Tillitsdeklaration för RA

Pointsharp Secure Cloud Net iD SweID

Classification:	Internal
Publication No.:	PSC-Rd22-12
Document version:	1.0
Document status:	Final
Date:	03 Jun 2022

Table of Contents

Om detta dokument

Detta formulär måste besvaras av organisationer som vill ansöka om rätten att utfärda LoA3 elektroniska identiteter (e-legitimationer) inom PoSC Net iD SweID-tjänsten (hädanefter kallad "Tjänsten") i enlighet med Tillitsramverket för PoSC Net iD SweID (hädanefter kallad "Tillitsramverket"). Detta gäller första ansökan och efterföljande periodiska granskningar. Tillitsdeklarationen måste återspegla de faktiska förhållandena inom de delar av organisationen som hanterar Tjänsten.

I det här formuläret listas kraven för Tillitsramverket tillsammans med en förklaring av det specifika kravet och vägledning om vad svaren ska innehålla. Det rekommenderas starkt att läsa Tillitsramverket i förväg för att kunna besvara blanketten korrekt.

Svaren ska skrivas i rutorna avsedda för ändamålet. Texterna i rutorna anpassas automatiskt efter hur mycket text man skriver. Om svarsrutan inte räcker till kan utförligare svar bifogas i separat dokument. Om svaret hänvisar till interna handlingar ska de bifogas och märkas med det stycke från vilket de hänvisas eller på annat sätt lätt kunna identifieras.

1 Allmänna krav och information

1.1 Sökandes information

Sökande organisation	
Organisationsnamn	
Organisationsnummer	
Leveransadress	
Postnummer	
Postadress	
Kontaktperson	
Namn	
E-post	
Telefonnummer	

1.2 Inlämning av ansökan

Ansökningshandlingen i original ska skickas med rekommenderat brev eller överlämnas i förseglat kuvert till:

Pointsharp AB
att: PsPT
Uddvägen 7
SE-131 54 Nacka
Sweden

Denna tillitsdeklaration lämnas in av:

Organisationsnamn:	
Organisationsnummer:	
Formulärets versionsnummer:	
Plats och datum för inlämning:	
Namn (kontaktperson):	
E-post (kontaktperson):	
Telefonnummer (kontaktperson):	

1.3 Process för granskning av ansökan

Baserat på svaren i denna ansökan kommer Pointsharp service Policy Team (hädanefter kallad "PsPT") att bedöma om sökanden uppfyller de krav som följer av ansökningsformuläret och återspeglas i Tillitsramverket. I samband med granskningen kan Pointsharp begära komplettering om svaren i ansökan inte är tillräckliga för att avgöra om kraven är uppfyllda.

> ⚠ Där denna blankett används för periodisk granskning är stycke *1.4 Godkännande och undertecknande av avtal* och *1.5 Återkallande av godkännande* inte tillämpliga.

1.4 Godkännande och undertecknande av avtal

Efter godkännandet av ansökan bör sökanden och Pointsharp utan dröjsmål söka teckna ett avtal med villkor som anges i *Kundavtal för Pointsharp Secure Cloud Net iD SweID*.

Godkännandet gäller i 3 månader och upphör automatiskt om inget avtal ingåtts.

1.5 Återkallande av godkännande

Pointsharp förbehåller sig rätten att återkalla ett godkännande om det före ingående av avtal skulle visa sig att sökanden inte uppfyller kraven. Denna situation kan uppstå om de uppgifter som lämnats i ansökan visar sig vara felaktiga eller om det inträffar händelser efter att ansökan beviljats som väsentligt påverkar bedömningen.

1.6 Finansiell position

Den sökande ska beskriva sin finansiella och ekonomiska ställning.

1.7 Affärsverksamhet

Sökanden bör vid tidpunkten för avtalets ingående vara fullt operativ i de delar som berörs av detta avtal.

