars säkerställas att identifieringsverktyget inte kan användas innan den sökande har gjort en inledande identifiering enligt 17 § i autentiseringslagen.		

			[...]		
81.	S, H	Personuppgifterna för fysiska personer kontrolleras i befolkningsdatasystemet vid utfärdande av ett identifieringsverktyg och regelbundet under verktygets giltighet.	Autentiseringslag: 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 M72A: 12 § Minimiuppsättning uppgifter som ska förmedlas i förtroendenätet		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.
82.	S, H	Utfärdande, leverans och aktivering av identifieringsverktyg	Autentiseringslag: 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.		Avtalsvillkor (bl.a. 15 § i autentiseringslagen) ingår i frågor som aktören själv ska ta reda på och som inte omfattas av kvalitetsrevision.

Anvisning

211/2019 O
x.x.2019

164 (192)

		Förfarandet för överlåtelse eller leverans av identifieringsverktyg säkerställer att verktyget inte obehörigt kommer i någon annans besittning.	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. Säkerställa att den sökande är medveten om villkoren förenade med användningen av medlet för elektronisk identifiering. 2. Säkerställa att den sökande är medveten om rekommenderade säkerhetsåtgärder kopplade till medlet för elektronisk identifiering. Autentiseringslag: 21 § Överlåtelse av identifieringsverktyg till sökande Leverantören av ett identifieringsverktyg ska överlåta identifieringsverktyget till sökanden på det sätt som anges i avtalet. <u>Leverantören ska säkerställa att verktyget inte obehörigt kommer i någon annans besittning vid överlåtelser, på ett sådant sätt att åtminstone de krav uppfylls som gäller för tillförlitlighet väsentligt enligt avsnitt 2.2.2 i</u>	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 överlåtelser. Se LOA guidance: Möjliga mekanismer är till exempel följande: • personlig leverans • leverans som ett rekommenderat brev • en sådan aktiveringsmetod där det rimligen kan antas att endast personen har de uppgifter som behövs för aktivering, till exempel en standardpinkod som levereras åtskild från identifieringsmedlet.
--	--	--	---	--

Anvisning

211/2019 O
x.x.2019

165 (192)

			<u>bilagan till förordningen om tillitsnivåer vid elektronisk identifiering.</u> Bilagan till LOA: 2.2.2 Utfärdande, leverans och aktivering Efter utfärdandet levereras medlet för elektronisk identifiering via en mekanism genom vilken det kan antas att medlet levereras endast till ägaren.		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.
83.	H	Utfärdande, leverans och aktivering av identifieringsverktyg Förfarandet för överlåtelse eller leverans av identifieringsverktyg säkerställer att verktyget inte obehörigt kommer i någon annans besittning.	Bilagan till LOA: 2.2.2 Utfärdande, leverans och aktivering Hög Aktiveringsprocessen kontrollerar att medlet för elektronisk identifiering endast levererades till ägaren.		
84.	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. <u>Leverantören av identifieringsverktyg ska se till att det är möjligt att när som helst göra en anmälan enligt 1 mom.</u>		jfr (autentiseringslagen innehåller ingen hänvisning till 2.2.3 i LOA, dvs. det tillämpas endast om metoden anmäls) Bilagan till LOA: 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.

Anvisning

211/2019 O
x.x.2019

167 (192)

		<u>Leverantören ska utan dröjsmål återkalla identifieringsverktyget eller förhindra dess användning efter det att anmälan har mottagits.</u> 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. <u>Systemet ska vara sådant att en tjänsteleverantör som använder identifieringstjänster lätt kan kontrollera uppgifterna i systemet vilken tid på dygnet som helst. Skyldighet att ordna möjlighet att kontrollera uppgifterna föreligger dock inte, om användning av identifieringsverktyget kan förhindras med hjälp av tekniska medel eller om verktyget kan spärras.</u> [...]		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.
--	--	--	--	---

Anvisning

211/2019 O
x.x.2019

168 (192)

