Viestintävirasto

12.12.2018

Dnr:
1003/620/2018

Kommunikationsverkets[1] anvisningar om bedömning av överensstämmelsen hos en identifieringstjänst 2019

1 Bakgrund

1.1 Arten av denna promemoria om tolkning

Till denna promemoria har Kommunikationsverket samlat anvisningar i frågor gällande tillämpning av kraven för bedömning av identifieringstjänster. Anvisningarna har utarbetats på en allmän nivå. Kommunikationsverket övervakar på eget initiativ att alla krav för bedömning av en identifieringstjänst uppfylls enligt riktlinjerna i avsnitten 2.1 och 2.2.

Vid behov kan Kommunikationsverket komplettera promemorian.

Leverantören av identifieringstjänster ska sköta ledningen avseende informationssäkerheten i identifieringstjänsterna och på ett ändamålsenligt sätt beakta riskerna och hoten mot sina tjänster. Om Kommunikationsverket är tvunget att fatta tillsynsbeslut för enskilda tjänsteleverantörer, beaktar verket alla fakta i det aktuella fallet och de föreskrivna kraven.

1.2 Bestämmelser

I 29 § i lagen om stark autentisering och betrodda elektroniska tjänster 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 enligt denna lag. Syftet med en kvalitetsrevision är att bedöma i vilken utsträckning en identifieringstjänst och företagets verksamhet uppfyller de uppställda kraven.

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

I 15 § i Kommunikationsverkets föreskrift 72A/2018 M preciseras de kravområden som ska ingå i en oberoende bedömning. I 16 § i föreskriften preciseras de kravområden som en leverantör av identifieringstjänster kan visa en egen utredning om.

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

De nämnda bestämmelserna i autentiseringslagen trädde i kraft den 1 juli 2016. Enligt övergångsbestämmelsen skulle inspektionsberättelsen lämnas till Kommunikationsverket senast den 31 januari 2017.

[1] Kommunikationsverket fortsätter som en del av Transport- och kommunikationsverket (Traficom) 1.1.2019.

Viestintävirasto

Enligt 10 § i autentiseringslagen ska anmälan om inledande av verksamhet innehålla 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, och Kommunikationsverket ska utan dröjsmål skriftligen underrättas om ändringar i de anmälda uppgifterna.

Kommunikationsverket har utfärdat anvisningar om modellkriterier för kvalitetsrevision 211/2016 och om inspektionsberättelse 215/2016. Uppdateringen och kompletteringen av anvisningarna inleddes den 28 november 2018.

1.3 Behandling av de inspektionsberättelser som lämnades in i januari 2017

Före utgången av januari 2017 hade Kommunikationsverket fått inspektionsberättelser av alla de leverantörer av tjänster för stark autentisering som var införda i ett register enligt 12 § i autentiseringslagen redan innan lagändringarna hade trätt i kraft.

Kommunikationsverket har begärt kompletteringar i alla inspektionsberättelser och i vissa berättelser två gånger.

En del av leverantörerna av identifieringstjänster har dessutom lämnat in anmälningar om ändringar och inspektionsberättelser för anmälningarna.

I juli 2017 gjorde Kommunikationsverket en första halvtidsöversyn över alla inspektionsberättelser. Översynen fokuserade på vissa delar så att tillitsnivån i nästan alla tjänster för stark autentisering infördes i det register som avses i 12 § i lagen, trots att det fanns några brister i uppgifterna eller implementeringen. I fråga om Befolkningsregistercentralens identifieringscertifikat registrerades medborgarcertifikat och organisationscertifikat. Vad gäller de övriga pågår behandlingen fortfarande.

1.4 Anmälningar och inspektionsberättelser som har lämnats in vid andra tidpunkter

Utöver dem som nämns i avsnittet ovan har Kommunikationsverket fått anmälningar och inspektionsberättelser av en del nya leverantörer av identifieringstjänster. Kommunikationsverket har krävt att dessa inspektionsberättelser i alla väsentliga delar ska kompletteras innan identifieringstjänsten kan registreras.

2 Frågor och Kommunikationsverkets anvisningar och riktlinjer

2.1 När ska en ny inspektionsberättelse lämnas till Kommunikationsverket om leverantören av identifieringstjänster lämnade in inspektionsberättelsen i januari 2017?

Enligt lagen är inspektionsberättelsen i kraft högst i två år. I anvisning 215/2016 fastställer Kommunikationsverket att inspektionsberättelsen ska lämnas in senast två år efter att den föregående inspektionsberättelsen godkänts.

Viestintävirasto

Den tidpunkt från vilken två år räknas lämnar rum för tolkning, eftersom Kommunikationsverket har varit tvunget att begära kompletteringar i inspektionsberättelserna och behandlingen av berättelserna fortfarande pågår.

Kommunikationsverket har preliminärt meddelat leverantörerna av identifieringstjänster att verket utreder följande två tolkningsalternativ för den tidpunkt då en inspektionsberättelse kan anses vara godkänd:

- när tillitsnivån för en redan registrerad identifieringstjänst registreras (vilket med andra ord i huvudsak gjordes för gamla tjänster i juli 2017), eller
- den dag som en enskild leverantör av identifieringstjänster har lämnat in alla nödvändiga kompletteringar till inspektionsberättelsen.

Den tidigaste möjliga tidpunkten är på så sätt juli 2019. Senare tidpunkter för enskilda tjänsteleverantörer är i regel under 2020 eftersom Kommunikationsverket fortfarande har flera aktuella begäranden om komplettering. Därför anser Kommunikationsverket **inte** att nya inspektionsberättelser ska lämnas in i januari 2019, dvs. inom två år räknat från den dag för inlämnande av inspektionsberättelse som fastställs i lagen.

