E-LEGITIMATIONS NÄMNDEN

PM
Datum
2018-02-27

Granskningsmetod

Om metoden

1.1 Syfte

Syftet med dokumentet är att beskriva en metod för att utvärdera hur sökande uppfyller kraven enligt regelverket som gäller för Leverantörer av eID-tjänst i Valfrihetssystem och kvalitetsmärkta utfärdare av Svensk e-legitimation, både vid tidpunkten för ansökan och för att löpande utvärdera sökandes förmåga att kontinuerligt uppfylla kraven. Målet med granskningsmetoden är att säkerställa att alla sökande bedöms efter samma kriterier av granskningsgruppen. Metoden beskriver hur granskningsgruppen ska granska ansökningar.

1.2 Förutsättningar för att följa metoden

För att göra det möjligt att utföra stegen i denna metod har följande stöd tagits fram:

- Granskningsprogram
- Granskningsdokumentation
- Rapporteringsmall

Granskningsprogrammet innehåller detaljer med de krav och kriterier som ställs inom varje område. Dokumentet *Vägledning till uppfyllnad av tillitramverkets krav* har använts vid skapandet av granskningsprogrammet. Dokumentet riktar sig till sökande men det är viktigt för kravuppfyllnaden att både sökande och granskare har samma bild av vad kraven innebär.

Dokumentet *Granskningsdokumentation* följer strukturen i granskningsprogrammet och användas för att dokumentera granskningsarbetet inklusive alla ställningstaganden och slutsatser i granskningsprocessen. Dokumentationen ska bland annat användas för att visa vilken nivå som utfärdaren lever upp till inom varje område. Utestående frågor eller krav på kompletteringar ska också tydligt framgå i dokumentet tillsammans med en logg, utformad så att alla inom granskningsgruppen kan följa status för ärendet och även ta över delar av granskningen om så behövs.

Granskningsdokumentationen ska även utgöra underlag för att skapa den rapport som nämnden ska fatta sitt beslut utifrån. Därför måste slutsatserna för varje steg vara tydliga i dokumentet så att dessa kan föras över till rapporten. Varje granskat område ska avslutas med en sammanfattning av fullständighet, avvikelser, riskområden och slutsats om godkänd nivå, så att detta tydligt framgår i beslutsunderlaget till nämnden.

1.3 Granskningsgruppen

Granskningsgruppen är rådgivande till E-legitimationsnämnden, och syftar till att bistå med särskild kompetens till stöd för E-legitimationsnämndens arbete med granskning av aktörer inför anslutning. Granskningsgruppens föreslagna sammansättning framgår av resursbeskrivningen nedan, där huvudgrupperingens konsulter står för den största delen av arbetet med granskningen av aktörer. Kansliresursen är ordförande och sammankallande till gruppen, och det är även formellt ordföranden som ansvarar för de beslut som fattas av granskningsgruppen enligt nedan. Granskningen kan genomföras med endast två granskare, se fotnot.

Resurs	Beskrivning
	Huvudgrupperingen
1	Konsult – it-säkerhetsrevisor
2[1]	Konsult – it-säkerhet/tillitsramverksspecialist
3	Kansliresurs – ordförande och sammankallande
4	Representant från tillsynsmyndighet (eller motsvarande, om tillämpligt)
	Kompletterande resurser till förfogande
5	Konsult – tekikspecialist
6	Kansliresurs – administrativ

Granskningsgruppen sammanträder vid behov och inför följande beslut:

- Beslut om att påbörja granskning efter att *Steg 3 – Bedömning av formalians fullständighet* har genomförts. Om granskningsgruppen anser att en ansökan är så bristfällig att en granskning inte kan inledas informeras sökanden om bristerna och bereds möjlighet att återkomma med en omarbetad ansökan.
- Beslut om plan för kompletterande granskning (efter steg 5).
- Beslut om fastställande av granskningsrapport och den rekommendation från genomförd granskning som lämnas till nämnden för beslut (steg 8).