1.8 Underleverantörer

Om sökanden avser att anlita underleverantörer för att utföra någon del av verksamheten inom Tjänsten bör detta återspeglas i ansökan. Eventuell underleverantör som tillkommer under avtalsperioden måste godkännas av PsPT i förväg innan underleverantören används.

1.9 Obligatorisk dokumentation

Följande handlingar ska bifogas ansökan:

- Registreringsbevis utfärdat av en officiell registreringsmyndighet för organisationer, t.ex. i Sverige "Bolagsverket"
- senast fastställda ekonomiska årsredovisning
- Informationssäkerhetspolicydokument eller motsvarande

1.10 Instruktioner

Frågorna i formuläret hänvisar till respektive stycke i Tillitsramverket. Frågor kan besvaras helt eller delvis genom att hänvisa till dokumentationen. I så fall ska refererad dokumentation bifogas och numreras.

- Ansökan ska skrivas på svenska.
- Alla frågor måste besvaras
- Reservationer mot några villkor kommer inte att accepteras.

Om frågorna innehåller referenser till dokumentationen från Pointsharp, t.ex. *Pointsharp Secure Cloud Net iD SweID Tillitsramverk för RA* eller *Pointsharp Secure Cloud Net iD SweID CP och CPS*, kan dessa dokument laddas ner från https://repository.pointsharpsecurecloud.com.

Om du har frågor om denna ansökan, vänligen kontakta PsPT på pspt@pointsharp.com.

1.11 Assistera vid granskningen

Sökanden ska vara till hjälp under hela den inledande granskningen och de efterföljande periodiska granskningarna.

1.12 Diskvalifikation för godkännande

Pointsharp förbehåller sig rätten att avböja godkännande av någon av skälen nedan:

- Sökanden är föremål för konkurs eller likvidation, genomgår rekonstruktion eller om det finns andra indikationer på finansiell insolvens..
- Sökanden är föremål för ansökan om konkurs, likvidation, rekonstruktion eller motsvarande.
- Någon av sökandens företagsföreträdare har dömts för brott med anknytning till yrket.
- Sökanden har inte fullgjort sina skyldigheter avseende betalning av sociala avgifter eller betalning av skatter i sitt ursprungsland eller i en annan stat som hör till Europeiska ekonomiska samarbetsområdet.

Svar 1.12a – Den sökandes intygande

Sökanden intygar att ingen av de omständigheter som anges i stycke *1.12 Diskvalificering för godkännande* föreligger. Detta gäller även eventuella företagsrepresentanter och underleverantörer.

☐ Ja

1 Kommentarer

1.13 Sekretess

Pointsharp kommer endast att avslöja någon av informationen i Tillitsdeklarationen på begäran av sökanden eller på juridiska grunder på begäran från brottsbekämpande myndigheter. Vidare kommer endast behörig personal inom PsPT, eller annan personal auktoriserad av PsPT, att ha tillgång till informationen.

2 Organisation och styrning

Svar 2a – Organisation och styrning

Beskriv kort hur RA-funktionen är organiserad och i vilken del av organisationen de aktiviteter som är relevanta för Tillitsdeklarationen hanteras.

Svar 2b – Underleverantörer

Om sökanden avser att anlita en underleverantör för att utföra någon del av arbetet inom ramen för utfärdarens skyldigheter ska detta anges i ansökan. Det ska tydligt framgå vilka delar av de efterfrågade tjänsterna som sökanden avser att lägga ut på entreprenad. Lista underleverantörerna med deras fullständiga juridiska namn och organisationsnummer.

Svar 2c – Ekonomisk ställning

Beskriv organisationens finansiella och ekonomiska ställning. I den mån detta inte kan fastställas genom en kreditupplysning, eller om sökanden är medveten om eller misstänker att sådan information kan vara felaktig eller inaktuell, kan sökanden i detta stycke förklara varför så är fallet och hur kravet på en stabil finansiell ställning uppfylls.