		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		
--	--	---	--	--

Anvisning

211/2019 O
x.x.2019

169 (192)

			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.		
85.	S, H	Förnyande och ersättning av identifieringsverktyg	Autentiseringslag: 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. Bilagan till LOA: 2.2.4 Förnyelse och ersättning Med beaktande av riskerna för ändring i personidentifiersuppgifterna måste förnyelse eller ersättning uppfylla		Paragraf 8 i autentiseringslagen och avsnitt 2.2.1 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 överläts på nytt vid förnyelse/ersättning eller återaktivering. Se Tolkningsställningstagande dnr: Traficom/106/09.02.00/2019 (25.3.2019) Transport- och kom-

Anvisning

211/2019 O
x.x.2019

170 (192)

			samma tillitskrav som det ursprungliga styrkandet och kontrollen av identiteten eller grundas på ett giltigt medel för elektronisk identifiering med samma eller högre tillitsnivå.		<i>munikationsverkets tolkningspro-memoria om användning av kör-kort vid styrkande av en persons identitet när personens identifie-ringsverktyg är låst eller när per-sonen ska beviljas ett nytt identifi-eringsverktyg eller en ny autenti-seringsfaktor. Ställningstagandet finns på ämbetsverkets webbplats på https://www.kyberturvallisuus-keskus.fi/sv/elektronisk-identifie-ring</i>
86.	H	Förnyande och ersättning av identifie-ringsverktyg	Bilagan till LOA: 2.2.4 Förnyelse och ersättning Hög: Med beaktande av riskerna för ändring i personidentifie-ringsuppgifterna 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 tillits-nivå.		

Anvisning

211/2019 O
x.x.2019

171 (192)

			Om förnyelse eller ersättning grundas på ett giltigt medel för elektronisk identifiering, kontrolleras identitetsuppgifterna mot en tillförlitlig källa.		
--	--	--	--	--	--

6 BILAGA C Särskilda kriterier gällande lösningar för mobilidentifiering

Allmänt

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

Den första versionen av kriterierna har tagits fram **främst för tillitsnivån väsentlig**. 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.

6.1 Arkitektur, planer och modeller för hotbilder

Kriterium	Grunder	Tilläggsinformation/ kommentarer
400. Alla komponenter i en app har identifierats och klassificerats och är nödvändiga.	2.4.6 punkt 1 i LOA 8 § 1 mom. 4 punkten i autentiseringslagen	

Anvisning

211/2019 O
x.x.2019

173 (192)

401. Säkerhetskontrollerna har genomförts i både appen och på servern.	2.4.6 punkt 1 i LOA 5.1 § 2c i M72A	
402. En arkitektur på hög nivå har definierats för själva appen och alla anslutna (externa) tjänster, och informationssäkerheten har beaktats i arkitekturen.	2.4.6 punkt 1 i LOA 8 § 1 mom. 4 punkten i autentiseringslagen	
403. Känsliga uppgifter som behandlas i appen har identifierats på ett tydligt sätt.	2.4.4 punkt 1 i LOA 2.4.6 punkterna 1 och 3 i LOA	
404. Hotbilder för appen och de tjänster som appen använder samt potentiella motåtgärder har identifierats.	2.3.1 punkt 2 i LOA, väsentlig 2.3.1 i LOA, hög	Angreppspotentialerna måttlig (väsentlig) eller hög (hög) bedöms.
405. Alla säkerhetskontroller har en centraliserad implementering.	2.4.6 punkt 1 i LOA	
406. Det finns en noggrant definierad metod för att hantera krypteringsnycklar, och metoden bygger på en internationellt godkänd, aktuell standard.	2.4.6 punkt 3 i LOA 2.4.6 i LOA, väsentlig	
407. Mobilappen anger numret på den använda versionen av operativsystemet och versionen av appen till servern. Bakänden har en mekanism som förhindrar drift med alltför gamla programversioner.	2.4.6 punkt 1 i LOA 5.1 § 2c i M72A	
408. En föråldrad mobilapp uppmanar användaren att uppdatera operativsystemet och/eller mobilappen för att transaktionen ska kunna genomföras.	(2.1.1 punkt 2 i LOA)	Rekommenderad praxis/Best practise (BP). 2.1.1 i LOA ingår inte i autentiseringslagen.
409. Informationssäkerhetspraxisen används under appens hela livscykel.	2.4.6 punkterna 1 och 4 i LOA	

