POINTSHARP

Tillitsramverk för RA

Pointsharp Net iD svensk e-legitimation

Classification:	Public
Publication No.:	PSC-Rd22-04
Document version:	2.1
Document status:	Final
Date:	13 Sep 2024

Table of Contents

Revisionshistorik

Version	Datum	Författare	Beskrivning
2.1	13 Sep 2024	PsPT	Förtydligat eller lagt i stycke: • 1.1 Bakgrund och syfte • 2.1 Övergripande krav • 3.1 Revision från Pointsharp • 3.2.2 Internrevision • 3.2.3 Informationssäkerhetsincidenter • 3.2.7 Spårbarhet, gallring och bevarande av information • 4.1.2 Bakgrundskontroll av RA Security Officer • 4.2 RA Auditor och RA Officer • 4.2.2 Bakgrundskontroll av RA Auditor samt RA Officer • 6.6.1 Identifiering vid beställning Nya stycken: • 2.2.1 Tjänstens CP och CPS • 2.2.2 Tillitsramverk för RA • 2.2.3 Tillitsdeklaration • 3.2.2.1 Återkommande granskningar • 4.3 Övriga roller Borttagna stycken: • 6.5.2 Identifiering vid beställning

1. Inledning

1.1. Bakgrund och syfte

Pointsharp Net iD (hädanefter kallad "Tjänsten") tillhandahåller e-legitimationer för identifiering och signering för verksamheter inom privat och offentlig sektor. Tjänsten uppfyller kraven ställda i Tillitsramverk för Svensk e-legitimation framtagen av Myndigheten för digital förvaltning (Digg) (hädanefter kallad "Digg:s Tillitsramverk").

Detta dokument, Pointsharp Net iD Tillitsramverk för RA (hädanefter kallad "Tillitsramverk för RA"), beskriver det tillitsramverk för Tjänsten som alla anslutna RA-organisationer ska efterleva och är baserat på de delar som avser RA i Digg:s Tillitsramverk.

~~beskriver det tillitsramverk för Tjänsten som alla anslutna RA-organisationer ska uppfylla och är baserat på valda delar av DIGG:s Tillitsramverk som även definierar grundkraven för PoSC Net iD SweID Certificate Policy and Certification Practice Statement (hädanefter kallad "Tjänstens CP och CPS"). Tillsammans utgör de basen för alla övriga dokument som ingår i Tjänstens dokumenthierarki.~~

Tillitsramverket för RA syftar till att etablera gemensamma krav inom Tjänsten. Tillämpning av Tillitsramverket för RA beskrivs i de rutiner som fastställs av Pointsharp service Policy Team (PsPT).

Alla RA-organisationer som ska ansluta sig till Tjänsten ska lämna in en tillitsdeklaration (Tillitsdeklaration för RA) där det beskrivs hur organisationen uppfyller kraven enligt Tillitsramverk för RA.

Tjänstens e-legitimationer inkluderar förutom elektroniska certifikat även de nyckelbärare (exempelvis smartkort och mobiltelefon) där certifikat och privata nycklar hanteras.

Kraven på processen för utfärdande av e-legitimationer ser olika ut beroende på tillitsnivå. Tillitsnivå är starkt kopplat till nivå av säkerställande att personen vars uppgifter framgår i e-legitimationen också är den person som den utfärdats till. ~~Med tillitsnivå menas graden av säkerhet och tillförlitlighet.~~ Desto högre tillitsnivå en e-legitimation har desto säkrare är den, både när det gäller teknisk och administrativ säkerhet. Tillitsnivåer förkortas ofta LoA (Level of Assurance). I detta Tillitsramverk beskrivs kraven för att LoA3 ska uppnås. LoA3 är den näst högsta nivån i standarden ISO/IEC 29115, vilken också beskrivs i Digg:s Tillitsramverk.

1.2. Målgrupp

Målgruppen för dokumentet är RA Security Officer, RA Auditor, verksamhetsansvariga inom anslutna RA-organisationer samt rollinnehavare på Pointsharp.

