# Ansökningsformulär för ansökan om att bli Utfärdare av Svensk e-legitimation på tillitsnivå 2

Ansökningsformulär för ansökan om att bli Utfärdare av Svensk e-legitimation på tillitsnivå 2 1

Del A – Upplysningar, generella krav och underskrift 5

1.1 Bakgrund 5

1.2 Ansökans inlämnande 5

1.3 Handläggningstid 6

1.4 Process för granskning av ansökan 6

1.5 Godkännande 6

1.6 Återkallelse av godkännande 7

1.7 Ekonomisk stabilitet 7

1.8 Verksamhets bedrivande 8

1.9 Underleverantörer 8

1.10 Uteslutning av sökande 8

1.11 Anvisningar 8

1.12 Information om sökanden 9

1.13 Ansökans omfattning 10

1.14 Bekräftelse att efterfrågad information har lämnats 10

1.15 Form för ansökan 10

1.16 Medverkan i granskningsprocess 10

1.17 Uteslutning av sökanden 11

1.18 Sekretess 12

1.19 Underskrift 13

Del B – Svar avseende krav på tjänsten 14

1. Inledande krav 14

1.1 Allmän beskrivning 14

1.2 Tillhandahållna e-legitimationer och tillitsnivåer 14

1.3 Tillämplighet och begränsningar 14

1.4 Ändringsförfarande och godkännandeprocess 15

1.5 Kontaktuppgifter 15

2. Allmänna åtaganden 15

2.1 Parter och deras ansvarsområden 15

2.2 Informationsutbyte 16

2.2.1 Rapporteringsskyldighet 16

2.2.2 Periodicitet och former för rapportering 16

2.3 Behandling av personuppgifter 16

3. Organisation och styrning 17

3.1 Verksamhetsform och ägandestruktur 17

3.2 Finansiell ställning 17

3.3 Ledningssystem för informationssäkerhet 18

3.4 Underleverantörsförhållanden 18

4. Fysisk, administrativ och personalorienterad säkerhet 19

4.1 Fysisk säkerhet 19

4.1.1 Driftanläggningars beskaffenhet och lokalisering 19

4.1.2 Fysiskt tillträde till skyddade utrymmen 20

4.1.3 Strömförsörjning, miljö och brandskydd 20

4.2 Administrativ säkerhet 20

4.2.1 Betrodda roller inom organisationen 20

4.2.2 Åtgärder som kräver separation av arbetsuppgifter 21

4.2.3 Identifiering av personer i betrodda roller 21

4.3 Personalorienterad säkerhet 21

4.3.1 Bakgrund och kvalifikationer 21

4.3.2 Utbildning av personal 22

4.3.3 Krav vid utkontraktering av personal 22

4.4 Spårbarhet och loggning 22

4.4.1 Händelser som registreras i säkerhetslogg 22

4.4.2 Kontroll och uppföljning av säkerhetsrelaterade händelser 23

4.4.3 Skydd av spårbarhetsinformation 23

4.4.4 Handlingars bevarande 23

4.4.5 Gallring 24

4.5 Operationella aspekter 24

4.5.1 Kontinuitetsplanering 24

4.5.2 Incidenthantering 24

4.5.3 Avveckling av tjänsten 25

5. Teknisk säkerhet 25

5.1 Kryptografiska funktioner 25

5.1.1 Kryptografiska algoritmer och nyckeltyper 25

5.1.2 Nycklars livscykel 26

5.1.3 Omgivning och metodik för nyckelframställning 26

5.2 Förvaring och skydd av privata nycklar 26

5.2.1 Skydd av privata nycklar 26

5.2.2 Säkerhetskopiering av privata nycklar 27

5.2.3 Utplåning av privata nycklar 27

5.3 Säkerhet i drift- och utvecklingsmiljö 27

5.3.1 Systemsäkerhet 27

5.3.2 Systemutveckling 28

5.3.3 Systemunderhåll och styrning av ändringar i drift 28

5.3.4 Styrmedel för nätverkskommunikation 28

5.3.5 Spårbar tid 29

5.3.6 Säkerhetskopiering 29

5.3.7 Övervakning 29

6. Ansökan, identifiering och registrering 30

6.1 Ansökan och information om villkor 30

6.2 Identifiering och registrering 30

6.2.1 Fastställande av sökandens identitet 30

6.2.2 Registreringsförfarande 31

6.3 Utfärdande och spärr av e-legitimation 31

6.3.1 Utformning av tekniska hjälpmedel 31

6.3.2 Skapande av e-legitimationshandling 32

6.3.3 Tillhandahållande av e-legitimationshandling 32

6.4 Spärrtjänst 33

6.4.1 Rutin för begäran om spärr 33

6.4.2 Befogenhet att begära spärr 33

6.4.3 Behandlingstid vid begäran om spärr 33

7. Kontroll av innehavares elektroniska identitetet 34

8. Utställande av identitetsintyg 34

8.1 Intygsgivningstjänstens tillgänglighet 34

8.2 Skydd mot missbruk av identitetsintyg och intygsgivningstjänst 34

8.3 Skydd mot obehörig åtkomst 35

9. Revision 35

9.1 Revisionens periodicitet och omfattning 36

9.2 Revisorns kvalifikationer 36

9.3 Revisorns förhållande till den granskade parten 36

9.4 Åtgärder vid upptäckt av brist 37

10. Övrigt 37

10.1 Kundtjänst 37

10.2 Användbarhet och tillgänglighet 37

## Del A – Upplysningar, generella krav och underskrift

### 1.1 Bakgrund

I syfte att främja användningen av elektronisk identifiering och underskrift, erbjuder Myndigheten för digital förvaltning (DIGG) utfärdare av e-legitimation möjlighet att ansöka om att bli granskade gentemot kravställningen i Tillitsramverket för Svensk e-legitimation på nivå 2.

En genomgången granskning borgar för att utgivna e-legitimation uppfyller de ställda kraven och att offentliga och privata aktörer med e-tjänster som kräver elektronisk identifiering kan lita på e-legitimationen. Även användare kan känna sig trygga med en e-legitimation som har genomgått granskningen.

### 1.2 Ansökans inlämnande

Ansökan om godkännande ska vara skriven på svenska och lämnas i form av ifyllt ansökningsformulär kompletterat med bilagor. För fullständig ansökan fordras att alla i formuläret efterfrågande uppgifter har lämnats.

Samtliga bilagor ska vara förtecknade i ansökan och märkta med sökandens namn. Sökanden ska begränsa sin ansökan till att endast innehålla i ansökningsformuläret begärd information och dokumentation.

De dokument rörande denna ansökan som tillhandahålls av DIGG får inte ändras eller justeras. Reservationer till eller andra förändringar av krav eller avtalsvillkor accepteras inte.

Ansökan ska lämnas in i original undertecknat av behörig företrädare för sökanden. Om ansökningshandlingen inte undertecknas elektroniskt ska sökanden även lämna en fullständig digital kopia av ansökan (läsbart i Microsoft Office-format, pdf eller motsvarande). Om originalet och kopian skiljer sig åt äger originalet företräde.

Originalet ska i försluten försändelse märkt ”Ansökan Utfärdare av Svensk e-legitimation” lämnas eller sändas till:

Myndigheten för digital förvaltning

Box 14

851 02 Sundsvall

I det fall sökande önskar lämna sin ansökan personligen eller genom bud kan detta göras i DIGG:s reception på Storgatan 37 i Sundsvall. Receptionen är normalt öppen måndag–fredag kl. 09.00–16.00.

### 1.3 Handläggningstid

När en fullständig ansökan inkommit behandlas den av DIGG som bedömer om sökanden uppfyller de krav för godkännande som framgår av detta ansökningsformulär. Besked om godkännande ska lämnas till sökanden inom skälig tid efter att en fullständig ansökan har kommit in till DIGG. DIGG ska vid mottagande av ansökan ge sökande en uppskattning av tid för genomförande av granskningen.

### 1.4 Process för granskning av ansökan

Med utgångspunkt i sökandens svar i detta ansökningsformulär (med eventuella bilagor) kommer DIGG att granska huruvida sökanden uppfyller de krav för godkännande som framgår av ansökningsformuläret. I samband med granskningen kan DIGG komma att begära kompletteringar i en eller flera delar om svar i inkommen ansökan inte är tillräckliga för att kunna göra en bedömning avseende kravuppfyllnad. För att verifiera kravuppfyllnad kan det även komma att bli aktuellt med platsbesök och intervjuer hos sökanden samt stickprov. DIGG kommer att underrätta sökanden om sådana tillkommande kontroller utöver själva ansökningsformuläret blir aktuella. DIGG kan även komma att konsultera en referensgrupp bestående av experter från olika myndigheter vid granskningen.