	8 § 1 mom. 4 punkten i autentiseringslagen	
--	--	--

6.2 Lagring av information samt dataskydd

Kriterium	Grunder	Tilläggsinformation/kommentarer
410. Säkerhetstjänster/säkerhetsfunktioner i plattformen utnyttjas i full skala när appen lagrar känsliga uppgifter.	2.4.6 punkterna 1 och 3 i LOA	
411. Användaren informeras på ett tydligt sätt vilken nivå identifieringen kommer att ske på [en lämplig plats för detta krav, gemensamt överenskommen Best practise, t.ex. med vilka grafiska element eller andra element].	2.1.1 punkt 2 i LOA	Rekommenderad praxis
412. Känslig information lagras inte utanför appmiljöns eller plattformens lager för hemligheter.	2.4.6 punkt 1 i LOA 5.1 § 3b i M72A	
413. Känslig information lagras inte i appens loggdata.	2.4.6 punkt 1 i LOA 5.1 § 3b i M72A	
414. Känslig information delas inte med externa parter, om det inte i förväg har definierats i arkitekturen.	2.4.6 punkt 1 i LOA 5.1 § 3b i M72A	

Anvisning

211/2019 O
x.x.2019

175 (192)

Kriterium	Grunder	Tilläggsinformation/ kommentarer
415. Cacheminnet är inte tillgängligt i textinmatningsfält som kan innehålla känsliga uppgifter.	2.4.6 punkt 1 i LOA 5.1 § 3b i M72A	
416. Känsliga uppgifter och hemligheter (lösenord, pinkoder) röjs inte i något skede via användargränssnitt.	2.4.6 punkt 1 i LOA 5.1 § 3b i M72A	
417. Urklipp används inte i dataelement som kan innehålla känsliga uppgifter.	2.4.6 punkt 1 i LOA 5.1 § 3b i M72A	
418. Känsliga uppgifter delas inte när IPC-mekanismer används.	2.4.6 punkt 1 i LOA 5.1 § 3b i M72A	
419. Hemligheter som används vid identifiering lagras inte i något skede och överförs inte från det datalager som används i appen någon annanstans.	2.4.6 punkt 3 i LOA, låg 2.4.6 i LOA, väsentlig 5.1 § 3b i M72A	
420. När appen övergår i bakgrunden raderas de känsliga uppgifterna från alla komponenter i användargränssnittet.	2.4.6 punkt 1 i LOA 5.1 § 3b i M72A	
421. Känsliga uppgifter lagras inte onödigt lång tid i appens minne, och när uppgifterna inte längre behövs raderas de från minnet direkt.	2.4.6 punkt 1 i LOA 5.1 § 3b i M72A	
422. Appen rekommenderar att slutanvändaren tar i bruk enhets-säkerhet på miniminivå (skydd av telefon med pinkod och/eller en biometrisk mekanism för öppnande av telefon eller motsvarande).	2.1.1 punkt 2 i LOA	Rekommenderad praxis

Anvisning

211/2019 O
x.x.2019

176 (192)

Kriterium	Grunder	Tilläggsinformation/ kommentarer
423. Användaren informeras om bästa praxis som denne bör följa vid behandling av personliga uppgifter.	2.1.1 punkt 2 i LOA	Rekommenderad praxis