1.3. Identifiering

Detta tillitsramverk gäller för de e-legitimationer som utfärdas enligt nedanstående policyer.

Namn	Objektidentifierare (OID)	Beskrivning
Tillitsramverk för RA	{1.2.752.179.100.1.3}	Detta dokument
~~PoSC Net iD SweID Certificate Policy and Certification Practice Statement~~ Pointsharp Net iD Svensk E-legitimation Certificate Policy and Certification Practice Statement	{1.2.752.179.100.2.3}	Tjänstens CP och CPS

1.4. Termer och begrepp

Se Appendix A: Termordlista.

2. Organisation och styrning

2.1. Övergripande krav

RA-organisation som vill ansluta sig till Tjänsten, ska vara en aktiv juridisk person samt ha en god ekonomisk ställning. RA-organisationen är ansvarig för att eventuella

underleverantörer som utför uppdrag i Tjänsten för deras räkning, uppfyller kraven i Tillitsramverket som rör deras verksamhet. RA är ansvariga för att utföra granskning av de underleverantörer som de anlitar i Tjänsten.

En RA Officer ska inte ha provisionslön som påverkas av antalet utfärdade eller spärrade en e-legitimationer. En RA Officer får inte vara den som beslutar att en e-legitimation ska utfärdas. Detta ska istället göras av utsedd funktion i organisationen eller av användaren själv.

~~En RA Officer ska ha fast lön och inte provisionslön vilken påverkas av huruvida en e-legitimation ges ut eller ej. En RA Officer får inte initiera utfärdandet av en e-legitimation utan detta ska göras av utsedd funktion i organisationen eller av användaren själv.~~

2.1.1. Regelverk

Regelverket för Tjänsten ägs och förvaltas av PsPT. Regelverket beskrivs i Tjänstens dokumenthierarki.

2.1.2. Förvaltning

Förvaltare av Tjänsten är Pointsharp AB. Varje RA-organisation som ansluter sig för nyttjande av Tjänsten ska teckna avtal med Pointsharp AB.

2.2. Tjänstens dokumenthierarki

Alla regulatoriska och styrande dokument relaterade till Tjänsten ägs och förvaltas av PsPT. Tillitsdeklarationer ägs av de anslutna RA-organisationerna, men ska dokumenteras enligt mall från PsPT. RA-interna dokument ägs och utformas av de anslutna RA-organisationerna.

2.2.1. Tjänstens CP och CPS

Certifikatpolicyn (CP) definierar ramverket för PKI:n (public key infrastructure), och utfärdardeklarationen (CPS: certificate practice statement) anger de procedurer som används i PKI:n.

Tjänstens kombinerade CP och CPS heter *Pointsharp Net iD Svensk E-legitimation Certificate Policy and Certification Practice Statement*.

~~PoSC Net iD SweID Certificate Policy and Certification Practice Statement (hädanefter kallad "Tjänstens CP och CPS")~~