Sökanden ska vara behjälplig under hela ansöknings- och granskningsprocessen och ställa upp med nödvändiga resurser samt erbjuda tillgång till sådan dokumentation och sådana lokaler som krävs för att DIGG ska kunna verifiera kravuppfyllnad. Planering av platsbesök, intervjuer och stickprov ska ske i samråd mellan sökanden och DIGG och förläggas på ett sådant sätt att de innebär så liten påverkan på sökandens verksamhet som möjligt.

### 1.5 Godkännande

DIGG kommer att godkänna samtliga sökande som uppfyller de krav för godkännande som framgår av detta ansökningsformulär, såvida inte sökanden uteslutits i enlighet med avsnitt 1.11 nedan. Efter att DIGG beslutat om godkännande kommer myndigheten att snarast underrätta sökanden om beslutet och skälen för det.

Ett godkännande på tillitsnivå 2 följs inte av något avtalstecknande. Istället sker godkännandet för en begränsad tidsperiod (vanligen 12 månader), och godkännande måste därför förlängas regelbundet för att vara gällande.

### 1.6 Återkallelse av godkännande

DIGG rätt att återkalla eventuellt godkännande av sökanden, om det framkommer att sökanden inte uppfyller kraven för godkännande.

### 1.7 Ekonomisk stabilitet

Sökanden ska ha ekonomisk stabilitet och ekonomiska förutsättningar att kunna fullgöra de åtaganden som följer av Tillitsramverketet. Sökanden ska förfoga över tillräckliga ekonomiska medel för att kunna bedriva verksamheten i minst ett år och för att kunna bära risken för skadeståndsskyldighet. Verksamheten ska senast vid avtalstecknande drivas som en i Sverige registrerad juridisk person eller som ett inom Europeiska ekonomiska samarbetsområdet registrerat bolag i en form motsvarande svenskt aktiebolag.

För att DIGGs ska kunna bedöma om sökanden uppfyller kravet på ekonomisk stabilitet ska **utländsk** sökande bifoga dokumentation som motsvarar följande intyg.

1. Kopia på vid tiden för ansökan gällande registreringsbevis utfärdat av behörig officiell myndighet (i Sverige Bolagsverket).
2. ”Begäran om upplysningar vid offentlig upphandling”, Skatteverkets blankett SKV 4820. Blanketten ska vara ifylld av Skattemyndigheten. Blanketten kan rekvireras från <http://www.skatteverket.se>.

Sådan dokumentation får inte vara äldre än tre månader.

För svenska sökande beställer DIGG själv registreringsbevis och upplysningar motsvarande vad som lämnas genom blankett SKV 4820.

För företag under bildande gäller att företaget ska vara bildat när Tillitsramverket tecknas. Företaget ska vid samma tillfälle vara godkänd för F-skatt och uppvisa registreringsbevis utfärdat av Bolagsverket.

DIGGs bedömning av om en sökande ska godkännas med avseende på ekonomisk stabilitet kommer att ske utifrån sökandens finansiella och ekonomiska ställning samt förmåga att fullfölja ett åtagande under hela avtalsperioden. DIGG kommer att göra en helhetsbedömning och inhämta kreditupplysning samt eventuella referenser.

En sökande som inte är skyldig att offentliggöra årsredovisning enligt 6 kap. 1 § bokföringslagen (1999:1078) ska visa att sökanden har en stabil ekonomisk bas genom att tillhandahålla resultaträkning och balansräkning eller på begäran lämna referens till bank eller annan finansiär.

Sökande som är ett nystartat företag eller företag under bildande ska visa att företaget har en stabil ekonomisk bas genom att redovisa eget kapital, reserver och skulder, eller på begäran tillhandahålla en finansiell säkerhet (t.ex. lämna bankgaranti eller koncerngaranti) samt lämna referens till bank eller annan finansiär.

DIGG förbehåller sig rätten att från sökanden begära en ekonomisk plan för verksamhetens finansiering under de två första verksamhetsåren.

### 1.8 Verksamhets bedrivande

Sökande ska redan när ansökningshandlingen lämnas ha en etablerad verksamhet, vara fullt operationell i alla delar som berörs i detta ansökningsformulär, och vara väl insatt i de regler samt juridiska, tekniska och administrativa krav som ställs på en utfärdare av Svensk e-legitimation.

### 1.9 Underleverantörer

Om sökanden ska använda underleverantör för att i någon väsentlig del utföra verksamhet inom ramen för utfärdarens åtaganden ska detta anges i ansökan. Det ska tydligt anges vilka delar av efterfrågade tjänster som sökanden avser att lägga ut på underleverantör.

### 1.10 Uteslutning av sökande

DIGG får utöver vad som i övrigt anges i detta ansökningsformulär neka godkännande av en ansökan från en sökande om

1. sökanden är i konkurs eller likvidation, är under tvångsförvaltning eller är föremål för ackord eller tills vidare har inställt sina betalningar eller är underkastad näringsförbud,
2. sökanden är föremål för ansökan om konkurs, tvångslikvidation, ackord eller annat liknande förfarande,
3. någon av sökandens företrädare genom lagakraftvunnen dom är dömd för brott som avser yrkesutövningen,
4. någon av sökandens företrädare kan visas ha gjort sig skyldig till allvarligt fel i yrkesutövningen, eller
5. sökanden inte har fullgjort sina åligganden avseende socialförsäkringsavgifter eller skatt i hemlandet eller en annan stat inom Europeiska ekonomiska samarbetsområdet.

### 1.11 Anvisningar

Detta ansökningsformulär är upprättat med stöd av formulärfunktionen i Microsoft Word. Sökanden ska använda denna mall vid framtagningen av sin ansökan. Efterfrågade svar och redovisningar ska lämnas i formulärets kryss- och svarsrutor. Textrutornas storlek anpassas automatiskt till textens omfång. Om viss redovisning är omfattande kan sökanden lämna denna i en separat bilaga som bifogas ansökan. Textrutan ska då innehålla uppgift om bilagans beteckning.

I samband med flertalet svarsfält i formuläret finns en referens till styrande krav som ska vara uppfyllt i enlighet med Tillitsramverket för Svensk e-legitimation. Det är kraven såsom de anges i Tillitsramverket med dess vägledning som gäller för bedömning av kravuppfyllnad i ansökan. Förklarande text nedan i samband med svarsfälten syftar i huvudsak till att hjälpa sökanden med de beskrivningar som krävs för att kunna granska och bedöma kravuppfyllnad.

Sökanden ska lämna ett fullständigt ifyllt ansökningsformulär (detta dokument) och ska genom att tydligt redogöra för hur sökanden uppfyller Tillitsramverkets krav. Om DIGG har saklig grund att anta att de aktuella kraven inte är uppfyllda, eller om sökandens redogörelse är så ofullständig att DIGG inte kan bedöma om kraven uppfylls, får DIGG neka godkännande av ansökan.

En ansökan om att bli Utfärdare av Svensk e-legitimation är som huvudregel offentlig. Eftersom den efterfrågade tjänsten och granskningen av ansökningar förutsätter att vissa potentiellt konkurrens- och säkerhetskritiska frågor belyses i ansökan kan sekretess emellertid gälla för delar av ansökan enligt 18 kap. 8 § OSL och 31 kap. 16 § OSL. Om den sökande anser att några uppgifter i ansökan omfattas av sekretess ska dessa uppgifter tydligt markeras i ansökan och skälen för detta anges i samband med att ansökan lämnas in. Bedömningen av huruvida tillräckliga skäl för sekretess föreligger görs dock av DIGG eller den myndighet som mottagit uppgifterna inom ramen för granskningen och slutligt av förvaltningsdomstol, i samband med att någon begär att få tillgång till uppgifterna. Beträffande de uppgifter som avses i 31 kap. 16 § OSL, gäller sekretessen även för mottagande myndigheter som normalt inte varit tvungna att tillämpa sekretessbestämmelsen (sk. överföring av sekretess). Några garantier om att uppgifter inte kommer att lämnas ut kan dock inte lämnas.