6.3 Krypteringskrav

Kriterium	Grunder	Tilläggsinformation/ kommentarer
424. Appen använder inte enbart symmetriska krypteringsmetoder och hårdkodade nycklar som krypteringsmetod.	5.1 § 2g och 7 § i M72A	
425. Appen använder krypteringsmetoder som lämpar sig för olika användningstillfällen och som konstaterats vara bra.	5.1 § 2g i M72A	
426. Appen använder vare sig krypteringsprotokoll eller algoritmer som är föråldrade eller som har konstaterats vara dåliga.	5.1 § 2g i M72A	
427. Appen använder inte krypteringsnycklar på nytt.	2.4.6 punkt 1 i LOA 8 § 1 mom. 4 punkten i autentiseringslagen	
428. Den använda slumpalsgeneratoren är tillräckligt säker och högkvalitativ.	2.4.6 punkt 1 i LOA 8 § 1 mom. 4 punkten i autentiseringslagen	
429. En signaturreäknare används, dvs. servern kan eventuellt upptäcka försök att kлона appen.	2.3.1 punkt 2 i LOA, väsentlig 2.3.1 i LOA, hög	
430. Appen innehåller/använder inga hårdkodade användarnamn eller lösenord.	2.4.6 punkt 1 i LOA 6.2 och 6.3 i M72A	

Kriterium	Grunder	Tilläggsinformation/ kommentarer
431. 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.	2.4.6 punkterna 1 och 3 i LOA 2.4.6 i LOA, hög 5.1 § 2g i M72A	

6.4 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.

Kriterium	Grunder	Tilläggsinformation/ kommentarer
432. När appen specificeras i registreringsskedet säkerställs det att appen binds till ägaren av identifieringsverktyget.	1 (definitioner) punkt 2 i LOA 2.2.1 punkt 2 i LOA	
433. De hemligheter som genomför identifieringen är skyddade mot missbruk och endast tillgängliga på ett på förhand fastställt säkert sätt.	2.4.6 punkt 3 i LOA 2.4.6 i LOA, väsentlig 6 § 3 i M72A	Till exempel en privat nyckel.
434. Hemligheter/autentiseringsnycklar är individuella.	5.1 § 2g i M72A	
435. De asymmetriska hemligheter som genomför identifieringen skapas i terminalutrustningen (nyckelpar, någon annan hemlig nyckel eller hemlighet).	5.1 § 2g i M72A 5.1 § 3b i M72A	jfr RTS
436. Om de hemligheter som genomför identifieringen skapas ut- anför enheten, levereras de till den använda enheten på ett säkert sätt.	2.4.6 punkt 2 i LOA 2.4.6 i LOA, väsentlig 5.1 § 3b i M72A	jfr RTS
437. Identifieringen får inte enbart bygga på en delad hemlighet.	2.2.1 punkt 2 i LOA, väsentlig	

Anvisning

211/2019 O
x.x.2019

180 (192)

Kriterium	Grunder	Tilläggsinformation/ kommentarer
438. Vid formatering av en app binds hemligheterna till terminalutrustningen så att de inte kan användas i en annan enhet genom kopiering eller överförs till en annan enhet så att hemligheterna kan användas på enheten.	2.2.1 punkt 2 i LOA, väsentlig 6 § 3 i M72A	
439. Appen lagrar inte i något skede identifieringsuppgifter/inloggningsuppgifter på klarspråk (lösenord, pinkoder, användarnamn osv.).	2.2.1 punkt 2 i LOA, väsentlig 2.2.1 punkt 2 i LOA, hög 2.3.1 punkt 2 i LOA, väsentlig 2.3.1 punkt 2 i LOA, hög 2.4.6 punkt 3 i LOA	
440. Om appen skickar meddelanden till servern där valideringen av meddelandena i bakänden leder till identifiering, ska meddelandena skickas på ett säkert sätt genom användning av aktuella och godkända krypteringsprotokoll, till exempel Mutual/2-way TLS 1.2 eller senare version.	2.4.6 punkt 2 i LOA 5.1 § 2g i M72A 7 § 1-4 i M72A	
441. Om personuppgifter byts mellan appen och servern, skyddas uppgifterna även genom kryptering på meddelandenivå.	2.4.6 punkt 2 i LOA 2.4.6 i LOA, väsentlig 5.1 § 2g i M72A	
442. Om appen bygger på en metod baserad på engångslösenord eller den innehåller en komponent som bygger på en sådan metod, ska	5.1 § 2g i M72A	