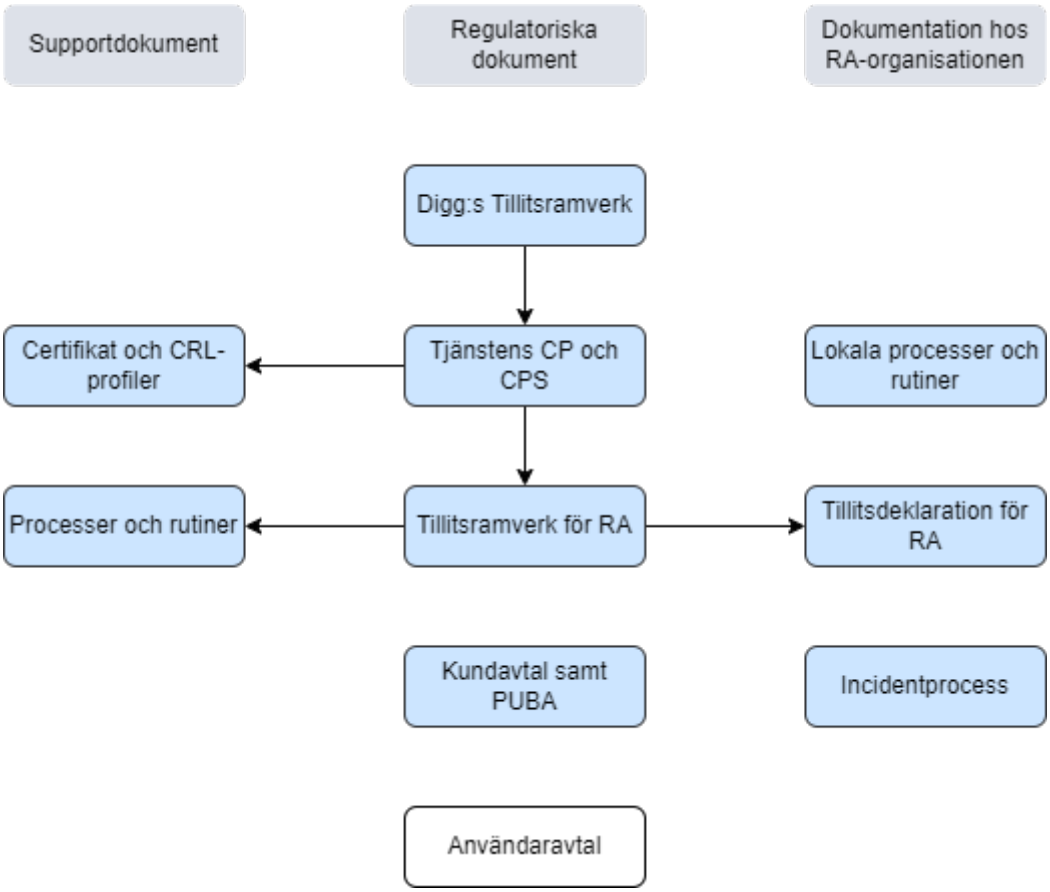
2.2.2. Tillitsramverk för RA

Detta dokument.

2.2.3. Tillitsdeklaration

Alla RA-organisationer som ska ansluta sig till Tjänsten ska lämna in en tillitsdeklaration (Tillitsdeklaration för RA) till Pointsharp samt få den godkänd innan anslutning kan ske. Alla anslutna RA-organisationer ska varje år lämna in en tillitsdeklaration. Tillitsdeklarationen är ett frågeformulär där RA-organisationen gör en

självskattning av hur organisationen uppfyller kraven enligt Tillitsramverk för RA inom sin RA-domän.



1 Tjänstens dokumenthierarki

3. Säkerhet och revision

Personal hos ansluten RA-organisation ska vara tillgänglig och behjälplig med framtagande av information i samband med:

- revision som Pointsharp utför inför anslutning av RA-organisation till Tjänsten samt vid återkommande revisioner som Pointsharp kan komma att genomföra under den tid som RA-organisationen är ansluten till Tjänsten,
- säkerhetsincidenter,
- andra rapporterade fel, avvikelser och brister.

3.1. Revision från Pointsharp

Innan en RA-organisation blir ansluten till Tjänsten görs en revision av Pointsharp utsedd revisor för att säkerställa tillitsdeklarationens efterlevnad.

Ansluten RA-organisation kommer därefter att vara föremål för ~~stickprovsmässig revision från Pointsharp~~ revision från Pointsharp genom riskbaserat urval samt stickprov.
Revisionen kommer att genomföras i enlighet med den vid varje tidpunkt gällande

processen.
Åtgärder av de brister som upptäcks i samband med revisionen ska dokumenteras i en åtgärdsplan som sedan följs upp av RA-organisationen tills dess att åtgärder genomförts.

Vid revision ska RA-organisationen omgående bistå med att ta fram nödvändig information och säkerställa att personal med rätt kompetens finns tillgänglig.