1.4 Arbetsinsatser

En uppskattning av det antal konsulttimmar som förväntas vid ett normalfall har specificerats för varje steg. Om det finns omständigheter som gör att ytterligare resurser kan behövas för genomförande av granskning ska godkännande av avvikelsen inhämtas från E-legitimationsnämndens kansli.

1.5 Grundprinciper för metoden

Granskningen av en ansökan ska leda till något av följande förslag, som föredras för nämnden vid slutet av varje granskning:

[1] Minimibemanning; alltid tillsammans med en kansliresurs

- Granskningsgruppen bedömer att ansökan lever upp till kraven i Tillitsramverket. Beslutsunderlag och rekommendation om godkännande lämnas till nämnden som fattar beslutet.
- Granskningsgruppen bedömer att ansökan lever upp till kraven i Tillitsramverket med vissa undantag. Beslutsunderlag och rekommendation om godkännande med vissa förbehåll lämnas till nämnden som fattar beslutet.
- Granskningsgruppen bedömer att ansökan inte lever upp till kraven i Tillitsramverket. Beslutsunderlag och rekommendation om avslag lämnas till nämnden som fattar beslut.

Under pågående granskning kan det även förekomma behov av att informera och diskutera granskningsstatus med nämnden dels som ett led i att förankra vissa slutsatser, dels som underlag för delbeslut under granskningens förlopp.

1.5.1 Principer för avvikelser från kraven i Tillitsramverket

Det finns fyra bedömningsnivåer för graden av kravuppfyllelse:

1. Det finns kontrollrutiner som säkerställer att kraven uppfylls.
2. Kraven bedöms vara uppfyllda.
3. Kraven bedöms vara delvis uppfyllda.
4. Kravuppfyllelsen bedöms vara bristande.

Följande beskrivning avser att vägleda granskaren i sin bedömning när avvikelser från kraven har identifierats i utfärdarens ansökan. Det är således inte avsikten att här ge en beskrivning av hur en korrekt måluppfyllelse ser ut för respektive område, eftersom detta bör framgå tydligt i granskningsprogrammet.

Grundförutsättningen är att samtliga identifierade avvikelser ska vara åtgärdade för att kraven ska bedömas som uppfyllda. För vissa avvikelser kan det dock vara rimligt att göra en positiv slutbedömning *med förbehåll*, det vill säga ge ett godkännande på förhand under förutsättning att bristen sedan åtgärdas inom utsatt tid. Detta innebär att granskningen inte stoppas på grund av avvikelsen. Det förutsätter dock att bristen är av sådan karaktär att den, så snart den i praktiken har åtgärdas, enkelt kan verifieras av granskaren snarare än att en djupanalys behöver initieras för att kontrollera att kravet är uppfyllt. Det är således enklare avvikelser som kan leda till ett godkännande med förbehåll, exempelvis felaktig eller avsaknad av viss formalia men där granskaren ändå har kunnat verifiera att kravet är uppfyllt på annat sätt. Nedan följer två exempel:

- Kraven bedöms vara delvis uppfyllda om granskaren kan verifiera att en process eller rutin finns etablerad men att kontrolldokumentation saknas som ger stöd för att processen eller rutinen har satts i verket, t.ex. när processen eller rutinen är nyetablerad.

- Kraven bedöms vara delvis uppfyllda om avvikelser från kraven kan motiveras av utfärdaren med relevanta argument, och där målet med kravet ändå uppfylls av utfärdaren genom andra motsvarande åtgärder. För att bedöma ovanstående måste granskaren göra en professionell bedömning baserad på sin kompetens och erfarenhet. I detta fall bör avvikelsen inte påverka slutbedömningen negativt. Avvikelsen bör dock tydligt redovisas av granskaren i granskningsrapporten och det bör tydligt framgå att den alternativa lösningen är ändamålsenlig.

Kravuppfyllnaden bedöms dock som bristande om det efterfrågade kravet varken finns informellt etablerat eller dokumenterat och det heller inte kan verifieras att det efterlevs av verksamheten. I detta fall påverkas den slutliga bedömningen negativt och granskningen kan komma att stoppas tills vidare.

