Anvisningspromemoria för periodiska bedömningar av identifieringstjänster 2023

Allmänt

När periodiska bedömningar beställs/utförs år 2023 använder Transport- och kommunikationsverket denna promemoria för att ta fram olika teman. Temana gäller brister som upprepats i de tidigare periodiska bedömningarna eller förbättringsförslag till bedömningsprocessen. Syftet med rådgivningen är att minska behovet av preciserande kompletteringsbegäranden och att snabba upp behandlingen av bedömningen både hos leverantörer av identifieringstjänster och hos Traficom.

Författningar

I 29 § i lagen om stark autentisering och betrodda elektroniska tjänster (617/2009, autentiseringslagen) finns bestämmelser om skyldighet för en leverantör av identifieringstjänster att regelbundet låta ett sådant bedömningsorgan som nämns i 28 § bedöma om identifieringstjänsten uppfyller kraven på interoperabilitet, informationssäkerhet, dataskydd och annan tillförlitlighet som föreskrivs i lagen om stark autentisering och betrodda elektroniska tjänster. Syftet med en kvalitetsrevision är att bedöma i vilken utsträckning en identifieringstjänst och företagets verksamhet uppfyller de uppställda kraven.

Enligt 31 § i autentiseringslagen är inspektionsberättelsen i kraft den tid som anges i den standard som användes vid bedömningen, dock högst 2 år.

Bestämmelser om Transport- och kommunikationsverkets rätt att meddela närmare föreskrifter om bedömningsgrunderna vid bedömningen av överensstämmelsen hos en identifieringstjänst finns i 42 §.

Bestämmelser om förutsättningarna för identifieringstjänster ingår i lagen om stark autentisering och betrodda elektroniska tjänsten samt delvis i Europeiska unionens kommissions genomförandeförordning (EU) 2015/1502 (förordning om tillitsnivåer) och i bilagan till den.

I punkt 15 i Transport- och kommunikationsverkets föreskrift M72 B/2022 preciseras de kravområden som ska ingå i en oberoende bedömning. I punkt 16 i föreskriften preciseras de kravområden som en leverantör av identifieringstjänster kan visa en egen utredning om.

Transport- och kommunikationsverkets anvisning 211/2019 O om bedömning av elektroniska identifieringstjänster, som utfärdats som stöd för kvalitetsrevision av identifieringstjänster, innehåller de allmänna kriterierna för kvalitetsrevision av identifieringstjänster samt särskilda kriterier gällande lösningar för mobilidentifiering. Leverantörerna av identifieringstjänster kan använda de nämnda kriterierna eller andra kriterier eller kombinationer av andra kriterier som uppfyller kraven i punkt 15 § i föreskrift M72 B.

Tidsplan

Inspektionsberättelserna jämte bilagor ska skickas till Transport- och kommunikationsverket senast 31.12.2023.

Aktörerna kan lämna in den periodiska bedömningen även tidigare utan att det påverkar tidtabellen för följande bedömningsomgång.

Användning av övriga bedömningar eller certifieringar

Om det gjorts bedömningar av identifieringssystemet åren 2022 och 2023 kan de användas som en del av den periodiska bedömningen och för deras del behöver bedömningen inte göras på nytt, om den bedömda helheten inte har förändrats efter bedömningen. Bedömningarna skickas till Traficom även om de redan skickats i samband med en tidigare ändringsanmälan.

Certifieringar kan tillgodoräknas till den del de motsvarar bestämmelserna i autentiseringslagen och föreskrift M72 B. Till ämbetsverket ska lämnas en utredning om certifieringens andel av bedömningen av identifieringstjänster och hur överensstämmelse med autentiseringslagen och föreskrift M72 B/2022 har bedömts.

Saker som ska beaktas i den periodiska bedömningen år 2023

Kvalitetsrevisorns iakttagelser och korrigeringar

Om det vid bedömningen genast observeras avvikelser som ska åtgärdas ska de beaktas i materialet som skickas till ämbetsverket. Aktören ska anteckna kvalitetsrevisorns iakttagelser i den Excel-fil som skickas till ämbetsverket samt svara på iakttagelserna samtidigt.

Om det är möjligt att göra de behövliga korrigeringarna ska de göras omedelbart och beaktas i det material som skickas till ämbetsverket. Om det konstaterats bristfälligheter i bedömningsrapporten och om det inte är möjligt att göra korrigeringarna omedelbart ska leverantören av identifieringstjänster skicka en heltäckande utredning om de planerade korrigerande åtgärderna och om deras tidtabell.