3.2. Informationssäkerhet

Ansluten RA-organisation ska ha ett strukturerat informationssäkerhetsarbete relaterat till sina åtaganden inom Tjänsten som omfattar, men inte är begränsat till:

1. En riskhanteringsprocess som kontinuerligt analyserar hot och sårbarheter i verksamheten relaterat till Tjänsten.
2. Kontinuerligt genomförda och dokumenterade internrevisioner som genomförs och återrapporteras till Pointsharp via årlig Tillitsdeklaration.
3. En incidenthanteringsprocess som beskriver hantering av eventuella incidenter relaterade till Tjänsten.
4. Ett skydd av nyckelbärare mot fysisk skada och otillåten åtkomst.
5. En dokumenterad process för tilldelning av RA-roller i Tjänsteportalen.
6. En upprättad och testad kontinuitetsplan.
7. Arkivering av dokumentation och loggar.

3.2.1. Riskhantering

RA-organisationen ska ha en riskhanteringsprocess som kontinuerligt analyserar hot och sårbarheter i verksamheten relaterat till Tjänsten. Riskhanteringsprocessen ska med hjälp av riskanalyser bedöma sannolikhet för och konsekvens av identifierade risker för användare och RA-organisationen.

Resultatet från riskanalysen ska leda till säkerhetsåtgärder som ska balansera riskerna till acceptabla nivåer. Riskanalys och åtgärdsplan ska dokumenteras och kunna visas vid revision.

3.2.2. Internrevision

Ansluten RA-organisation ska minst var 12:e månad ha genomfört en internrevision av organisationens efterlevnad av Tillitsramverk för RA och den egna gällande tillitsdeklarationen. Under en treårsperiod ska samtliga delar i tillitsramverket ha blivit reviderade. Om internrevisionen delas upp på flera år ska det finnas en revisionsplan som visar vad organisationen planerar att revidera respektive år.

Avvikelser som hittats under internrevision hanteras i en åtgärdsplan som därefter ska genomföras.

Internrevision och åtgärdsplan med dess genomförande ska dokumenteras.

Dokumentationen ska minst omfatta:

- Problem/risk/avvikelse
- Grundorsaksanalys~~Orsaker~~
- Förbättringsförslag

- Slutsats/rekommendation
- Tidpunkt för åtgärden
- Ansvarig för åtgärden
- Mätning av effekt/nytta med förbättringsåtgärd från föregående internrevision.

Genomförda internrevisioner ska kunna redovisas vid revision från Pointsharp.
Internrevision ska ledas av RA Auditor eller oberoende extern revisor/kontrollfunktion.
Med oberoende menas att RA Auditor inte får ha några andra operativa RA-roller relaterat till Tjänsten, exempelvis rollen som RA Central Officer eller RA Local Officer, eller på annat sätt ansvara för eller delta i utfärdande av e-legitimationerna.

3.2.2.1. Återkommande granskningar

Ansluten RA-organisation ska minst en gång i kvatalet genomföra granskningar av sina loggar i Tjänsteportalen, loggar över utlämnade smartkort samt innehav av roller i RA-organisationen.

Avvikelser som hittats under denna granskning ska dokumenteras och åtgärdas enligt RA-organisationens incidenthanteringsprocess.

Granskningen ska minst omfatta:

- Kontrollera att användare som inte längre har en relation till RA-organisationen ej har giltiga e-legitimationer.
- Kontrollera att rolltilldelningar i Tjänsteportalen stämmer överens med beslut och kvittens på tilldelad roll.

3.2.3. Informationssäkerhetsincidenter

Ansluten RA-organisation ska ha en dokumenterad och etablerad process för att hantera informationssäkerhetsincidenter relaterade till Tjänsten.
Processen ska beskriva hur och när rapportering och eskalering till Pointsharp görs.