I ljuset av frågorna ovan kopplat till offentlighet och sekretess är det lämpligt att sökanden lämnar sina svar nedan på ett sådant sätt att särskilt känslig information ur ett säkerhets- eller kon­kurrensperspektiv undviks. DIGG erbjuder även möjlighet att komplettera ansökan med intervjuer och/eller platsbesök för de fall kravuppfyllnad inte kan verifieras med utgångspunkt i nedan angivna svar.

### 1.12

### Information om sökanden

**Svar A1.1 - Sökanden:**

|  |  |
| --- | --- |
| Namn: | |
| Organisationsnummer: | |
| Utdelningsadress: | |
| Postnummer, postadress: | |
| Kontaktperson, namn: | |
| Kontaktpersonens  e-postadress: | Kontaktpersonens  telefonnummer (kontoret, mobil): |
| Behörig företrädares namn: | |

### 1.13 Ansökans omfattning

**Svar A1.2 – Bekräftelse avseende ansökans omfattning:**

|  |  |
| --- | --- |
| Vi bekräftar att ansökan avser att bli Utfärdare av Svensk e-legitimation på tillitsnivå 2. | **Ja** |

### 1.14 Bekräftelse att efterfrågad information har lämnats

**Svar A1.3 - Bekräftelse att efterfrågad information har lämnats:**

|  |  |
| --- | --- |
| Vi bekräftar att vi är införstådda med att vi i denna ansökan ska redovisa samtliga efterfrågade uppgifter och redovisningar. | **Ja** |

### 1.15 Form för ansökan

**Svar A1.4 - Form för ansökan:**

|  |  |
| --- | --- |
| Ansökan lämnas enligt följande:   * i ett undertecknat skriftligt original, samt; * i en fullständig kopia i digitalt format. | **Ja** |

### 1.16 Medverkan i granskningsprocess

Sökanden ska vara behjälplig under hela ansöknings- och granskningsprocessen och ställa upp med nödvändiga resurser samt erbjuda tillgång till sådan dokumentation och sådana lokaler som krävs för att DIGG ska kunna verifiera kravuppfyllnad. Planering av platsbesök, intervjuer och stickprov ska ske i samråd mellan sökanden och DIGG och förläggas på ett sådant sätt att de innebär så liten påverkan på sökandens verksamhet som möjligt.

**Svar A1.5 - Bekräftelse kring medverkan i granskningsprocess:**

|  |  |
| --- | --- |
| Sökanden bekräftar att denne kommer att vara behjälplig under ansöknings- och granskningsprocessen och ställa upp med nödvändiga resurser samt erbjuda tillgång till sådan dokumentation och sådana lokaler som krävs för att DIGG ska kunna verifiera kravuppfyllnad. | **Ja** |

### 1.17 Uteslutning av sökanden

DIGG förbehåller sig rätten att neka godkännande av sökande, eller avseende punkt 3 och 4 företrädare för den juridiska personen, som

1. sökanden är i konkurs eller likvidation, är under tvångsförvaltning eller är föremål för ackord eller tills vidare har inställt sina betalningar eller är underkastad näringsförbud,
2. sökanden är föremål för ansökan om konkurs, tvångslikvidation, ackord eller annat liknande förfarande,
3. någon av sökandens företrädare genom lagakraftvunnen dom är dömd för brott som avser yrkesutövningen,
4. någon av sökandens företrädare kan visas ha gjort sig skyldig till allvarligt fel i yrkesutövningen, eller
5. sökanden inte har fullgjort sina åligganden avseende socialförsäkringsavgifter eller skatt i hemlandet eller en annan stat inom Europeiska ekonomiska samarbetsområdet.

**Svar A1.6a - Sökandens eget intygande, uteslutningsgrunder:**

|  |  |
| --- | --- |
| Sökanden intygar att denne och eventuell/-a underleve­rantör/-er samt företrädare för dessa företag, inte är före­mål för de under punkt 1-5 ovan uppräknade omstän­digheterna.  *Kommentar: Notera att DIGG kan komma att kontrollera sökandens uppgifter i för DIGG tillgängliga register.* | **Ja** |

Sökande ska uppfylla i Sverige eller i hemlandet lagenligt ställda krav avseende registrerings-, skatte- och avgiftsskyldigheter. I det fall sökande avser att använda underleverantör för att utföra delar av åtagandet ska även underleverantör uppfylla detta krav.

Sökande eller av denne anlitad underleverantör får inte under de två senaste åren ha ådragit sig skulder för socialförsäkringsavgifter eller skatter i Sverige eller i det egna landet som lett till att skulden registrerats hos Kronofogden eller motsvarande myndighet i hemlandet. Kravet är inte tillämpligt för sådana skulder som avser försum­bara belopp eller motsvarande omständigheter.

**Svar A1.6b - Sökandens eget intygande, fullgjorda skyldigheter:**

|  |  |
| --- | --- |
| Härmed intygas att sökanden och samtliga redovisade underleverantörer uppfyller ställda krav avseende sina registrerings-, skatte- och avgifts­skyldigheter.  *Kommentar: DIGG kommer att kontrollera uppgifterna genom att begära in intyg från Skatteverket (SKV 4820) eller motsvarande intyg från utländsk myndig­het. Sökande ska vara beredd att tillhandahålla aktuella dokument i det fall DIGG inte har möjlighet att själva ta del av dessa.* | **Ja** |

### 1.18 Sekretess

Handlingar som inkommer till myndigheten blir som regel allmän handling som är offentlig om den inte omfattas av sekretess.

Sekretess gäller då normalt heller inte för hela handlingen, utan endast för de uppgifter i en handling vars röjande kan skada det allmännas eller enskildas ekonomiska intressen. Detta innebär att de uppgifter som är sekretessbelagda maskeras av myndigheten, men att handlingen i övrigt lämnas ut. Sökanden ska därför ange vilka uppgifter man anser omfattas av sekretess och skälen till detta. Det underlättar myndighetens sekretessprövning. Det är viktigt att komma ihåg att det inte är myndigheten som slutgiltigt prövar och beslutar vilka uppgifter som anses omfattas av sekretess. Myndigheten kan således inte i förväg garantera att uppgifter i anbud kan behandlas konfidentiellt.

**Svar A1.7 – Beskrivning av uppgifter som enligt sökanden bör omfattas av sekretess:**

|  |
| --- |
|  |

### 1.19 Underskrift

Samtliga villkor i detta ansökningsformulär, inklusive avtal och övriga bilagor, godkänns genom nedan­stående underskrift av behörig företrädare för sökanden.

Datum       Ort

Underskrift, behörig företrädare

Namnförtydligande

## Del B – Svar avseende krav på tjänsten

*Observera att det i denna del refereras till ”utfärdare” istället för ”sökande”. Detta med hänsyn till den koppling som görs mot tillsvarande krav i Tillitsramverket.*

### 1. Inledande krav

#### 1.1 Allmän beskrivning

Detta avsnitt ska innehålla en allmän beskrivning av utfärdaren och den tillhandahållna tjänsten. Beskrivningen ska innefatta vid vilka verksamhetsställen utfärdarverksamheten bedrivs samt strukturen för utfärdarorganisationen. Utfärdaren ska även bifoga en utfärdardeklaration med sådant innehåll som följer av Tillitsramverket.

Styrande krav i Tillitsramverket

* K2.2, K5.3

**Svar B1.1a - Allmän beskrivning:**

|  |
| --- |
|  |

**Svar B1.1b – Bifoga utfärdardeklaration:**

|  |  |
| --- | --- |
| Bekräfta att utfärdarens utfärdardeklaration finns bilagerad ansökan. | **Ja** ­ |

#### 1.2 Tillhandahållna e-legitimationer och tillitsnivåer

Ange nedan vilka typer av e-legitimationer som utfärdaren avser tillhandahålla på tillitsnivå 2.

**Svar B1.2 – Beskrivning av tillhandahållna e-legitimationer på tillitsnivå 2:**

|  |
| --- |
|  |

#### 1.3 Tillämplighet och begränsningar

Beskrivningarna i ansökan ska omfatta samtliga delar av verksamheten som berörs av Tillitsramverket. I vissa fall kan det dock vara praktiskt att dela upp beskrivningarna, t.ex. då flera utfärdare samarbetar kring ett koncept. Det kan också vara så att hanteringen av e-legitimationer utgör en avgränsad del av utfärdarens hela verksamhet. I sådana fall ska den tillämplighet och eventuella avgränsningar som följer därav beskrivas i detta avsnitt.

