MYNDIGHETEN FÖR DIGITAL FÖRVALTNING
Agency for Digital Government

Ärendenr 2018-158

Bilaga 4 till licensavtal för utfärdare av Svensk e-legitimation

Rapporteringsrutiner

1. Bakgrund och syfte

1.1 Detta dokument är en bilaga till huvudtexten i Licensavtalet för utfärdare av Svensk e-legitimation (Avtalet). De begrepp som definieras i huvudtexten har samma betydelse i denna bilaga.

1.2 Bilagan redovisar de rutiner som ska gälla avseende rapportering av säkerhetsrelaterade händelser, funktionsfel och övriga störningar.

2. Definitioner

I denna bilaga betyder

1. *Rapporteringspliktig säkerhetsincident*: en oönskad och oplanerad händelse som kan påverka säkerhetsskyddet omgärdande hanteringen av e-legitimationer eller den generella tilltron till Svensk e-legitimation, eller som kan innebära en störning i Utfärdarens förmåga att fullgöra de åtaganden enligt Avtalet,

2. *Allvarlig säkerhetsincident*: Rapporteringspliktig säkerhetsincident som kan komma att föranleda omedelbara åtgärder från Myndigheten för digital förvaltnings sida.

3. Kontaktvägar

3.1 Utfärdaren ska rapportera till Myndigheten för digital förvaltning.

3.2 Utfärdaren ska:

(a) etablera och upprätthålla kontaktvägar för rapportering till och från Myndigheten för digital förvaltning, samt

(b) hålla Myndigheten för digital förvaltning underrättad om aktuella kontaktvägar och kontaktuppgifter för denna rapportering.

3.3 Rapportering och återkoppling ska ske med elektroniska medel.

4. Incidentrapportering

4.1 Utfärdaren ska utan dröjsmål rapportera Allvarliga säkerhetsincidenter.

4.2 Så länge en händelse, som är rapporterad enligt punkt 4.1, är pågående ska Utfärdaren hålla Myndigheten för digital förvaltning uppdaterad om händelsen.

4.3 Incidentrapport enligt 4.1 ska omfatta:

(a) Utfärdarens namn (**rapportör**),

(b) kort beskrivande benämning på händelsen (**namn**),

(c) unik referens för händelsen (**referens**),

(d) status på händelsen (**status**),

(e) kategorisering av händelsen (**kategorisering**),

(f) när händelsen inträffade eller den uppskattade tidpunkten för den (**tidpunkt**),

(g) när Utfärdaren upptäckte händelsen (**upptäckt**),

(h) en översiktlig beskrivning av händelsen (**beskrivning**), och

(i) bedömning av händelsens omfattning och konsekvenser samt annan information som kan vara av värde (**analys**).

Rapporten ska, såvitt avser struktur och format, utformas enligt Myndigheten för digital förvaltnings vid var tid skäligen lämnande instruktioner.

Om Utfärdaren inte har fullständiga uppgifter i alla delar för rapporten vid rapporteringsögonblicket kan rapporten kompletteras vid senare tillfälle.

I vissa fall kan det vara lämpligt eller nödvändigt att lämna begränsat med information i incidentrapporten. Det kan till exempel gälla om händelsen polisanmäls eller för att inte känslig information ur ett informationssäkerhetsperspektiv ska avslöjas. Se även avsnitt 8 om allmän handling.

4.4 På anmodan av Myndigheten för digital förvaltning ska Utfärdaren komplettera inlämnade uppgifter om en Rapporteringspliktig säkerhetsincident med de uppgifter som behövs för att klarlägga hur händelsen kan påverka säkerhetsskyddet omgärdande hanteringen av e-legitimationer.

4.5 Om Utfärdaren använder sig av underleverantör för att utföra del av tjänst, ska Utfärdaren genom avtal med underleverantören säkerställa att Rapporteringspliktiga säkerhetsincidenter kan hanteras och rapporteras på det sätt som framgår av denna bilaga.

5. Rapportering

5.1 Utfärdare ska två gånger per år sammanställa en rapport avseende alla Rapporteringspliktiga säkerhetsincidenter som inträffat under den gångna sexmånadersperioden, sammanställt med antal händelser fördelade på kategori och påverkansgrad.

5.2 Rapporterna ska avse perioderna januari till och med juni respektive juli till och med december och vara Myndigheten för digital förvaltning tillhanda senast sista vardagen i månaden efter respektive sexmånadersperiods utgång.

5.3 Rapporten ska, såvitt avser struktur och format, utformas enligt Myndigheten för digital förvaltnings vid var tid skäligen lämnande instruktioner.

6. Förändringar

6.1 Utfärdaren ska till Myndigheten för digital förvaltning rapportera alla väsentliga förändringar i Utfärdarens utförande av sina åtaganden enligt Avtalet.

6.2 Rapportering av sådan förändring ska ske senast i samband med att förändringen träder i kraft.

7. Myndigheten för digital förvaltnings återkoppling

7.1 Myndigheten för digital förvaltning ska ge återkoppling till Utfärdaren vad som framkommit av Utfärdarens rapporter och Myndigheten för digital förvaltnings arbete i övrigt avseende säkerhetsfrågor.

7.2 Återkoppling ska ges regelbundet och i övrigt när det behövs för säkerhetsskyddet omgärdande hanteringen av e-legitimationer.

8. Allmän handling, sekretess, etc.

8.1 Information som inkommer till eller lämnas ut av Myndigheten för digital förvaltning blir allmän handling hos myndigheten. Allmän handling kan begäras utlämnad. Vid utlämnade ska en sekretessprövning ske. Även om myndigheten bedömer att handlingen inte kan lämnas ut på grund av att handlingen innehåller uppgifter som omfattas av sekretess kan det inte garanteras att handlingen inte kommer att lämnas ut, eftersom myndighetens beslut kan komma att prövas i domstol. Rapportering till och från Myndigheten för digital förvaltning bör därför inte omfatta information som kan skada säkerhetsskyddet omgärdande hanteringen av e-legitimationer eller annan typ av information som kan betraktas som affärshemlig.