1.5.2 Utvärdering av resultatet

För varje granskat område ska en sammanfattning, inklusive avvikelser, visa graden av kravuppfyllelse. En slutlig bedömning ska även göras för samtliga områden. För att göra en sammanfattande beskrivning av samtliga områden inklusive avvikelser måste granskaren göra en professionell bedömning baserad på sin kompetens och erfarenhet.

Den slutliga bedömningen utgör det beslutsunderlag som nämnden sedan fattar sitt beslut om godkännande på.

För att granskningsmetoden ska vara kostnadseffektiv samt bygga på tillit och balans gäller följande grundprinciper:

- Granskningen ska fokusera på riskområden.
- Granskningen ska fokusera på internkontroll som syftar till att säkerställa att kraven uppfylls och upprätthålls över tid.
- Dra nytta av eventuellt annat revisionsarbete som bedrivs inom den sökandes organisation.
- Utfärdare med tidigare erfarenhet bör bedömas med lägre risk än helt nya utfärdare, vilket påverkar omfattningen av granskningsgruppens kontroll av utfärdarens ansökan före ett eventuellt godkännande. Detta bygger på antagandet att tidigare utfärdare redan har gått igenom liknande kontroller vid tidigare anslutningsprocesser.
- Lita i stor utsträckning på att de underlag som utfärdare bilägger sin ansökan är sanna och riktiga, eftersom resurserna att verifiera efterlevnad är begränsade. Välj ett riskbaserat tillvägagångssätt vid val av områden som ändå ska kontrolleras.

2 Metoden steg 1–10

2.1 Steg 1 – Informationsmöte

Ansökningsprocessen börjar med en intresseanmälan från en part som vill använda kvalitetsmärket Svensk e-legitimation som utfärdare eller leverantör av eID-tjänster i Valfrihetssystem (nämndens trafikavtal). Efter intresseanmälan ska nämnden erbjuda tid för ett första informationsmöte inom två veckor. Mötet följer en förutbestämd agenda och beräknas ta två timmar.

2.1.1 Arbetsfördelning i granskningsgruppen

Deltagande på mötet är en till två resurser. Minst en av de deltagande ska vara en kansliresurs.

2.1.2 Konsulttimmar

5 konsulttimmar beräknas för varje möte.

2.2 Steg 2 – Bekräfta ansökan

I steget ingår följande uppgifter:

- Ta emot ansökan.
- Tilldela diarienummer och registrera handlingen.
- Bekräfta mottagen ansökan till utfärdaren inom tidsramen två arbetsdagar och beskriv nästa steg: *”Vi gör nu en första bedömning av fullständigheten i ansökan vilket avgör om vi kommer påbörja granskningen eller begära kompletteringar. Besked om fortsatt granskning och tidsram lämnas inom två veckor”.*
- Utse en granskningsledare för ansökan.
- Kommunicera till granskningsgruppen att ansökan har mottagits och vem som har utsetts som granskningsledare.

2.2.1 Arbetsfördelning i granskningsgruppen

Aktiviteter i steg 1 görs av kansliets administrativa resurs (resurs 6), förutom att utse granskningsledare, som görs av ordföranden i granskningsgruppen (resurs 3). Dessa två roller kan utgöras av samma person.

2.2.2 Konsulttimmar

Detta steg utförs av kanslipersonal utan konsultinsats.

2.3 Steg 3 – Bedömning av formalians fullständighet

I steget ingår följande uppgifter:

- Gå igenom formalians fullständighet (med en checklista och granskningsprogrammet som stöd) samt identifiera avvikelser från kraven på vad som ska ingå i ansökan, exempelvis att rätt blanketter har använts, att alla efterfrågade uppgifter finns med, att alla efterfrågade dokument finns bifogade (t.ex. årsredovisning) osv. Om avvikelser finns i formalian ska dessa värderas och beslut tas enligt följande:
- Besluta om granskningsgruppen ska gå vidare med granskningen trots att vissa delar saknas, dvs. parallellt med att kompletteringar inväntas. Besluta i så fall om tidpunkt (maximalt 90 dagar) för kompletteringar och meddela sökanden.
- Besluta om genomgången ska stoppas tills vidare, i väntan på kompletteringar. Meddela sökanden.
- Besluta att rekommendera till nämnden att avslå ansökan, eftersom den inte bedöms vara tillräcklig för att lägga till grund för granskning.