**Svar B1.3 – Beskrivning av tillämplighet och begränsningar:**

|  |
| --- |
|  |

#### 1.4 Ändringsförfarande och godkännandeprocess

Detta avsnitt ska beskriva det interna ändringsförfarandet och den godkännandeprocess som utfärdaren tillämpar innan ändringar av utfärdarens utförande av sina åtaganden enligt Tillitsramverketet införlivas i verksamheten.

Beskrivningen av processen ska också innefatta de kriterier som används för att bedöma om en ändring är att anse som väsentlig och alltså kräver DIGG:s godkännande, eller av sådan mindre betydelse att den kan införlivas utan inblandning av DIGG.

**Svar B1.4 – Beskrivning av ändringsförfarande och godkännandeprocess:**

|  |
| --- |
|  |

#### 1.5 Kontaktuppgifter

Här ska de uppgifter DIGG ska använda för att komma i kontakt med ansvariga inom utfärdarens organisation anges. Roller vars kontaktuppgifter ska anges innefattar DIGG:s kontakt i frågor som rör efterlevnad, teknisk drift samt jourhavande för incidentberedskap.

Styrande krav i Tillitsramverket

* K2.4

**Svar B1.5 – Beskrivning av kontaktuppgifter:**

|  |
| --- |
|  |

### 2. Allmänna åtaganden

#### 2.1 Parter och deras ansvarsområden

I denna del ska redogöras för hur utfärdarens verksamhet är organiserad med avseende på e-legitimationers livscykelhantering, samt vilket ansvar som åligger respektive part eller organisationsenhet i denna del. Beskrivning av verksamhet utlagt till tredje part ska beskrivas nedan under avsnitt 3.4.

Styrande krav i Tillitsramverket

* K2.2

**Svar B2.1 – Beskrivning av organisation, parter och deras respektive ansvarsområden**

|  |
| --- |
|  |

#### 2.2 Informationsutbyte

Under detta avsnitt ska utfärdaren beskriva former för vidarerapportering till DIGG av inträffade incidenter. En incidenter är en oönskad och oplanerad händels som haft eller kunnat få påverkan på säkerheten i den tjänst utfärdaren levererar. Incidenter som kan föranleda åtgärder från DIGG:s sida ska rapporteras utan dröjsmål.

##### 2.2.1 Rapporteringsskyldighet

I detta avsnitt ska utfärdaren beskriva vilka fastställda rutiner som införts för att säkerställa att skyldigheten att rapportera incidenter efterlevs. Denna beskrivning ska innefatta vilka rapporteringsvägar som inrättats, vilka kriterier som tillämpas för att avgöra om en incident ska rapporteras utan dröjsmål, samt vilken roll inom organisationen som bär ansvaret för vidarerapporteringen till DIGG.

Styrande krav i Tillitsramverket

* K2.4

**Svar B2.2.1 – Beskrivning av rutiner för rapporteringsskyldighet:**

|  |
| --- |
|  |

##### 2.2.2 Periodicitet och former för rapportering

Allvarliga incidenter som kan komma att föranleda omedelbara åtgärder från DIGGs sida ska rapporteras utan dröjsmål. Mindre allvarliga incidenter och andra uppgifter som omfattas av rapporteringsskyldigheten ska rapporteras med vissa intervall. I detta avsnitt ska utfärdaren beskriva periodiciteten och formerna för den regelbundna rapporteringen.

Styrande krav i Tillitsramverket

* K2.4

**Svar B2.2.2 – Beskrivning av periodicitet och former för rapportering:**

|  |
| --- |
|  |

#### 2.3 Behandling av personuppgifter

Utfärdaren ska i detta avsnitt redogöra för vilka personuppgifter som behandlas, varifrån uppgifterna hämtas, ändamålen med behandlingen, hur länge de bevaras och till vilka mottagare eller kategorier av mottagare som uppgifterna kan komma att lämnas ut.

Styrande krav i Tillitsramverket

* K5.3

**Svar B2.3 – Beskrivning av behandling av personuppgifter:**

|  |
| --- |
|  |

### 3. Organisation och styrning

#### 3.1 Verksamhetsform och ägandestruktur

I beskrivningen ska bland annat redogöras för vilka aktörer och intressenter som står bakom verksamheten, samt eventuella koncernförhållanden eller samriskbolag som verksamheten är en del av.

Styrande krav Tillitsramverket

* K2.1, K5.4

**Svar B3.1 – Beskrivning av verksamhetsform och ägandestruktur:**

|  |
| --- |
|  |

#### 3.2 Finansiell ställning

Under denna rubrik ska utfärdaren redogöra för sin finansiella och ekonomiska ställning. I den mån detta inte går att fastställa genom kreditupplysningsinstitut, eller om utfärdaren är medveten om eller misstänker att sådan information kan vara felaktig eller inaktuell, så kan utfärdaren i detta avsnitt redogöra för varför så är fallet och hur kravet om stabil ekonomisk ställning är uppfyllt.

Beskrivningarna ska även innefatta för verksamheten relevanta försäkringsskydd som åberopas för kravuppfyllnad.

Styrande krav i Tillitsramverket

* K2.1, K2.3

**Svar B3.2a – Beskrivning av finansiell ställning:**

|  |
| --- |
|  |

**Svar B3.2b – Bifoga årsredovisning:**

|  |  |
| --- | --- |
| Bekräfta att utfärdarens senaste årsredovisning (alternativt resultat- och balansräkning samt revisionsberättelse från auktoriserad revisor) finns bilagerad ansökan. | **Ja** ­ |

#### 3.3 Ledningssystem för informationssäkerhet

I detta avsnitt ska utfärdaren beskriva det ledningssystem för informationssäkerhet som denne infört för att styra informationssäkerhetsarbetet och kontrollera risker.

Redogörelsen förväntas fokusera på det övergripande ledningssystemet som syftar till att upprätta, införa, driva, övervaka, granska, underhålla och förbättra informationssäkerheten inom utfärdarorganisationen.

Styrande krav i Tillitsramverket

* K2.4, K2.5

**Svar B3.3a – Beskrivning av ledningssystem för informationssäkerhet:**

|  |
| --- |
|  |

Vidare ska utfärdaren beskriva sitt arbete med hantering av risker i verksamheten, innefattande den riskanalysmetodik som utfärdaren tillämpar för att erhålla konsistenta, korrekta och jämförbara resultat över tid. Beskrivningen ska också innefatta arbetet med att utforma, införa och följa upp risklindrande åtgärder, samt utverkande av riskägarens godkännande av kvarvarande risk.

**Svar B3.3b – Beskrivning av utfärdarens arbete med riskhantering:**

|  |
| --- |
|  |

#### 3.4 Underleverantörsförhållanden

I den mån utfärdaren anlitat underleverantörer för fullgörande av delar av de åtaganden som följer av Tillitsramverketet, så ska sådana underleverantörsförhållanden beskrivas i detta avsnitt. Det ska särskilt belysas vilka underleverantörer som anlitats och i vilka delar.

Styrande krav i Tillitsramverket

* K2.6

**Svar B3.4a – Uppgift om utfärdarens samt­liga eventuella underleverantörers företagsnamn och organisations­num­mer:**

|  |
| --- |
| Underleverantör/-er, fullständigt företagsnamn och organisationsnummer: |

**Svar B3.4b – Beskrivning av hur utfärdaren avser att organisera verksamheten inklusive vilka uppgifter som utfärdaren själv kommer att svara för och vilka delar i åtagandet som respektive ovan redovisad underleverantör avses utföra:**

|  |
| --- |
|  |

### 4. Fysisk, administrativ och personalorienterad säkerhet

#### 4.1 Fysisk säkerhet

##### 4.1.1 Driftanläggningars beskaffenhet och lokalisering

I detta avsnitt ska utfärdaren beskriva de driftanläggningar, inklusive eventuella alternativa driftanläggningar, som utfärdaren använder eller kan komma att använda för att tillhandahålla de tjänster som ska levereras; innefattande tjänster för intygsutgivning, spärrtjänst och utfärdande av e-legitimationer.

Driftanläggningars lokalisering ska preciseras på minst regionnivå, och anläggningens beskaffenhet bör beskrivas utifrån den klassificering som finns i stöldskyddsföreningens normer för mekaniskt stöldskydd (SSF 200) och larmanläggningar (SSF 130).