En incidentrapport ska upprättas och rapporteras till Pointsharp via kundsupportverktyget som tillhandahålls av Tjänsten.
Se Kundavtalet för mer information om incidentklassificering och incidenthantering.

I händelse av en incident ska lämpliga åtgärder vidtas i samråd med Pointsharp för att mitigera effekten och förhindra ytterligare skador samt minimera risken för återupprepning av incident. RA-organisationen ska även genomföra en grundorsaksanalys på den uppkomna incidenten. Perioden för RA-organisationen att genomföra åtgärderna beslutas av Pointsharp och är relaterat till händelsens allvar.

RA-organisationen ska föra en incidentlogg där alla säkerhetsincidenter relaterade till Tjänsten noteras.
Incidentloggen ska innehålla följande information men är inte begränsad till:

- rapportör, utfärdarens namn
- namn, kort beskrivande benämning på händelsen
- referens, unik referens för händelsen
- status, status på händelsen
- kategorisering, kategorisering av händelsen
- tidpunkt, när händelsen inträffade eller den uppskattade tidpunkten för den
- upptäckt, när utfärdaren upptäckte händelsen

- beskrivning, en översiktlig beskrivning av händelsen
- analys, bedömning av händelsens omfattning och konsekvenser samt annan information som kan vara av värde
- grundorsaksanalys (RCA), resultat av genomförd grundorsaksanalys

3.2.4. Fysisk säkerhet

Nyckelbärare ska skyddas fysiskt mot skada och otillåten åtkomst.

Tillträdeskontroll ska tillämpas så att åtkomst till känsliga utrymmen är begränsad till behörig personal. RA Local Officer ska ha tillgång till låsbar förvaring för ännu inte uthämtade nyckelbärare. RA Security Officer och annan utpekad personal ska ha exklusiv tillgång till låsbar förvaring för arkivmaterial.

3.2.5. Administrativ säkerhet

Åtkomst till Tjänsteportalen för RA-roller kräver identifiering med e-legitimation av tillitsnivå 3 (LoA3) samt avtal mellan RA-organisation och Pointsharp.

RA-organisationen tilldelar RA-roller för den egna organisationen och ska ha en dokumenterad process för tilldelning och konfiguration av sådana roller. Processen ska även inkludera beställningsförfarandet av RA-roller, hur RA Central Officer får uppgiften att tilldela roller och förändra rolltillhörigheter i Tjänsteportalen, samt periodisk granskning av tilldelade roller.

3.2.6. Kontinuitetsplan

RA-organisationen ska ha en kontinuitetsplan med etablerade och testade rutiner för verksamhetskritiska funktioner som rör utfärdande och användande av e-legitimationer som utfärdats i Tjänsten.
Rutinerna ska innefatta planer för hantering av avbrott i de delar av Tjänsten som hanterar spärrstatus (OCSP och certifikatspärrlistor (CRL)) och utfärdande av e-legitimationer.
Varje RA-organisation är ansvarig för möjligheten att komma åt nyckelkomponenter såsom OCSP och certifikatspärrlistor.

Avbrott kan ha sitt ursprung hos RA-organisationen, i extern infrastruktur eller i Tjänsten.
En kontinuitetsplan bör även innehålla åtgärder i samband med externt genererade, allvarliga informationssäkerhets- eller tillgänglighetsincidenter som gör att Tjänsten inte är tillgänglig, till exempel översvämning, brand eller andra händelser i kategorin "force majeure".

3.2.7. Spårbarhet, gallring och bevarande av information

Ansluten RA-organisation ska bevara den information som nämns i detta stycke.

För att bistå RA-organisationen finns inom Tjänsten i flera fall elektroniska stöd framtagna och finns dessa ska de användas.