I tolkningen beaktar Kommunikationsverket lagen och motiveringen till lagen samt den omständigheten att behandlingen av bedömningarna vid Kommunikationsverket har dragit ut på tiden och att anvisningarna om bedömningen uppdateras 2018–2019. På så vis är anvisningarna, som stöder arbetet med nya bedömningar, ännu inte i början av 2019 till alla delar tillgängliga. Kommunikationsverket tar även hänsyn till att leverantörerna av identifieringstjänster inte helt själva har kunnat påverka den tidpunkt då Kommunikationsverket färdigställer sin bedömning av huruvida inspektionsberättelserna om överensstämmelse med kraven är tillräckliga.

De bedömningar som lämnades in i januari 2017 har till många delar utarbetats i slutet av 2016. Därför tar Kommunikationsverket hänsyn till att hoten och riskerna därefter har förändrats. På så sätt finns det ingen anledning att i onödan fördröja en ny bedömning.

Som anvisning konstaterar Kommunikationsverket följande:

- För alla fastställs jämlikt ett enda tidsschema enligt vilket Kommunikationsverket följer upp inlämnandet av inspektionsberättelser.
- Om bedömningar eller anskaffning av bedömningar inte har inletts ännu, ska det inledas i början av 2019 genast när identifieringstjänsten har fått tillräcklig information om kraven på bedömningen. (Se närmare nästa avsnitt.)
- Inspektionsberättelserna ska lämnas in ofördröjligen när de har blivit färdiga.
- Inspektionsberättelserna ska lämnas in senast före utgången av 2019.

Viestintävirasto

2.2 När ska en ny inspektionsberättelse lämnas in om leverantören av identifieringstjänster fördes in i registret 2017 eller senare?

En ny inspektionsberättelse ska lämnas in inom två år efter att den nya leverantören av identifieringstjänster har förts in i Kommunikationsverkets register enligt 12 § i autentiseringslagen.

2.3 Hur omfattande ska den nya bedömningen som görs med två års mellanrum vara?

Som anvisning konstaterar Kommunikationsverket följande:

1. När det gäller redan registrerade identifieringstjänster behöver hela verksamheten inte bedömas på nytt.

2. Bedömningen ska beakta de faktorer som Kommunikationsverket har bett företaget/organisationen komplettera eller i begärandena om komplettering har konstaterat om att bedömningen eller inspektionsberättelsen framöver ska vara noggrannare eller mer omfattande.

3. Om en anmälan om ändringar och en inspektionsberättelse inte har lämnats till Kommunikationsverket, ska bedömningen beakta ändringarna.

4. Vad gäller ledning avseende informationssäkerheten räcker det med en bedömning av att kraven på identifieringstjänster (autentiseringslagen, eIDAS, LOA-förordningen och Kommunikationsverkets föreskrift) har beaktats i ledningssystemet.

5. När incidenthanteringen bedöms ska hänsyn tas till identifieringstjänstens kapacitet och beredskap att upptäcka och vid behov rapportera störningar. Kommunikationsverket får ett relativt litet antal anmälningar om störningar och anser att det är nödvändigt att fästa uppmärksamhet vid incidenthanteringen i identifieringstjänsterna.

6. 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.

    - 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.

- Dataflöden 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.

7. Om en leverantör har en mobilapp för identifiering, ska appen bedömas till de delar den påverkar identifieringens överensstämmelse med kraven. Om det också finns andra funktioner i appen, behöver funktionerna inte inkluderas i bedömningen till de delar de inte kan påverka tillförlitligheten för identifieringen.

8. Dessutom ska en scanningsrapport om den bedömning som avses i 7 § i föreskrift 72A lämnas in utöver inspektionsberättelsen. Rapporten ska visa TLS- och krypteringsprofilerna för gränssnittet utåt.

9. För underleverantörer ska överensstämmelsen med kraven bedömas till alla ovannämnda delar.

10. När det gäller förfarandena för beviljande av identifieringsverktyg (inledande identifiering, utfärdande och leverans) behöver en kvalitetsrevision av överensstämmelsen endast göras på nytt vad gäller ändringar.

    - Om en elektronisk inledande identifiering har införts, bör det vad gäller användningen av den bedömas att transaktionerna för inledande identifiering har registrerats enligt 24 § i autentiseringslagen och att uppgifterna är tillgängliga enligt 16 § i nämnda lag.
    - Vad gäller mobilappar, se punkt 7.

2.4 Anmälan om och bedömning av ändringar

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 alltid till exempel

- ändringar i identifieringsmetoden, dvs. autentiseringsfaktorerna och autentiseringsmekanismen
- tekniska ändringar i identifieringssystemet, dvs. ändringar i underhålls- och produktionssystemets struktur eller program, eller
- byte eller ändringar i underleverantörernas underhåll, utrustning, system eller program.

Kommunikationsverket har tillfrågats huruvida en bedömning ska göras när gränssnittet Tupas ersätts med SAML- eller OIDC-gränssnitt.

- En gränssnittsimplementering som faller bort under 2019 behöver inte bedömas (Tupas eller något annat gränssnitt).
- En ny implementering ska bedömas vad gäller administration av krypteringskrav och krypteringsnycklar. De förfaranden för administration av sådana krypteringsnycklar som krävs eller tillhandahålls för

tjänster för ärendehantering omfattas av bedömningen, medan tjänsterna för ärendehantering inte omfattas.

- Om bytet av protokoll inbegriper både konfiguration av gränssnittet och andra relevanta ändringar i identifieringssystemet eller dess arkitektur, ska ändringarna bedömas.