I den mån även andra utrymmen än de aktuella driftanläggningarna kan komma att användas för att förvara informationsbärande media eller utrustning innehållande känsliga uppgifter, så ska även dessa utrymmen innefattas i beskrivningarna.

Styrande krav i Tillitsramverket

* K3.1

**Svar B4.1.1 – Beskrivning av driftanläggningars beskaffenhet och lokalisering:**

|  |
| --- |
|  |

##### 4.1.2 Fysiskt tillträde till skyddade utrymmen

I detta avsnitt ska utfärdaren beskriva formerna för fysisk åtkomstkontroll till de skyddade utrymmen i vilka informationsbärande media eller utrustning innehållande känsliga uppgifter kan nås eller komma att förvaras. Beskrivningen ska innefatta den krets av personer som har fysiskt tillträde till utrymmena, samt eventuellt tillkommande kontroller avsedda att begränsa obehöriga personers möjlighet att komma åt utfärdarens utrustning.

Styrande krav i Tillitsramverket

* K3.1

**Svar B4.1.2 – Beskrivning av principer för fysiskt tillträde till skyddade utrymmen:**

|  |
| --- |
|  |

##### 4.1.3 Strömförsörjning, miljö och brandskydd

Utfärdaren ska under denna rubrik beskriva driftanläggningarnas förutsättningar till kontinuerlig strömförsörjning och kontrollerad miljö samt de åtgärder som vidtagits för skydd mot brand i de skyddade utrymmena.

Styrande krav i Tillitsramverket

* K3.1

**Svar B4.1.3 – Beskrivning av strömförsörjning, miljö och brandskydd:**

|  |
| --- |
|  |

#### 4.2 Administrativ säkerhet

##### 4.2.1 Betrodda roller inom organisationen

I detta avsnitt ska utfärdaren redogöra för de betrodda roller som existerar inom organisationen, vilket ansvar som följer av respektive roll och på vilket sätt dessa roller är bemannade.

Styrande krav i Tillitsramverket

* K3.2

**Svar B4.2.1 – Beskrivning av betrodda roller inom organisationen:**

|  |
| --- |
|  |

##### 4.2.2 Åtgärder som kräver separation av arbetsuppgifter

Vissa särskilt säkerhetskritiska åtgärder kan fordra att flera personer i förening krävs för genomförandet. Här ska utfärdaren i förekommande fall redogöra för vilka åtgärder som kräver sådana kontroller, vilka roller som involveras och på vilket sätt samt hur efterlevnad säkerställs.

Styrande krav i Tillitsramverket

* K3.2, K4.1

**Svar B4.2.2 – Beskrivning av åtgärder som kräver separation av arbetsuppgifter:**

|  |
| --- |
|  |

##### 4.2.3 Identifiering av personer i betrodda roller

Personer i betrodda roller besitter som regel sådan fysisk- och/eller logisk behörighet till informationstillgångar och informationsbehandlingsresurser som medför att ett särskilt säkerhetskritiskt ansvar vilar på dem. I detta avsnitt ska utfärdaren beskriva vilka kontroller som tillämpas för att identifiera dessa personer vid (fysisk och logisk) åtkomst till sådana informationstillgångar.

Styrande krav i Tillitsramverket

* K3.1, K4.1

**Svar B4.2.3 – Beskrivning av identifiering av personer i betrodda roller:**

|  |
| --- |
|  |

#### 4.3 Personalorienterad säkerhet

Följande avsnitt avses i första hand gälla personal i betrodda roller, men även övrig personal som i sitt arbete kan komma i kontakt med sådana informationstillgångar och system som används för att tillhandahålla tjänsten. Exempel innefattar säkerhetsansvariga, systemadministratörer, personal i registraturfunktion, handläggare och underhållspersonal.

##### 4.3.1 Bakgrund och kvalifikationer

Utfärdaren ska beskriva de rutiner som tillämpas för att säkerställa att personal i betrodda roller samt de som i övrigt kan komma i kontakt med känsliga informationstillgångar och system, kan anses pålitlig och har den utbildning och de kvalifikationer som krävs för att fullgöra sina arbetsuppgifter på ett korrekt och säkert sätt.

Styrande krav i Tillitsramverket

* K3.2

**Svar B4.3.1 – Beskrivning av kontroll av bakgrund och kvalifikationer:**

|  |
| --- |
|  |

##### 4.3.2 Utbildning av personal

Personal i betrodda roller kräver som regel specifik utbildning i de arbetsuppgifter de ska utföra. Utfärdaren ska beskriva hur denne bedriver utbildning av sådan personal, vid anställning och därefter regelbundet.

Styrande krav i Tillitsramverket

* K3.2

**Svar B4.3.2 – Beskrivning av utbildning av personal:**

|  |
| --- |
|  |

##### 4.3.3 Krav vid utkontraktering av personal

Då personal som inte är anställd vid utfärdaren (och inte genomgått bakgrundskontroll och utbildning hos utfärdaren) ska utföra tillfälligt arbete där denne kan komma i kontakt med informationstillgångar och system, krävs som regel att dessa kontrolleras eller att det på annat sätt säkerställs att säkerheten upprätthålls. I detta avsnitt ska utfärdaren beskriva sådana kontroller denne tillämpar då kontrakterad personal utför sådant arbete.

Styrande krav i Tillitsramverket

* K2.6, K3.2, K3.3

**Svar B4.3.3 – Beskrivning av krav vid utkontraktering av personal:**

|  |
| --- |
|  |

#### 4.4 Spårbarhet och loggning

Följande avsnitt avses omfatta all den information som krävs för att säkerställa uppföljning av säkerhetsrelaterade händelser, även innefattande den information som krävs för revision av ledningssystem, med mera.

##### 4.4.1 Händelser som registreras i säkerhetslogg

Registrering av så kallad behandlingshistorik eller säkerhetslogg ska innefatta samtliga händelser som relaterar till livcykelhanteringen av e-legitimationer, såväl som personals åtkomst till känsliga informationstillgångar och system. Utfärdaren ska här redogöra för de grundprinciper som gäller för sådan registrering.

Styrande krav i Tillitsramverket

* K2.7

**Svar B4.4.1 – Beskrivning av händelser som registreras i säkerhetslogg:**

|  |
| --- |
|  |

##### 4.4.2 Kontroll och uppföljning av säkerhetsrelaterade händelser

Utfärdaren ska beskriva under vilka premisser regelbunden och särskild kontroll av säkerhetsrelaterade händelser sker. Exempel kan innefatta stickprov av dokumentation som stödjer att utfärdandeprocessen fungerar som avsett, eller kontroller av vilken personal som sökt åtkomst till vilken information och när, samt i vilken mån de haft befogenhet att vidta dessa åtgärder.

Styrande krav i Tillitsramverket

* K2.9, K3.3

**Svar B4.4.2 – Beskrivning av kontroll och uppföljning av säkerhetsrelaterade händelser:**

|  |
| --- |
|  |

##### 4.4.3 Skydd av spårbarhetsinformation

Information som registreras i säkerhetslogg eller bevaras för revisions- och uppföljningsändamål kan vara av både integritetskänslig och säkerhetskritisk karaktär. Utfärdaren ska beskriva de åtgärder som vidtagits för att säkerställa dessa informationstillgångars sekretess, deras integritet samt även spårbarheten vid åtkomst till dem.

Styrande krav i Tillitsramverket

* K3.3, K4.1

**Svar B4.4.3 – Beskrivning av skydd av spårbarhetsinformation:**

|  |
| --- |
|  |

##### 4.4.4 Handlingars bevarande

Den spårbarhetsinformation som krävs för uppföljning ska bevaras i enlighet med bestämmelserna i Tillitsramverket. Utfärdaren ska beskriva hur sådant bevarande säkerställs då informationen t.ex. flyttas ur systemen för att arkiveras. Detta ska innefatta beskrivning av hur det är säkerställt att informationen kan eftersökas, läsas tillbaka och tolkas under hela tiden för bevarande. Beskrivningarna ska även innefatta hur det är säkerställt att fysiska handlingar kan återsökas under samma förutsättningar.