2.1 Övergripande krav

"Organisation som vill ansluta sig till Tjänsten, oavsett om det är direkt eller som tredjepart, ska vara en aktiv juridisk person."

Svar 2.1a – Företagsform och ägande

Beskriv den juridiska formen och ägarstrukturen för din organisation.

"Alla RA Officer ska ha fast lön och inte provisionslön vilken påverkas av huruvida en e-legitimation ges ut eller ej."

Svar 2.1b – Den sökandes intygande

Sökanden intygar att ingen anställd arbetar på provisionsbasis där inkomstnivån på något sätt är kopplad till antalet utfärdade e-legitimationer.

☐ Ja

2 Kommentarer

2.1.1 Förordningar

"Varje organisation som direktansluter sig ska lämna in en tillitsdeklaration. En självskattning av deras överensstämmelse med Tillitsramverket och PoSC Net iD CP och CPS inom sin RA-domän."

Svar 2.1.1a – Den sökandes intygande

Sökanden intygar att ha tagit del av innehållet i PoSC Net iD SweID Tillitsramverk och tillämpliga delar av PoSC Net iD SweID CP och CPS.

☐ Ja

2.1.2 Förvaltning

Där detta formulär används för periodisk granskning är stycke *2.1.2 Förvaltning* inte tillämpligt.

" Varje organisation som direktansluter sig för nyttjande av tjänsten ska teckna avtal med Pointsharp AB."

Svar 2.1.2a – Den sökandes intygande

Sökanden kommer efter godkännande av denna ansökan tillsammans med Pointsharp att initiera undertecknandet av ett kundavtal.

☐ Ja

2.2 Tjänstens övergripande dokumentstruktur

[har avsiktligt lämnats tom]

3 Säkerhet och revision

3.1 Informationssäkerhet

"Direktansluten organisation ska ha ett strukturerat säkerhetsarbete som ska omfatta:

1. *en riskhanteringsprocess som kontinuerligt analyserar hot och sårbarheter..."*

Svar 3.1a – Beskrivning av riskhanteringsprocessen

Beskriv riskhanteringsprocessen och hur de identifierade riskerna hanteras.

"En dokumenterad och strukturerad informationssäkerhetshantering:

- *ett dokumenterat informationssäkerhetsarbete med praxis och policyer.*
- *ett ledningssystem för informationssäkerhet (ISMS), enligt ISO/IEC 27001 eller motsvarande, finnas på plats."*

Svar 3.1b – Dokumentation

Den sökande har ett dokumenterat informationssäkerhetsledningsarbete med praxis och policys i form av en Informationssäkerhetspolicy eller motsvarande.

☐ Ja

3 Kommentarer

Svar 3.1c – ISMS

Sökanden har implementerat ett Information Security Management System (ISMS) som används för att säkerställa att den på ett förnuftigt sätt skyddar tillgångarnas konfidentialitet, tillgänglighet och integritet från hot och sårbarheter.

☐ Ja

4 Kommentarer

Svar 3.1d – Säkerhetshantering inom organisationen

Ge en uttömmande beskrivning av hur säkerhetshanteringen sköts i din organisation.

3.2 Kontinuitetsplan

"RA-organisationen måste ha en etablerad och testad kontinuitetsplan"

Svar 3.2a – Kontinuitetsplan: implementerad och testad

Sökanden har en upprättad och dokumenterad kontinuitetsplan som testas regelbundet.

☐ Ja

5 Kommentarer

Svar 3.2b – Kontinuitetsplan: beskrivning

Beskriv kontinuitetsplanen, särskilt med avseende på hur man hanterar om:

- spärrstatusinformation för certifikat (OCSP och/eller CRL) är otillgänglig, antingen genom avbrott hos RA, i internetinfrastrukturen eller i spärrstatustjänsterna som tillhandahålls av Tjänsten.
- utfärdandet av nya e-legitimationer är inte tillgängligt, antingen genom avbrott hos RA, i internetinfrastrukturen eller i Tjänsten.