Kriterium	Grunder	Tilläggsinformation/ kommentarer
lösningar som har konstaterats vara bra och som bygger på standarder användas vid skapandet av engångslösenord (OTP).		
443. För lagring av hemligheter som används vid identifiering används om möjligt tjänster/hårdvaruegenskaper som tillhandahålls av plattformen, såsom säkerhetslösning på hårdvarunivå eller sådana tjänster för lagring av känslig information som tillhandahålls av operativsystemet (t.ex. keychain).	5.1 § 2c i M72A 5.1 § 3b i M72A	
444. 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 nätuppkoppling saknas och meddelandena inte kan skickas till servern på ett säkert sätt, följer appen själv samma logik. (PSD2: regeln om 5 fel)	2.4.6 punkt 1 i LOA 5.1 § 2f i M72A	jfr RTS och SCA [Öppnande? Eller identifikatorer som har lagrats i operativsystemet, exempelvis fingeravtryck?]
445. Mellan appen och servern används tekniker som kan förhindra replay-angrepp och vid nonce: Bounded Probability of a Birthday Collision	2.3.1 punkt 2 i LOA, väsentlig 2.3.1 i LOA, hög	
446. Vid användning av sessionsidentifikatorer används slumpmässiga sessionsidentifikatorer.	2.3.1 punkt 2 i LOA, väsentlig 2.3.1 i LOA, hög	
447. (Programvaru/OAuth) Vid lösningar med token-baserad teknik säkerställs det att token har signerats med en godkänd säker algoritm.	2.4.6 punkt 2 i LOA 7.1 § 2 i M72A	

Kriterium	Grunder	Tilläggsinformation/ kommentarer
448. En sessions eller tokens giltighetstid fastställs i bakänden.	2.4.6 punkterna 1 och 4 i LOA	
449. I (identifierings)bakänden fastställs behörighetspolicyer för åtkomst till målappen/tjänsten.	2.4.6 punkterna 1 och 4 i LOA	
450. Om personer som är registrerade i terminalutrustningen inte kan skiljas åt vid genomförande av autentiseringsfaktorn på grund av plattformens egenskaper, gäller det att använda en kombination så att användaren kan specificeras på ett tillförlitligt sätt (t.ex. terminalutrustning = administration, pinkod för hemlighet = information och fingeravtryck = egenskap).	2.2.1 punkt 1 i LOA, väsentlig	Till exempel Apple iOS, biometri
451. 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.	2.2.1 punkt 1 i LOA, väsentlig 2.1.1 punkt 2 i LOA 1 (definitioner) punkt 2 i LOA	2.1.1 i LOA Ingår inte i autentiseringslagen; god praxis.
452. Om appen 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 nya kombinationen	1 (definitioner) punkt 2 i LOA 2.2.1 punkt 2 i LOA, väsentlig 2.2.4 i LOA, väsentlig	Autentiseringsfaktorernas oberoende ska säkerställas. Det innebär till exempel byte av

Kriterium	Grunder	Tilläggsinformation/ kommentarer
möjliggör. Kombinationerna ska dokumenteras och bedömas som enskilda helheter.		autentiseringsfaktor i en kategori eller tillägg av en ny autentiseringsfaktor i en kategori, varvid det används autentiseringsfaktorer från tre kategorier.
453. 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.	1 (definitioner) punkt 3 i LOA 2.2.1 punkt 2 i LOA, väsentlig 2.3.1 punkt 2 i LOA, väsentlig	
454. Vid genomförande av en biometrisk autentiseringsfaktor används endast gränssnitt som tillhandahålls av plattformen.	2.4.6 punkt 1 i LOA 5.1 § 2c i M72A	
455. Vid utnyttjande av en biometrisk faktor överförs själva biometrisk inspelningen (fingeravtrycket, ansiktsfotot, den skannade bilden på irisen) inte från appen någon annanstans.	2.2.1 punkt 2 i LOA, väsentlig 2.3.1 punkt 2 i LOA, väsentlig	
456. Känsliga uppgifter eller personuppgifter som används i registreringsskedet kan endast med säkra metoder överföras till bakänden för bedömning.	2.4.6 punkt 2 i LOA	