Styrande krav i Tillitsramverket

* K2.8

**Svar B4.4.4 – Beskrivning av handlingars bevarande:**

|  |
| --- |
|  |

##### 4.4.5 Gallring

Då tiden för bevarande förlöpt ska spårbarhetsinformationen gallras. Vid gallring ska sådan information utplånas på ett säkert sätt, så att den inte enkelt kan återskapas. Olika informationstyper kan också ha olika tid för bevarande. Utfärdaren ska redogöra för hur information gallras på ett sådant sätt att dessa krav är uppfyllda.

Styrande krav i Tillitsramverket

* K2.8

**Svar B4.4.5 – Beskrivning av gallring:**

|  |
| --- |
|  |

#### 4.5 Operationella aspekter

##### 4.5.1 Kontinuitetsplanering

Utfärdaren ska ha upprättat en kontinuitetsplan som säkerställer förmågan att återställa kritiska processer vid händelse av allvarliga incidenter eller kris. Denna kontinuitetsplan ska även regelbundet testas och övas. Utfärdaren ska redogöra för det övergripande innehållet i denna kontinuitetsplan, och med vilken frekvens den testas och övas.

Styrande krav i Tillitsramverket

* K2.4, K6.9, K7.1

**Svar B4.5.1 – Beskrivning av kontinuitetsplanering:**

|  |
| --- |
|  |

##### 4.5.2 Incidenthantering

Incidenthanteringen är ett av de viktigaste verktygen att förebygga och att lindra konsekvenserna av en säkerhetshändelse. I detta avsnitt ska utfärdaren redogöra för hur de interna rutinerna kring incidenthanteringen fungerar, till exempel innefattande hur händelseförlopp och rotorsaker utreds, införande av konsekvensbegränsande och förebyggande åtgärder samt utvärdering och uppföljning.

Styrande krav i Tillitsramverket

* K2.4

**Svar B4.5.2 – Beskrivning av incidenthanteringsprocessen:**

|  |
| --- |
|  |

##### 4.5.3 Avveckling av tjänsten

En avveckling av tjänsten ska ske under kontrollerade former. Utfärdaren ska redogöra för de övergripande momenten i en sådan avvecklingsprocess, innefattande hur dess användare informeras och hur information som ska bevaras hålls tillgänglig.

Styrande krav i Tillitsramverket

* K5.5

**Svar B4.5.3 – Beskrivning av avveckling av tjänsten:**

|  |
| --- |
|  |

### 5. Teknisk säkerhet

#### 5.1 Kryptografiska funktioner

Säkerheten i hanteringen och användningen av e-legitimationer beror till betydande del på starka kryptografiska funktioner. För att säkerställa denna styrka är det viktigt att de kontroller som omgärdar nyckelhanteringen är baserade på välkända och genomlysta funktioner och metoder. I de följande underavsnitten ska utfärdaren visa hur denne har säkerställt en hög säkerhet i kryptografiska funktioner och kring hanteringen av sådant känsligt kryptografiskt nyckelmaterial som används för att utfärda e-legitimationer, identifiera innehavare och ställa ut identitetsintyg.

##### 5.1.1 Kryptografiska algoritmer och nyckeltyper

Grundläggande är att utfärdaren har identifierat vilka kryptografiska nycklar denne hanterar inom ramen för utfärdarverksamheten, och kategoriserat dessa. I detta avsnitt ska utfärdaren redogöra för de kryptografiska algoritmer och de kategorier, hierarkier och kedjor av kryptografiskt nyckelmaterial som säkerheten i utfärdarverksamheten kan komma att bero på.

Styrande krav i Tillitsramverket

* K4.1, K4.3

**Svar B5.1.1 – Beskrivning av kryptografiska algoritmer och nyckeltyper:**

|  |
| --- |
|  |

##### 5.1.2 Nycklars livscykel

I detta avsnitt ska utfärdaren redogöra för de olika administrativa livslängder som utfärdaren tilldelat olika kategorier av nycklar, det vill säga vilken utbytesfrekvens som ska gälla och vilka olika faser som existerar i nycklarnas livscykel.

Styrande krav i Tillitsramverket

* K4.1

**Svar B5.1.2 – Beskrivning av nycklars livscykel:**

|  |
| --- |
|  |

##### 5.1.3 Omgivning och metodik för nyckelframställning

Det sätt på vilket krypteringsnycklar framställs kan vara avgörande för de kryptografiska säkerhetsfunktionernas styrka. I detta avsnitt ska utfärdaren beskriva det sätt och den omgivning som används för att framställa nycklar inom utfärdarverksamheten. Den källa och metod till slumptalsframställning, samt den metod som används för att säkerställa nyckelparametrars kvalitet ska även beskrivas.

Styrande krav i Tillitsramverket

* K4.1, K4.3

**Svar B5.1.3 – Beskrivning av omgivning och metodik för nyckelframställning:**

|  |
| --- |
|  |

#### 5.2 Förvaring och skydd av privata nycklar

Stora delar av informationssäkerhetsskyddet utgår ifrån att utfärdarens privata nycklar hålls konfidentiella över förhållandevis lång tid. Detta fordrar rigorösa kontroller i nyckelhanteringen.

##### 5.2.1 Skydd av privata nycklar

I enlighet med tillitsramverket ska konfidentiellt nyckelmaterial som utfärdaren hanterar i anslutning till e-legitimationer skyddas genom användning av kryptografisk hårdvarumodul med aktiva säkerhetsmekanismer som skyddar mot både fysiska och logiska försök att röja nyckelmaterialet. I detta avsnitt ska utfärdare beskriva hur skyddet är inordnat och hur åtkomsten att bruka nycklarna är styrd.

Styrande krav i Tillitsramverket

* K4.3

**Svar B5.2.1 – Beskrivning av skydd av privata nycklar:**

|  |
| --- |
|  |

##### 5.2.2 Säkerhetskopiering av privata nycklar

Vissa privata nycklar kan behöva säkerhetskopieras då de inte med enkelhet snabbt kan bytas vid en eventuell förlust. Utfärdare ska övergripande redogöra för vilka nycklar denne anser kräver säkerhetskopiering, och hur dessa säkerhetskopior görs och hur säkerhetskopiorna skyddas.

Styrande krav i Tillitsramverket

* K4.1, K4.3

**Svar B5.2.2 – Beskrivning av säkerhetskopiering av privata nycklar:**

|  |
| --- |
|  |

##### 5.2.3 Utplåning av privata nycklar

I detta avsnitt ska utfärdaren övergripande redogöra för de procedurer som denne tillämpar för att utplåna känsligt nyckelmaterial ifrån t.ex. uttjänt lagringsmedia eller utrangerad utrustning.

Styrande krav i Tillitsramverket

* K4.1

**Svar B5.2.3 – Beskrivning av procedurer för utplåning av privata nycklar:**

|  |
| --- |
|  |

#### 5.3 Säkerhet i drift- och utvecklingsmiljö

##### 5.3.1 Systemsäkerhet

Utfärdare ska redogöra för de principer denne tillämpar för att upprätthålla den tekniska systemsäkerheten i de olika delsystemen, innefattande säkerhet i operativsystem, åtkomststyrning, införande av kritiska säkerhetsrättningar, granskningar, med mera.

Styrande krav i Tillitsramverket

* K4.1

**Svar B5.3.1 – Beskrivning av principer för upprätthållande av systemsäkerhet:**

|  |
| --- |
|  |

##### 5.3.2 Systemutveckling

Utfärdare som utvecklar egen programvara som används inom utfärdarverksamheten och är av betydelse för säkerheten, ska redogöra för de principer som råder för säkerställande av kvalitet och säkerhet i utvecklingsprocessen.

Styrande krav i Tillitsramverket

* K4.1, K4.4

**Svar B5.3.2 – Beskrivning av kvalitetssäkringsrutiner i systemutvecklingsprocessen:**

|  |
| --- |
|  |

##### 5.3.3 Systemunderhåll och styrning av ändringar i drift

I systemunderhåll ingår att regelbundet införa ny funktionalitet, ändringar och programrättningar i operativ- och tillämpningssystem. I detta avsnitt ska utfärdaren redogöra för principerna för hur sådana ändringar testas och införs i driftmiljön, och hur det är säkerställt att informationssäkerhetsskyddet upprätthålls i samband med sådana ändringar. Utfärdaren ska även redogöra för hur ofta servicetillfällen förekommer, hur de planeras och godkänns samt vilka åtgärder som vidtas om avbrott riskerar att vara längre än planerat.