- Om formalian är fullständig och granskningen ska fortsätta, så ska granskaren göra en uppskattning om arbetsinsatsen för genomgång av resten av ansökan, inklusive det bedömda behovet av granskning på plats hos utfärdaren.
- Besluta om hur arbetet ska fördelas bland medlemmarna inom granskningsgruppen, beroende på deras kompetensområde eller annan grund.

Steget bör vara klart inom två veckor från att ansökan har kommit in.

2.3.1 Arbetsfördelning i granskningsgruppen

Steg 3 utförs huvudsakligen av resurs 1, 2 eller 3.

2.3.2 Konsulttimmar

Ca 16 konsulttimmar.

2.4 Steg 4 – Gör en preliminär riskbedömning av aktören

I steget ingår att bedöma sökanden utifrån tillgänglig information om dennes organisation, i syfte att skapa en uppfattning om risker i dennes verksamhet. En checklista för detta ändamål bör ingå i granskningsprogrammet. Med sådan tillgänglig information avses uppgifter som lämnats i ansökan som svar på Tillitsramverkets K2.1-K2.3 och K2.6. Bedömningen bör bland annat omfatta följande aspekter på sökandens verksamhet:

- Mognadsgrad i aktörens egen riskanalys – en mogen process för riskhantering talar för att aktören har förmåga att identifiera och hantera risker och därmed bidrar till en lägre riskbedömning.
- Hur länge aktören har bedrivit utfärdar- eller leverantörsverksamhet – tidigare erfarenhet av branschen talar för att aktören har förståelse för de tekniska och administrativa krav som ställs, och bidrar därmed till en lägre riskbedömning.

- Mognadsgrad i arbetet med ledningssystem för informationssäkerhet (LIS) – ett moget LIS-arbete innebär att aktörens säkerhetskontroller utvärderas på återkommande basis, vilket talar för en lägre risknivå.
- Finansiell ställning – en stark finansiell ställning talar för att aktören har utrymme att investera i förbättringsarbete om behov uppstår, vilket talar för en lägre risknivå.
- Tidigare erfarenheter från verksamhet som står under tillsyn – en aktör som sedan tidigare är van vid regelefterlevnad talar för en mogen process för hantering av regelefterlevnad och därmed en lägre risknivå.

För vart och ett av ovanstående områden görs en bedömning med alternativen *högre* eller *lägre*. Resultatet från varje delområde vägs samman till en övergripande riskbedömning på en skala 1-4 (där 1 motsvarar låg risk). Riskbedömningen används för att styra omfattningen av granskningen, t.ex. vid bestämning av stickprovskontroller.

2.4.1 Arbetsfördelning i granskningsgruppen

Den preliminära riskbedömningen görs av granskningsledaren tillsammans med ytterligare en granskningsresurs (resurs 1, 2 eller 3).

2.4.2 Konsulttimmar

Ca 4 konsulttimmar.

2.5 Steg 5 – Genomför grundläggande granskning enligt granskningsprogrammet

Efter den preliminära riskbedömningen har genomförts fortsätter granskningen till dess att all grundläggande granskning som anges i granskningsprogrammet har genomförts.

2.5.1 Arbetsfördelning i granskningsgruppen

Granskningsarbetet utförs av resurs 1–3 och 5, fördelat efter kompetensbehov och tillgänglighet. Kvalitetssäkring görs av granskningsledaren.

2.5.2 Konsulttimmar

Ca 40 konsulttimmar.

2.6 Steg 6 – Planera kompletterande granskning

Med hjälp av den ifyllda granskningsdokumentationen görs en bedömning av behovet av kompletterande granskning hos aktören. Granskningsprogrammet beskriver ett antal obligatoriska utökade granskningsåtgärder som ska genomföras för samtliga aktörer. För aktörer som i den preliminära riskbedömningen har klassificerats som riskkategori 1 eller 2 kan omfattningen av stickprovskontroller minskas något. Utöver de obligatoriska utökade granskningsåtgärderna bör granskningsledaren tillsammans med granskare bedöma om det

finns behov av att genomföra ytterligare kompletterande granskning. Eventuell ytterligare kompletterande granskning dokumenteras i granskningsdokumentationen.