Syftet är att det inte skulle vara nödvändigt att skriva sådana frågor i beslutet om periodisk bedömning som revisorn redan beaktat och antecknat för korrigering. Aktören är redan medveten om dessa iakttagelser.

Bedömningens längd och omfattning

Bedömningen ska täcka hela identifieringssystemet. Bedömningen ska även omfatta tekniska prov (teknisk observation).

Kvalitetsrevisionens tillämpningsområde ska omfatta kvalitetsrevisionens omfattning och gränser, såsom de verksamhetsställen, organisationsenheter, informationssystem, funktioner och processer som ska kvalitetsrevideras. Det är möjligt att använda ett urvalsförfarande vid kvalitetsrevisioner, vilket betyder att det inte är nödvändigt att utföra en kvalitetsrevision för varje verksamhetsställe vid varje omgång. Om helheten av kvalitetsrevisionen består av flera än en kvalitetsrevision ska kvalitetsrevisionerna i sin helhet dock gälla hela identifieringssystemet.

Krav på åtgärdandet i beslutet och bedömning av dem

Om ämbetsverkets beslut av den periodiska bedömningen omfattar kritiska avvikelser som kräver åtgärdande så snabbt som möjligt bör de utföras och verifieras i enlighet med inspektionspraxis samt inom den av ämbetsverket utsatta tiden ska man skicka ett färdigt svar till ämbetsverket, inte separata bilagor. Det vore bra om svaret förses med utvärderarens utlåtande om verifiering av åtgärdandet.

Syftet är att de begärda korrigeringarna har antingen gjorts eller är försedda med en plan för åtgärdande och svaret om detta skickas till ämbetsverket. Syftet är inte att ge ämbetsverket separata bilagor så att ämbetsverket behöver göra en ny bedömning i samband med genomgång av ändringarna.

Plan för verksamhetens upphörande

Leverantörer av identifieringstjänster ska enligt autentiseringslagen ha en omfattande plan för identifieringstjänstens upphörande. Syftet med planen för verksamhetens upphörande är att vara ett hjälpmedel för aktören vid eventuella ändringar eller upphörande. Det väsentliga är inte en detaljerad plan utan att man har planerat och listat de nödvändiga åtgärderna och faserna.

I planen ska man fästa uppmärksamhet till exempel vid en eventuell nedläggning av systemen, hur och när användarna, förtroendenätet och de förlitande parterna underrättas om upphörandet och hur man sörjer för lagringen av uppgifterna enligt 24 § i autentiseringslagen efter det att verksamheten upphört. Planen för verksamhetens upphörande ska vara daterad och uppdaterad.

Riskbedömning

Identifieringsmetoden ska basera sig på en riskbedömning. Den ska utgöra en del av bedömningsrapporten. Riskbedömningen ska visa att metoden och de relaterade riskhanteringsegenskaperna uppfyller kraven på tillitsnivån väsentlig enligt LoA (t.ex. engångslösenordslista, operativsystemversion som stöds i mobilenheten osv.). Lämpligheten kan visas genom att beräkna angreppspotential.

Rapportering till Traficom och Excel-fil

Traficom har gjort en modell för bedömningen. Med tanke på att de periodiska bedömningarna sker smidigt är det önskvärt att denna tabell används som stöd/bilaga till bedömningsorganets verbala bedömningsrapport i samband med de periodiska bedömningarna.

Genom att använda tabellen kan leverantören av identifieringstjänster också enklare konkurrensutsätta bedömningar och försäkra sig om att alla nödvändiga delar blir bedömda. Tabellen baserar sig på Traficoms bedömningskriterier i anvisningen 211/2019 O. Både tabellen och anvisningen 211 uppdateras under våren 2023. Om bedömningarna har startat innan den nya anvisningen har publicerats ska aktören säkerställa att förändringarna i föreskrift 72B beaktas i bedömningen.

Traficom påminner er också om att ju heltäckande bedömningsrapporterna och bilagorna till Traficom är, desto bättre går det att granska den periodiska bedömningen. Det är också viktigt att hålla fast vid de utsatta tiderna så att bedömningsomgångarnas tidtabell blir standardiserad och att tidsfristerna för korrigeringar förblir jämlika.