Styrande krav i Tillitsramverket

* K4.1, K4.4

**Svar B5.3.3 – Beskrivning av rutiner för styrning av ändringar i drift:**

|  |
| --- |
|  |

##### 5.3.4 Styrmedel för nätverkskommunikation

Logiskt sektionerade nätverk med indelning i olika säkerhetszoner och filtrering av kommunikation däremellan är en generell metod för att hantera de hot och lindra de sårbarheter som uppstår vid kommunikation över öppna nätverk. Utfärdare ska på en principiell nivå redogöra för hur sådan sektionsindelning och filtrering är införd. Vidare ska sådana krypteringsåtgärder som vidtagits för att förhindra insyn, manipulation och återuppspelning av kommunikation beskrivas. Även mekanismer som införts och förberedelser som vidtagits för att lindra effekterna av eventuella överbelastningsangrepp ska belysas.

Styrande krav i Tillitsramverket

* K4.1, K4.2, K6.8, K7.1

**Svar B5.3.4 – Beskrivning av styrmedel för nätverkskommunikation:**

|  |
| --- |
|  |

##### 5.3.5 Spårbar tid

Korrekt tid är en avgörande faktor för säkerheten vid utfärdande och användning av e-legitimationer, utställande av identitetsintyg och registrering av händelser i behandlingshistorik (säkerhetslogg). Utfärdaren ska redogöra för de åtgärder man vidtagit för att säkerställa tillgången till korrekt och spårbar tid.

Styrande krav i Tillitsramverket

* K4.1

**Svar B5.3.5 – Beskrivning av tillgång till spårbar tid:**

|  |
| --- |
|  |

##### 5.3.6 Säkerhetskopiering

I detta avsnitt ska utfärdaren beskriva vilka åtgärder som vidtagits för att förhindra dataförlust, samt hur förmågan att återställa information från säkerhetskopior inom erforderlig tid upprätthålls, t.ex. genom återläsningstester. Det ska även framgå principer för förvaring av säkerhetskopior och hur ofta återställning testas.

Styrande krav i Tillitsramverket

* K4.1

**Svar B5.3.6 – Beskrivning av rutiner för säkerhetskopiering:**

|  |
| --- |
|  |

##### 5.3.7 Övervakning

Utfärdare ska redogöra för principer kring hur övervakning av kritiska system görs, och med vilka fastställda prioriteringar och åtgärdstider upptäckta avvikelser hanteras.

Styrande krav i Tillitsramverket

* K4.1

**Svar B5.3.7 – Beskrivning av rutiner för övervakning:**

|  |
| --- |
|  |

### 6. Ansökan, identifiering och registrering

#### 6.1 Ansökan och information om villkor

Utfärdaren ska beskriva hur ansökningsfarandet går till och hur det säkerställs att villkoren förknippade med tjänsten kommer den som söker e-legitimation till del innan denne ingår avtal med utfärdaren. Även förutsättningar för att förändra dessa villkor ska belysas.

Styrande krav i Tillitsramverket

* K5.1, K5.2, K5.6, K5.7

**Svar B6.1a – Beskrivning av ansökningsförfarandet och information om villkor:**

|  |
| --- |
|  |

**Svar B6.1b – Bifoga allmänna villkor:**

|  |  |
| --- | --- |
| Bekräfta att utfärdarens allmänna villkor finns bilagerad ansökan. | **Ja** ­ |

#### 6.2 Identifiering och registrering

##### 6.2.1 Fastställande av sökandens identitet

Utfärdaren ska i denna del belysa hur identiteten på den som ansöker om e-legitimation fastställs, om det är fråga om ett distansförfarande eller om identifiering sker vid ett personligt besök.

Om distansförfarande enligt K5.11 används ska utfärdaren även beskriva det rättsligt eller ekonomiskt betydelsefulla förhållande som råder mellan den som ansöker om e-legitimation och utfärdaren, samt de metoder som används för att på ett säkert sätt identifiera sökanden på distans.

För andra distansförfaranden åligger det utfärdaren genom lämnade beskrivningar visa att de rutiner och metoder som tillämpas är tillräckliga mot bakgrund av de risker som föreligger i fastställandet av sökandens identitet. Det innebär att särskilt höga krav ställs på utfärdaren att lämna ingående beskrivningar. För metoder som bygger på biometrijämförelser ska intyg från genomförda tekniska provningar bifogas som bekräftar tillförlitligheten i metoderna utifrån de konfigurationsparametrar som utfärdaren tillämpar.

Styrande krav i Tillitsramverket

* K5.8-K5.13

**Svar B6.2.1 – Beskrivning av fastställande av sökandens identitet:**

|  |
| --- |
|  |

##### 6.2.2 Registreringsförfarande

Utfärdaren ska beskriva hur lämnade uppgifter om den som ansöker om e-legitimation verifieras, vilka uppgifter som lämnas och registreras samt den metod och källa utfärdaren använder för att kontrollera uppgifter, samt rutiner för att hålla detta register aktuellt.

Styrande krav i Tillitsramverket

* K5.8, K5.9, K5.14

**Svar B6.2.2 – Beskrivning av registreringsförfarandet:**

|  |
| --- |
|  |

#### 6.3 Utfärdande och spärr av e-legitimation

##### 6.3.1 Utformning av tekniska hjälpmedel

I detta avsnitt ska utfärdaren beskriva utformningen av de tekniska hjälpmedel (e-legitimationshandling och eventuellt tillkommande tekniskt stöd) som denne tillhandahåller den som ansöker om e-legitimation.

Utfärdaren ska också beskriva vilka skyddsmekanismer som omgärdar användares privata nyckelmaterial, innefattande hur kraven upprätthålls gällande kvalitet i personlig kod och skydd mot att koden röjs till utomstående.

Vidare ska beskrivas hur, om och under vilka förutsättningar användares e-legitimationer kan komma att blockeras. Med blockering avses här i den mån e-legitimationen har sådant aktivt skydd som blockerar (spärrar) användningen om aktivering misslyckats.

I den mån biometrisk aktivering används ska utfärdaren beskriva säkerheten och tillförlitligheten i den biometriska avläsningen och jämförelsen, så att motsvarande nivå av skydd erhålls som vid aktivering med personlig kod.

Styrande krav i Tillitsramverket

* K6.1, K6.2, K6.3

**Svar B6.3.1a – Beskrivning av utformning av tekniska hjälpmedel:**

|  |
| --- |
|  |

**Svar B6.3.1b – Exempel på tekniska hjälpmedel:**

|  |  |
| --- | --- |
| Bekräfta att utfärdaren på begäran från DIGG kan tillhandahålla exemplar av tekniska hjälpmedel för granskning i samband med ansökan. | **Ja** ­ |

##### 6.3.2 Skapande av e-legitimationshandling

Utfärdaren ska redogöra för hur innehavares privata nycklar skapas, lagras och skyddas då de tillhandahållits innehavaren.

I de fall då symmetriska kryptografiska funktioner används för identifiering av innehavare, ska även anges och hur dessa nycklars eller koders konfidentialitet skyddas i utfärdarens tekniska omgivning vid verifiering av sådana e-legitimationer.

Utfärdaren ska också beskriva vilka identitetsbegrepp (unika identifierare, löpnummer eller motsvarande) denne använder internt för kontroll och spärr av enskilda e-legitimationshandlingar.

Styrande krav i Tillitsramverket

* K4.3, K6.2, K6.4, K6.5

**Svar B6.3.2 – Beskrivning av skapande av e-legitimationshandling:**

|  |
| --- |
|  |

##### 6.3.3 Tillhandahållande av e-legitimationshandling

Utfärdaren ska i detta avsnitt beskriva hur tillhandahållandet av e-legitimat­ionshandlingen sker, om detta sker vid personligt besök eller på distans och hur det annars säkerställs att e-legitimationshandlingen tillhandahålls till rätt mottagare.

Om aktiveringsdata framställts som del i utgivningsprocessen behöver även detta distribueras till innehavaren på ett säkert sätt. Normalt tillhandahålls aktiveringsdatat skilt från e-legitimationshandlingen. Under denna process är det viktigt att aktiveringsdatats konfidentialitet skyddas. Utfärdaren ska mot bakgrund av vad denne angett i det föregående beträffande aktiveringsdata, beskriva de procedurer som används för att distribuera aktiveringsdatat till de avsedda mottagarna.