3.3 Revision från PsPT

”Ansluten organisation kommer regelbundet att vara föremål för revision från PsPT. Revisionen kommer att genomföras i enlighet med den vid varje tidpunkt gällande revisionsprocessen.”

Svar 3.3a – Sökandens certifiering – revision

Den sökande accepterar att när som helst bli granskad av PsPT i enlighet med den revisionsprocess som är gällande.

☐ Ja

"I en sådan granskning ska RA-organisationen omedelbart hjälpa till med att ta fram information och säkerställa att relevant personal finns tillgänglig."

Svar 3.3b – Den sökandes certifiering

Den sökande kommer, i händelse av en revision, omedelbart tillhandahålla den begärda informationen och säkerställa att relevant personal finns tillgänglig för att bistå.

☐ Ja

3.4 Internrevision

"RA-organisationer måste genomföra en internrevision minst var 24:e månad".

Svar 3.4a – Internrevision

Beskriv processer, rutiner och frekvens för internrevision, de områden som omfattas och hur avvikelser hanteras.

3.5 Säkerhetsincidenter

"RA-organisationer måste ha en dokumenterad och implementerad process för hantering av säkerhetsincidenter relaterade till Tjänsten"

Svar 3.5a – Säkerhetsincidenter

Beskriv incidenthanteringsprocessen, särskilt med avseende på de system och miljöer där utfärdandet äger rum och där nyckelbärare lagras. Processen måste innehålla följande:

- eskaleringspunkter, hur och när eskalering inom organisationen och till PsPT görs.
- hur reaktiva, förebyggande och mildrande åtgärder beslutas och implementeras.
- när och på vilket sätt incidentrapporterna görs tillgängliga för PsPT.

3.6 Spårbarhet, gallring och bevarande av dokumentation

"Direktansluten organisation ska bevara den dokumentation som nämns i detta stycke."

Svar 3.6a – Spårbarhet, gallring och bevarande av dokumentation

Beskriv hur dokumentationen bevaras, hur läsbarheten över tid säkerställs samt om och hur gallring genomförs.

4 RA-organisationen

"Varje ansluten RA-organisation måste utse en RA Security Officer, en RA Auditor och RA Officers, samt upprätta en organisation för ansökan, beställning, utdelning, support och spärr av e-legitimationer inom RA-domänen.

Svar 4a – RA-organisationen: organisation

Beskriv hur RA-funktionen är organiserad och vilka roller i organisationen som är utsedda till RA-rollerna.

Svar 4b – RA-organisationen: tillsättningar

Ange namn och kontaktinformation för de personer som utsetts till RA Security Officer och RA Auditor.

RA Security Officer	
Namn	
e-postadress	
Telefonnummer	
RA Auditor	
Namn	
e-postadress	
Telefonnummer	

"Personer som tilldelats en RA-roll måste ha visat lämplighet för rollen."

Svar 4c – RA-organisationen: lämplighet för roll

Beskriv på vilka kriterier du bedömer lämplighet för roller inom RA-organisationen.

4.1 Krav på RA Security Officer

"en identitetskontroll måste utföras av en representant inom RA-organisationen med lämpligt mandat"

Svar 4.1a – Krav på RA Security Officer: Identitetskontroll

Beskriv på vilket sätt och av vem identitetskontrollen utförs.

Svar 4.1b – Krav på RA Security Officer: Resurser

Hur säkerställer den sökande att den som tilldelas rollen har tillräcklig tid och resurser för att utföra arbetet på ett tillfredsställande sätt?

4.1.1 Bakgrundskontroll

"En bakgrundskontroll måste göras av den person som får rollen som RA Security Officer"

Svar 4.1.1a – Krav på RA Security Officer: Bakgrundskontroll

Beskriv processen för bakgrundskontroll, vilka kontroller som görs och på vilka kriterier personen anses lämplig i förhållande till respektive kontroll.