Anvisning

211/2019 O
x.x.2019

184 (192)

Kriterium	Grunder	Tilläggsinformation/ kommentarer
457. Användaren ska ha möjlighet att tillfälligt spärra en hemlighet i a) en enhet, b) flera enheter eller c) alla enheter på en gång.	2.2.3 punkt 1 i LOA, väsentlig	
458. För att en tillfälligt spärrad hemlighet ska kunna öppnas krävs det alltid identifiering på minst samma nivå som den nivå som används när appen tas i bruk.	2.2.3 punkt 3 i LOA, väsentlig	
459. Användaren ska ha möjlighet att på ett säkert sätt inaktivera identifieringsappen och hemligheten i a) en enhet, b) flera enheter eller c) alla enheter.	2.2.3 punkterna 1 och 2 i LOA, väsentlig	
460. Det ska vara möjligt att tillfälligt spärra och inaktivera hemligheter i enskilda enheter även i bakänden.	2.2.3 punkterna 1 och 2 i LOA, väsentlig	
461. Identifieringen binds till önskad transaktion eller webbläsarsession, dvs. identifieringsappen visar på ett tydligt sätt information om vad som sker.		Till exempel RTS, dynamisk länkning. EU 2018/389
462. Identifieringsappen genomför även så kallad binding message där användaren får möjlighet att på ett begripligt sätt länka identifieringen i mobilenheten exempelvis med en webbläsarsession.	2.3.1 punkt 2 i LOA, väsentlig	
463. Om identifieringsappens svar bygger på en asymmetrisk signatur, används principen WYSIWYS, dvs. den information som visas för användaren är också en information som ska signeras.	2.3.1 punkt 2 i LOA, väsentlig	

Anvisning

211/2019 O
x.x.2019

185 (192)

Kriterium	Grunder	Tilläggsinformation/ kommentarer
464. Appen styr användaren att välja starka pinkoder.	2.1.1 punkt 2 i LOA, väsentlig 5.1 § 2g i M72A	2.1.1 i LOA ingår inte i autenti- seringslagen; god praxis.
465. Appen godtar inte pinkoder som kan gissas lätt och inte heller andra hemligheter som bygger på användarens minne.	2.3.1 punkt 2 i LOA, väsentlig 2.4.6 punkt 1 i LOA	
466. Användarens indata, till exempel pinkoder, valideras på ett säkert sätt.	2.3.1 punkt 2 i LOA, väsentlig 5.1 § 3b i M72A	
467. Om appen utnyttjar terminalutrustningens säkerhetsegenskaper på hårdvarunivå, exempelvis TEE eller motsvarande, meddelar appen den använda komponenten på hårdvarunivå och eventuell övrig information till servern i anslutning till formateringen så att servern kan fastställa om det använda systemet är sårbart på hårdvarunivå (även i fortsättningen).	2.4.6 punkt 1 i LOA 5.1 § 3d i M72A	Ny, 29.4.2019: CVE-2018-11976 → Servern ges möjlig- het att reagera om det är känt att en komponent på hårdvaru- nivå är sårbar.