När granskningsledaren har godkänt planen för kompletterande granskning kontaktar kansliet aktören och bokar tid för granskningsbesök. Samtidigt begär kansliet eventuell kompletterande dokumentation.

Kompletterande granskning som avviker mycket från schablonen måste godkännas av kansliet.

2.6.1 Arbetsfördelning i granskningsgruppen

Planering av kompletterande granskning utförs av resurs 1–3. Granskningsledaren godkänner planen.

2.6.2 Konsulttimmar

Ca 4 konsulttimmar.

2.7 Steg 7 – Genomför kompletterande granskning

Planerad kompletterande granskning genomförs hos aktören.

2.7.1 Arbetsfördelning i granskningsgruppen

Samma resurser som för steg 4–6.

2.7.2 Konsulttimmar

Ca 16 konsulttimmar exklusive eventuella tekniska tester. Verifiering av intrångsskydd i intygsgivningsfunktionen eller motsvarande tester förväntas ta mellan 10 och 30 konsulttimmar i anspråk.

2.8 Steg 8 – Avstämning av bedömning med utfärdaren (remiss)

Varje slutförd granskning ska dokumenteras i ett passande format och stämmas av med utfärdaren som under två veckor får möjlighet att inkomma med synpunkter/förtydliganden utifrån granskningsgruppens bedömningar.

Synpunkter och förtydliganden från utfärdaren hanteras av en utsedd person inom granskningsgruppen. Om behov finns kan ett möte bokas med utfärdaren för återkoppling.

2.8.1 Arbetsfördelning i granskningsgruppen

Rapportskrivning och hantering av svar görs av respektive granskare. Kommunikation med sökande görs av en resurs från kansliet (resurs 3 eller 6).

2.8.2 Konsulttimmar

32 konsulttimmar för författande av rapport och svar på frågor.

2.9 Steg 9 – Sammanfattning och föredragning för granskningsgruppen

Varje slutförd granskning av en ansökan ska föredras inför hela granskningsgruppen för att man gemensamt ska kunna komma fram till vilken rekommendation (inklusive motivering) som ska ges till nämnden avseende beslutet: godkänd, godkänd med förbehåll (ska alltid innehålla en maximal tidsgräns, exempelvis 12 månader) eller icke godkänd.

Granskningsgruppen kompletterar även beslutsunderlaget (i den mån godkännande rekommenderas) med en plan för fortsatt kontroll av partens efterlevnad över tid, exempelvis årlig kontroll. Aktiviteten fungerar både som efterkontroll och som påminnelse till utfärdaren om att upprätthålla kvaliteten i sin efterlevnad av Tillitsramverket. I beslutsunderlaget ska det finnas en redogörelse av hur granskningsgruppen har kommit fram till sin rekommendation. Granskningsgruppen har en rådgivande funktion till nämnden. Det är granskningsgruppens ordförande som har mandat att besluta om vilken rekommendation som ska lämnas efter respektive granskning.

Granskningsgruppens sammanträden bör bokas ca två veckor innan det att nämnden sammanträder, så att nämndens ledamöter i god tid före mötet kan ta del av materialet som ska utgöra beslutsunderlaget.

2.9.1 Arbetsfördelning i granskningsgruppen

Granskningsledaren är föredragande. Hela granskningsgruppen deltar på mötet.

2.9.2 Konsulttimmar

Ca 4 konsulttimmar.

2.10 Steg 10 – Nämnden fattar beslut

Nämnden fattar beslut med granskningsgruppens rekommendationer som underlag. Granskningsgruppens ordförande är föredragande i ärendet. Utfärdaren meddelas beslutet.

2.10.1 Arbetsfördelning i granskningsgruppen

Resurs 3 eller 6 meddelar beslutet.

2.10.2 Konsulttimmar

Inga konsulttimmar.