Svar 4.1.1b – Krav på RA Security Officer: Kvalifikationer

Beskriv processen för att bedöma om en person är kvalificerad för att ta på sig rollen som RA Security Officer.

4.2 RA Security Officers skyldigheter

4.2.1 Bakgrundskontroll av RA Auditor och RA Officers

"Innan en person tilldelas en RA-roll inom RA-organisationen måste RA Security Officer kontrollera personens identitet och utföra en bakgrundskontroll"

Svar 4.2.1a – Personliga kontroller av RA Auditor och RA Officers

Beskriv processen för bakgrundskontroller, vilka kontroller som görs och på vilka kriterier en person anses lämplig i förhållande till respektive kontroll.

4.2.2 Utbildning av RA Auditor och RA Officers

"RA Auditor samt alla RA Officers måste ha adekvat kunskap och förmåga."

Svar 4.2.2a – Utbildning av RA Auditor och RA Officers

Beskriv proceduren för att säkerställa att RA Auditor och RA Officers har adekvat kompetensnivå och hur denna kompetens upprätthålls över tid genom kontinuerlig utbildning.

4.3 RA Auditors skyldigheter

"Rollen RA Auditor får inte kombineras med en annan roll inom RA-domänen"

Svar 4.3a – RA Auditors skyldigheter

Sökanden intygar att RA Auditor inte deltar i, eller på annat sätt är involverad i, verksamheten inom RA-domänen.

☐ Ja

4.4 Krav på kontinuitetsplan

[har avsiktligt lämnats tom]

5 Avveckling av RA-domän

"En ansluten organisation som vill avsluta sin anslutning till Tjänsten ska informera Pointsharp genom att säga upp sitt kundavtal som det stipuleras i Kundavtalet."

Svar 5a – Avveckling av RA-domän

Sökanden intygar att i händelse av uppsägning av anslutning, dvs. avveckling av RA-domän, kommer alla steg för uppsägning som beskrivs i Tillitsramverket att följas.

☐ Ja

6 Kommentarer

6 Fysisk och administrativ säkerhet

6.1 Fysisk säkerhet

"Nyckelmaterial och aktiveringsdata ska skyddas fysiskt mot skada och otillåten åtkomst."

Svar 6.1a – Fysisk säkerhet: skydd av nyckelbärare och aktiveringsdata

Beskriv i detalj hur nyckelbärare och känslig data skyddas mot skada och obehörig åtkomst.

Svar 6.1b – Fysisk säkerhet: spårbarhet

Beskriv hur spårbarhet uppnås så att det vid intrång kan upptäckas vad som saknas eller vilken konfidentiell information som kan ha lämnats ut. Särskilt när det gäller nyckelbärare.

6.2 Administrativ säkerhet

"Åtkomst till Tjänsteportalen kräver identifiering med en e-legitimation (minst LoA3) utfärdad till respektive RA Officer."

Svar 6.2 – Administrativ säkerhet: åtkomstkontroll

Den sökande intygar att all personal är informerad om att e-legitimationer som tas emot i deras RA-roll är strikt för personligt bruk.

☐ Ja

7 E-legitimationer

Detta stycke berör processer för hantering av e-legitimationer och är nära relaterat till hanteringsflöden för e-legitimationer som tillhandahålls av Tjänsten, se PoSC Net iD SweID Officer's Guide.

7.1 Användningsområden

[har avsiktligt lämnats tom]

7.2 Villkor

"E-legitimationer får endast lämnas ut efter att användaren har underrättats om, och accepterat Användaravtalet, det vill säga villkoren för användningen av e-legitimationen."

Svar 7.2a – E-legitimationer: Villkor

Beskriv hur du säkerställer att användaren har tagit del av Användaravtalet (villkor för användning av e-legitimationer) innan en e-legitimation delas ut. Prenumerantavtalet kommer att presenteras för användaren på skärmen innan det accepteras och signeras och e-legitimationen tas emot. För att göra processen smidigare rekommenderas att abonnenten får möjlighet att läsa prenumerantavtalet i förväg, antingen skriftligt eller via en webblänk. Användaravtalet tillhandahålls av Tjänsten.