6.5 Datakommunikation

Kriterium	Grunder	Tilläggsinformation/ kommentarer
468. Nättrafiken mellan appen och servern är skyddad med internationellt eller nationellt rekommenderade protokoll, och de skyddade kanalerna används i appen på ett enhetligt sätt.	2.4.6 punkt 2 i LOA 5.1 § 2g i M72A	Några krypteringskrav har inte fastställts för <i>interna</i> förbindelser i identifieringssystem. Utgångspunkten kan dock anses vara de krypteringsprotokoll för datakommunikation <i>mellan leverantörer</i> som avses i 7 § i M72A.
469. Appen kontrollerar inställningarna i krypteringsprotokollet TLS (eller motsvarande) och säkerställer att de följer god praxis.	2.4.6 punkt 2 i LOA 5.1 § 2g i M72A	Några krypteringskrav har inte fastställts för <i>interna</i> förbindelser i identifieringssystem. Utgångspunkten kan dock anses vara de krypteringsprotokoll för datakommunikation <i>binääri</i> som avses i 7 § i M72A.
470. Appen använder hard-fail certificate pinning.	2.4.6 punkt 2 i LOA	

Kriterium	Grunder	Tilläggsinformation/ kommentarer
471. I kritiska funktioner, såsom formatering och skapande av hemligheter för enskilda användare, använder appen inte osäkra kommunikationskanaler, till exempel e-post, sms.	1 (definitioner) punkt 2 i LOA 2.2.1 punkt 2 i LOA, väsentlig	I praktiken ska personifieringen i appen bygga på stark autentisering.
472. Appen använder endast uppdaterade programbibliotek för att genomföra förbindelserna och informationssäkerheten.	2.4.6 punkterna 1 och 4 i LOA	

6.6 Interaktion mellan plattform och app

Kriterium	Grunder	Tilläggsinformation/ kommentarer
473. Appen begär endast de behörigheter som den behöver av terminalutrustningen.	2.4.6 punkt 1 i LOA 5.1 § 2c i M72A	
474. All indata som kommer utanför appen/från externa källor kontrolleras och renas.	2.4.6 punkt 4 i LOA 5.1 § 2c i M72A	

Anvisning

211/2019 O
x.x.2019

188 (192)

Kriterium	Grunder	Tilläggsinformation/ kommentarer
475. Vid användning av ett separat URL-schema eller IPC-mekanismer överförs information inte utanför appen, om mekanismerna inte är skyddade.	2.4.6 punkt 2 i LOA 5.1 § 2c i M72A	
476. I WebView-komponenter används endast nödvändiga protokoll och de övriga spärras eller det säkerställs att dessa inte är tillgängliga.	2.4.6 punkt 1 i LOA 5.1 § 2c i M72A	
477. Utgångspunkten är att JavaScript inte är tillgängligt i WebView-komponenterna.	2.4.6 punkt 1 i LOA 5.1 § 2c i M72A	
478. De ursprungliga metoderna har förhindrats om programversionen av plattformen har konstaterats vara sårbar.	2.4.6 punkt 1 i LOA 5.1 § 2c och 3d i M72A	I fråga om JavaScript kan till exempel genomförandet av en äldre version av operativsystemet Android vara oskyddat.
479. Om de ursprungliga metoderna i appen är öppna för WebView-komponenter, säkerställs det att endast JavaScript som ingår i applikationspaketet får aktiveras.	2.4.6 punkt 1 i LOA 5.1 § 2c i M72A	
480. WebView-komponenternas åtkomst till lokala resurser är förbjuden/förhindrad.	2.4.6 punkt 1 i LOA 5.1 § 2c i M72A	
481. Vid serialisering av objekt används skyddade API.	2.4.6 punkterna 1 och 3 i LOA 2.4.6 i LOA, väsentlig	

Kriterium	Grunder	Tilläggsinformation/ kommentarer
	5.1 § 2c i M72A	

6.7 Programvarukodens säkerhet, kvalitet och utvecklingsmiljö

Kriterium	Grunder	Tilläggsinformation/ kommentarer
482. Appen har signerats och levererats med ett giltigt och tillförlitligt certifikat.	2.4.6 punkt 1 i LOA	
483. Appen har tagits fram i release mode, dvs. så att till exempel felsökning är svårare.	2.4.6 punkt 1 i LOA 5.1 § 2c i M72A	
484. Vid applikationsutveckling används god informationssäkerhetspraxis för programutveckling/kodning.	2.4.6 punkt 1 i LOA 5.1 § 2c i M72A	All JavaScript som används ska koda och renas i syfte att minska XSS angreppsrisken.
485. Symbolerna för felsökning har tagits bort från det binära tal-systemet.	2.4.6 punkt 1 i LOA 5.1 § 2c i M72A	