Information som ska bevaras:

- godkänd tillitsdeklaration;

- dokumentation från interna revisioner samt tillhörande åtgärdsplaner;
- incidentloggar för incidenter som är relaterade till Tjänsten samt tillhörande incidentrapporter med information om genomförda åtgärder;
- förteckning över innehavare av RA-roller ~~samt deras ansvarsområden~~, inklusive historik; och
- avtal med eventuella underleverantörer relaterat till genomförande av Tjänsten.
- ~~användarnas kvittenser avseende mottagna e-legitimationer samt godkännande av Användaravtalet (hanteras automatiskt av Tjänsten).~~

Tiden för bevarande ska inte understiga 5 (fem) år från skapandedatum och material ska kunna tas fram i läsbar form under hela denna tid, såvida inte krav på gallring påkallats av integritetsskäl och har stöd i lag eller annan författning. Tiden för bevarande (minst 5 år) gäller även om avtalsförhållanden med Pointsharp har avslutats.

4. RA-organisationen

Varje ansluten RA-organisation ska utse en RA Security Officer, och en RA Auditor samt upprätta en organisation för utfärdande, support och spärr av e-legitimationer inom RA-domänen. Förändringar av RA Security Officer och RA Auditor som ingår i RA-domänen ska skyndsamt meddelas till Pointsharp.

Varje person som utses till en roll i RA-organisationen ska ha uppvisat sig lämplig för respektive roll. Alla innehavare av en roll i RA-organisationen ska ha tillräckligt med tid avsatt för att klara sina uppdrag.

Då RA-organisationen ansluts till Tjänsten så ingår en obligatorisk utbildning av de första personerna som utsetts till RA Officer inom RA-domänen. Utbildning av övriga som ska ha en roll i RA-organisationen är organisationen själv ansvarig för.

RA-organisationen är ansvarig för att utbilda sina rollinnehavare i RA-organisationen kring GDPR. Till exempel gällande rutiner för behandling av persondata. Pointsharp agerar som personuppgiftsbiträde till organisationen.

4.1. RA Security Officer

4.1.1. Krav på RA Security Officer

En RA Security Officer får inte ha ett annat uppdrag eller befattning inom RA-organisationen som kan bedömas stå i konflikt med arbetet som RA Security Officer.

Om RA Security Officer lämnar rollen ska RA-organisationen skyndsamt utse ny RA Security Officer som ska kommuniceras till Pointsharp. Under tiden som RA Security Officer saknas övertar RA-organisationens ordinarie informationssäkerhetsansvarige temporärt de skyldigheter som normalt åligger RA Security Officer.

En RA Security Officer ska ha de kvalifikationer och den utbildning som krävs för att på ett korrekt och säkert sätt utföra de arbetsuppgifter som följer av rollen.

4.1.2. Bakgrundskontroll av RA Security Officer

Det ska utföras en bakgrundskontroll på personen som ska ha rollen RA Security Officer enligt nedanstående lista. Syftet med bakgrundskontrollen är att förvissa sig om att personen kan anses vara pålitlig och lämplig för rollen.

Alla RA-organisationer ska ha en process för bakgrundskontroll av RA Security Officer med lämplighetsprövning.

Bakgrundskontrollen ska inkludera men är inte begränsad till:

- identifiering vid ett fysiskt möte,
- kontroll av nuvarande anställning,
- lämplighetsbedömning för rollen,
- genomgången relevant utbildning,
- finansiell riskbedömning, och
- kontroll mot belastningsregistret eller en granskning som motsvarar detta.

4.1.3. RA Security Officers skyldigheter

RA Security Officer ska:

- ha det övergripande ansvaret för att upprätta en RA-domän med tillräckliga personalresurser för att uppfylla organisationens åtaganden;
- ha kunskap om Tillitsramverk för RA och andra regulatoriska och styrande dokument relaterade till Tjänsten;
- ansvara för att RA-domänen följer Tjänstens regler och rutiner om ansökan, beställning, uthämtning och spärr av e-legitimationer till personer;
- ansvara för processen för registrering av användare från betrott register;
- ansvara för att lämna in tillitsdeklarationen till Pointsharp;
- ansvara för att bakgrundskontroller utförs på alla RA Auditor samt RA Officer inom RA-domänen och att delar av bakgrundskontrollerna återupprepas med en bestämd periodicitet;
- ansvara för att RA Auditor samt RA Officer har adekvat kunskap och kompetens för att upprätthålla organisationens åtagande över tid;
- ansvara för att utvärdera RA-domänens efterlevnad av utfärdandeprocesser för e-legitimationer;
- ansvara för hantering av roller inom organisationen för åtkomst till Tjänsteportalen;
- om RA Auditor lämnar rollen skyndsamt tillse att en ny RA Auditor utses samt under den tid som RA Auditor saknas temporärt överta de skyldigheter som normalt åligger RA Auditor;
- ansvara för att informationssäkerhetsincidenter och brister i Tjänsten rapporteras till Pointsharp, samt där tillämpligt åtgärdas;
- bidra till upprättandet och förvaltningen av de delar i RA-domänens kontinuitetsplan som rör Tjänsten, samt testa och dokumentera dess rutiner; samt;
- genomföra riskanalyser inom RA-domänen.

4.2. RA Auditor och RA Officer

Tjänsteportalen har ett antal definierade roller för att utfärdande av e-legitimationer samt hantering av e-legitimationer ska ske på ett säkert sätt. Termen RA Officer avser rollerna RA Central Officer samt RA Local Officer, men kan även inkludera andra RA-roller.

RA Auditor är ansvarig för att utvärdera samt utföra internrevision på RA-domänens efterlevnad av processer för hantering av användare och e-legitimationer.

4.2.1. Krav på RA Auditor samt RA Officer

En RA Auditor samt RA Officer får inte ha annat uppdrag som kan bedömas stå i konflikt med arbetet inom RA-domänen. Rollen RA Auditor får inte kombineras med en annan operativ roll inom RA-domänen.

RA Auditor samt alla RA Officer ska ha adekvat kunskap och förmåga. RA Security Officer ska tillse att deras kunskap upprätthålls så att de kan fullgöra sina arbetsuppgifter på ett sådant sätt att tilliten till Tjänsten säkras. Uppföljning av utbildning av RA Officer ska genomföras så att nödvändig kunskap upprätthålls inom RA-organisationen.

Personal från Pointsharp utbildar RA-domänens första RA Officers vid anslutning av RA-organisationen till Tjänsten. Därefter är RA-organisationen själv ansvarig för att utbilda sina RA Officers.

4.2.2. Bakgrundskontroll av RA Auditor samt RA Officer

Innan en person tilldelas en roll inom RA-organisationen ska RA Security Officer, eller en annan person denna delegerat utförandet till, ha genomfört en bakgrundskontroll. Syftet med bakgrundskontrollen är att förvissa sig om att personen kan anses vara pålitlig och har de kvalifikationer och den utbildning som krävs för att på ett tillfredsställande, korrekt och säkert sätt utföra de arbetsuppgifter som följer av rollen.

RA-organisationer ska upprätta en egen process för bakgrundskontroll av RA Auditor och RA Officers med lämplighetsprövning.

Bakgrundskontrollen ska inkludera men är inte begränsad till:

- identifiering vid ett fysiskt möte,
- kontroll av nuvarande anställning,
- lämplighetsbedömning för rollen,
- genomförd relevant utbildning,
- en finansiell riskbedömning, och
- ~~kontroll mot brottregistret.~~
- kontroll mot belastningsregistret eller en granskning som motsvarar detta.

4.2.3. RA Auditors skyldigheter

En RA Auditor ansvarar för att utvärdera RA-organisationens efterlevnad av utfärdandeprocesser för e-legitimationer. I detta ingår ansvar för att internrevisioner genomförs samt tillsyn av RA Security Officer arbete.

4.2.4. RA Officers skyldigheter

En RA Officer medverkar i administrationen av användare, e-legitimationer och nyckelbärare inom RA-organisationen.