7.3 Giltighetstid för e-legitimation

[har avsiktligt lämnats tom]

7.4 Ansökan om e-legitimation

"e-legitimationer kan tilldelas anställda och konsulter inom RA-organisationerna eller till andra personer med en relation till RA-organisationen"

Svar 7.4a – E-legitimationer: ansökan och organisatorisk relation

Beskriv hur du säkerställer att en användare som man utfärdar en e-legitimation till har en relation till din organisation och beskriv vilka typer av relationer som kommer att vara relevanta (till exempel anställda, konsulter, partners, kunder, studenter)

”En ansökan om e-legitimation ska knytas till personnummer eller styrkt samordningsnummer samt till de uppgifter som i övrigt är nödvändiga för att kunna tillhandahålla e-legitimation."

Svar 7.4b – E-legitimationer: unikhet hos användaridentitet

Beskriv hur du säkerställer att användaridentiteten är unik inom din organisation.

7.5 Beställning av e-legitimation

7.5.1 Kontroll av personuppgifter

"RA Officer ska kontrollera att uppgifterna knutna till ansökan är fullständiga och stämmer överens med de uppgifter som finns registrerade i ett betrott register... "

Svar 7.5.1a – E-legitimationer: Kontroll av personuppgifter

Beskriv vilken/vilka pålitliga kataloger du använder för att kontrollera personuppgifterna när du registrerar användarna i Tjänsten. Beskriv också hur integriteten hos informationen i katalogen/katalogerna garanteras.

7.5.2 Identifiering vid beställning

"Användarens identitet ska verifieras mot ett betrott register, t.ex. Skatteverkets SPAR-tjänst samt visa giltig svensk id-handling."

Svar 7.5.2a – E-legitimationer: identifiering vid beställning

Beskriv hur de olika typerna av användare ursprungligen identifieras när relationen med organisationen etableras.

7.6 Utlämning av e-legitimation

7.6.1 Identifiering vid personligt möte

"All identifiering ska ske enligt av PsPT fastställda rutiner."

Svar 7.6.1a – E-legitimationer: Identifiering vid personligt möte

Beskriv proceduren för att identifiera användaren i samband med utlämnande av en e-legitimation och hur identifiering går till med avseende på "Utlämningsprocess" som beskrivs i Tillitsramverket.

7.6.2 Utlämning vid personligt möte

"Användaren väljer själv sin PIN-kod"

Svar 7.6.2a – E-legitimationer: Utlämning vid personligt möte

Beskriv hur användarens PIN-kod skyddas från obehörigt avslöjande under PIN-inmatningsproceduren.

7.7 Spärr av e-legitimation

"Spärrbegäran måste omedelbart och säkert verkställas av auktoriserad personal"

Svar 7.7a – Spärr av e-legitimation

Beskriv procedurerna för spärr av e-legitimation samt RA-organisationens tillgänglighet för att ta emot och utföra spärrbegäran.

Svar 7.7b – Spärr av e-legitimation: Identifiering av användare

Beskriv kontrollerna som finns för att verifiera att en person som begär spärr av en e-legitimation och påstår sig vara användaren faktiskt är användaren och inte någon annan.

8 Bilagor

Skriv hela dokumentnamnet på de bifogade dokumenten samt numrera dokumenten.

9 Underskrifter

Plats

Datum

Underskrift Sökande organisations kontaktperson

Namnförtydligande

Website
https://www.pointsharp.com

Disclaimer
Specifications subject to change without further notice, unless stated otherwise in agreement.

Classification: Internal
Publ. No.: PSC-Rd22-12
Document version: 1.0
Document status: Final
OID:
Published: 03 Jun 2022