Anvisning

211/2019 O
x.x.2019

190 (192)

Kriterium	Grunder	Tilläggsinformation/ kommentarer
486. Felsökningskoden och felsökningsmeddelandena har tagits bort.	2.4.6 punkt 1 i LOA 5.1 § 2c i M72A	
487. Tredje parts samtliga komponenter som används av mobilappen har identifierats samt kontrollerats och analyserats med tanke på kända sårbarheter.	2.4.6 punkt 4 i LOA 5.1 § 3d i M72A	
488. Appen söker och behandlar alla incidenter på ett ändamålsenligt sätt.	2.4.6 punkt 4 i LOA 5.1 § 2f och 3d i M72A	
489. Appen eller servern minimerar informationen i felmeddelanden.	2.4.6 punkt 1 i LOA 5.1 § 2c i M72A	
490. Utgångspunkten är att felbehandlingen vid säkerhetskontroller förhindrar åtkomst i felsituationer.	2.4.6 punkt 1 i LOA 5.1 § 2c i M72A	
491. Minnet reserveras, används och frigörs på ett säkert sätt.	2.4.6 punkt 1 i LOA 5.1 § 2c i M72A	
492. De informationssäkerhetsegenskaper som tillhandahålls av plattformen/utvecklingsmiljön är tillgängliga.	2.4.6 punkt 1 i LOA 5.1 § 2c i M72A	

6.8 Säkerhetskontroller och skydd (EN: Resilience)

Kriterium	Grunder	Tilläggsinformation/ kommentarer
493. Appen använder den skyddsmekanism som presenteras i detta avsnitt.	2.4.6 punkt 1 i LOA	Programvarans kapacitet att skydda mot angrepp ska bedömas som helhet.
494. Appen har en eller flera funktioner som försöker upptäcka enheter som används av tredje part eller är rotade.	2.4.6 punkt 4 i LOA 5.1 § 2f i M72A	
495. Appen skickar ett meddelande till genomförandet i bakänden när den har upptäckt en enhetsplattform som har rotats till en sandlåda eller som används av tredje part, eller kan själv fastställa vad som ska göras när miljön är rotad eller används av tredje part.	2.4.6 punkt 4 i LOA 5.1 § 2f i M72A	
496. Appen försöker förhindra försök till felsökning och reagerar om den upptäcker att en lösning som används för felsökning har anslutits till appen.	2.4.6 punkt 1 i LOA 5.1 § 2c i M72A	
497. Appen försöker upptäcka och reagera om filer eller kritiska data/filer i appens sandlåda förändras under nedladdningen.	2.4.6 punkt 4 i LOA 5.1 § 2f i M72A	
498. Appen upptäcker och reagerar på allmänt tillämpade verktyg som försöker utreda källkoden för appen (reverse engineering).	2.4.6 punkt 4 i LOA 5.1 § 2f i M72A	
499. Appen upptäcker och reagerar om den används i en emulator.	2.4.6 punkt 4 i LOA	

Anvisning

211/2019 O
x.x.2019

192 (192)

Kriterium	Grunder	Tilläggsinformation/ kommentarer
	5.1 § 2f i M72A	
500. Appen upptäcker och reagerar på ett ändamålsenligt sätt när den har upptäckt förändringar/manipulation i minnesutrymmet.	2.4.6 punkt 4 i LOA 5.1 § 2f i M72A	
501. Lösningar som är viktiga/relevanta för appen är i tillämpliga delar krypterade på informationssystemnivå. Sådana lösningar kan inte dekrypteras genom analyser.	2.4.6 punkterna 1 och 3 i LOA 2.4.6 i LOA, väsentlig 5.1 § 3b i M72A 5.1 § 2c i M72A	