Styrande krav i Tillitsramverket

* K6.2, K6.6, K6.7

**Svar B6.3.3a – Beskrivning av process för tillhandahållande av e-legitimationshandling:**

|  |
| --- |
|  |

**Svar B6.3.3b – Exempel på tillhandahållande av e-legitimationshandling:**

|  |  |
| --- | --- |
| Bekräfta att utfärdaren på begäran från DIGG kan tillhandahålla exempel på sådan kommunikation som används i samband med tillhandahållande av e-legitimationshandling. | **Ja** ­ |

#### 6.4 Spärrtjänst

##### 6.4.1 Rutin för begäran om spärr

Utfärdaren ska beskriva vilka sätt som står till buds för innehavare att spärra sin e-legitimation, och hur det är rimligt säkerställt att missbruk av spärrfunktionen inte kan förekomma.

Styrande krav i Tillitsramverket

* K6.8, K6.9

**Svar B6.4.1 – Beskrivning av rutin för begäran om spärr:**

|  |
| --- |
|  |

##### 6.4.2 Befogenhet att begära spärr

Utfärdaren ska beskriva vilka andra, förutom innehavaren själv, som har befogenhet att begära spärr av en e-legitimationshandling och vilka kontroller som i så fall tillämpas.

Styrande krav i Tillitsramverket

* K6.8, K6.9

**Svar B6.4.2 – Beskrivning av befogenhet att begära spärr:**

|  |
| --- |
|  |

##### 6.4.3 Behandlingstid vid begäran om spärr

Utfärdaren ska beskriva hur lång tid det maximalt ska ta från det att denne erhållit en spärrbegäran till dess att begäran är effektuerad och i kraft.

Styrande krav i Tillitsramverket

* K6.8, K6.9

**Svar B6.4.3 – Beskrivning av behandlingstid vid begäran om spärr:**

|  |
| --- |
|  |

### 7. Kontroll av innehavares elektroniska identitetet

Utfärdaren ska i detta avsnitt beskriva det autentiseringsförfarande som används för att verifiera innehavares elektroniska identiteter och hur det är säkerställt att utomstående inte genom gissning, avlyssning, återuppspelning eller manipulation av processen kan forcera skyddsmekanismerna.

Styrande krav i Tillitsramverket

* K7.1, K7.2

**Svar B7.1 – Beskrivning av autentiseringsförfarandet:**

|  |
| --- |
|  |

### 8. Utställande av identitetsintyg

Utfärdaren ska i detta avsnitt, i tillämpliga delar, beskriva den eller de tjänster som tillhandahålls för utställande av identitetsintyg.

#### 8.1 Intygsgivningstjänstens tillgänglighet

Beskrivningarna i denna del ska innefatta vilken utlovad tillgänglighet funktionen för utställande av identitetsintyg har, hur denna tillgänglighet mäts och följs upp, vad som ska betraktas som godtagbara svarstider samt vilka åtgärder som är vidtagna för att säkerställa upprätthållandet av denna servicegrad.

Styrande krav i Tillitsramverket

* K8.1

**Svar B8.1 – Beskrivning av intygsgivningstjänstens tillgänglighet:**

|  |
| --- |
|  |

#### 8.2 Skydd mot missbruk av identitetsintyg och intygsgivningstjänst

Utfärdaren ska i detta avsnitt beskriva vilka åtgärder som vidtagits för att förhindra att identitetsintyg missbrukas av obehöriga. Denna redogörelse ska innefatta:

* säkerhetsåtgärder vidtagna för att förhindra eller försvåra för så kallat nätfiske och motsvarande bedrägliga metoder som syftar till att lura användaren att legitimera sig mot en falsk intygsgivningstjänst,
* säkerhetsåtgärder vidtagna för att förhindra eller försvåra avlyssning eller manipulation av kommunikation och intyg,
* lämnade intygs giltighetstid, samt
* de tidsbegränsningar av identifierade användarens anslutningar, varefter en ny identifiering av användaren krävs.

Styrande krav i Tillitsramverket

* K8.2, K8.3

**Svar B8.2 – Beskrivning av skydd mot missbruk av identitetsintyg och intygsgivningstjänst:**

|  |
| --- |
|  |

#### 8.3 Skydd mot obehörig åtkomst

Den riskanalys utfärdaren regelbundet ska genomföra förväntas identifiera intygsgivningstjänsten som särskilt utsatt för risk, då denna i normalfallet har en hög exponeringsgrad samtidigt som säkerhetsberoendet till denna funktion är mycket stort. Särskilt rigorösa tekniska säkerhetskontroller och kvalitetssäkringsrutiner förväntas därför omgärda denna del.

Utfärdaren ska redogöra för vilka särskilda skyddsåtgärder denne vidtagit i intygsgivningsfunktionen, och som syftar till att:

* förhindra missbruk eller röjande av det känsliga kryptografiska nyckelmaterial som tjänsten kräver åtkomst till,
* förhindra kvalificerade och motiverade angripare från att göra intrång i intygsgivningstjänsten,
* försök till eller faktiskt sådant intrång, missbruk eller röjande av nyckelmaterial inte ska kunna undgå upptäckt.

Styrande krav i Tillitsramverket

* K4.1

**Svar B8.3 – Beskrivning av skydd mot obehörig åtkomst:**

|  |
| --- |
|  |

### 9. Revision

För att verifiera att införda kontroller fungerar och är effektiva ska utfärdaren genomföra internrevision av de delar av utfärdarverksamheten som omfattas av tillitsramverket. I den mån revision av ledningssystemet för informationssäkerhet sker separat från revision gentemot tillitsramverkets krav ska även aspekter kopplade till detta belysas i efterföljande avsnitt.

#### 9.1 Revisionens periodicitet och omfattning

Utfärdare ska redogöra för den funktion för internrevision som inrättats för att granska verksamheten. Det ska framgå med vilken periodicitet och med vilken omfattning varje revision ska görs. Redogörelsen ska även omfatta process för revisionsplanering samt beskrivning av revisionsrapportering, inklusive hantering av uppföljning av eventuella avvikelser.

Styrande krav i Tillitsramverket

* K2.9

**Svar B9.1a – Beskrivning av revisionens periodicitet och omfattning:**

|  |
| --- |
|  |

**Svar B9.1b – Bekräftelse avseende revisionsplan och revisionsrapport:**

|  |  |
| --- | --- |
| Bekräfta att utfärdaren på begäran från DIGG kan presentera revisionsplan samt revisionsrapport från senast genomförda revision. | **Ja** ­ |

#### 9.2 Revisorns kvalifikationer

Utfärdaren ska redogöra för vilka formella kompetenskrav som ställs på den huvudansvariga revisorn.

Styrande krav i Tillitsramverket

* K2.9

**Svar B9.2 – Beskrivning av revisorns kvalifikationer:**

|  |
| --- |
|  |

#### 9.3 Revisorns förhållande till den granskade parten

Utfärdaren ska redogöra för det förhållande som råder mellan den ansvariga revisorn och ansvariga inom utfärdarverksamheten, i syfte att garantera revisorns oberoende gentemot utfärdarverksamheten.

Styrande krav i Tillitsramverket

* K2.9

**Svar B9.3 – Beskrivning av revisorns förhållande till den granskade parten:**

|  |
| --- |
|  |

#### 9.4 Åtgärder vid upptäckt av brist

Utfärdaren ska redogöra för hur upptäckta brister kommuniceras och hur lämpliga förbättringsåtgärder utvecklas och införs.

Styrande krav i Tillitsramverket

* K2.4, K2.9

**Svar B9.4 – Beskrivning av åtgärder vid upptäckt av brist:**

|  |
| --- |
|  |

### 10. Övrigt

#### 10.1 Kundtjänst

Utfärdaren ska här beskriva den kundtjänst och support till slutanvändare och förlitande parter som erbjuds. Utfärdaren ska även ange öppettider för sådan kundtjänst samt kontaktuppgifter till den.

**Svar B10.1 – Beskrivning av kundtjänst:**

|  |
| --- |
|  |

#### 10.2 Användbarhet och tillgänglighet

Utfärdaren ska övergripande redogöra för sitt arbete med användbarhet och tillgänglighet i de gränssnitt som möter slutanvändare som utfärdaren ansvarar för.

**Svar B10.2 – Beskrivning av arbete med användbarhet och tillgänglighet:**

|  |
| --- |
|  |