~~Termen RA Officer avser åtminstone rollerna RA Central Officer samt RA Local Officer, men kan även inkludera andra RA-roller. Tjänsteportalen har ett antal definierade roller för att utfärdande av e-legitimationer samt hantering av e-legitimationer ska ske på ett säkert sätt. Dessa roller finns beskrivna på Tjänstens webbsida, se https://www.pointsharpsecurecloud.com.~~

RA Officers arbetsuppgifter inkluderar men är inte begränsade till att:

- hantera användare i Tjänsteportalen,
- tilldela privilegier till alla RA roller i Tjänsteportalen,
- identifiera användare i samband med beställning och uthämtning av e-legitimation,
- utfärda ordinarie och tillfälliga e-legitimationer,
- genomföra beställning av smartkort från kortleverantör,
- spärra e-legitimation och nyckelbärare,
- låsa upp spärrade nyckelbärare, och
- utföra batchbeställning av smartkort.

4.3. Övriga roller

Tjänsten möjliggör tillsättandet av kompletterande roller i RA-organisationen samt Tjänsteportalen. Dessa roller ingår ej i utfärdandeprocesserna av e-legitimationer.

Följande övriga roller är tillgängliga i Tjänsteportalen:

- RA Revocation Officer
- RA Helpdesk Officer
- RA Report Officer

4.3.1. Krav på övriga roller

Innehavare av ovan nämnda roller ska ha adekvat kunskap och förmåga. RA Security Officer ska tillse att deras kunskap upprätthålls så att de kan fullgöra sina arbetsuppgifter på ett sådant sätt att tilliten till Tjänsten säkras. Uppföljning av utbildning av ovan nämnda roller ska genomföras så att nödvändig kunskap upprätthålls inom RA-organisationen.

4.3.2. Bakgrundskontroll av övriga roller

Inga specifika krav om bakgrundskontroll föreligger.

4.3.3. Övriga rollers skyldigheter

RA Revocation Officer kan spärra e-legitimationer och nyckelbärare för användare i RA-organisationen.

RA Helpdesk Officer kan se befintliga användare, nyckelbärare och e-legitimationer i Tjänsteportalen för att ge support till användarna. RA Helpdesk Officer kan inte ändra någon information om användare, nyckelbärare och e-legitimationer.

RA Report Officer kan skapa, läsa och exportera rapporter om användare, nyckelbärare och e-legitimationer som hanteras i Tjänsteportalen.

5. Avveckling av RA-domän

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

Den anslutna organisationen ska:

1. informera alla användare och parter som organisationen har avtal eller överenskommelser med,
2. avsluta avtal och behörigheter för RA-domänen,
3. spärra alla e-legitimationer som är utfärdade inom RA-domänen, samt
4. tillse att alla arkiv och loggar bevaras enligt gällande anvisningar i stycke 3.2.7 Spårbarhet, gallring och bevarande av information.

6. E-legitimationer

Detta stycke berör processer för hantering av e-legitimationer och är nära relaterat till hanteringsflöden för e-legitimationer som tillhandahålls i Tjänsteportalen.

6.1. Användningsområden

E-legitimationer utfärdade inom Tjänsten är personliga och ska användas för att identifiera fysiska personer verksamma i, eller på annat sätt har en relation till, RA-organisationer anslutna till Tjänsten vid legitimering och underskrift.

6.2. Villkor

E-legitimationer får endast lämnas ut efter att användaren har tagit del av och godkänt användaravtalet med tillhörande villkor. Användaravtalets villkor ska göras tillgängliga för användaren innan besöket för uthämtning av e-legitimationen så att användaren har tid på sig att läsa igenom villkoren.

Användaren ska informeras om att förvara koder och nyckelbärare så att obehöriga inte får tillgång till dessa samt att koder och nyckelbärare ska förvaras fysiskt åtskilda.

6.3. Giltighetstid för e-legitimation

E-legitimation kommer beroende på nyckelbärare som används att ha de maximala giltighetstiderna enligt tabellen nedan.

Nyckelbärare	Giltighetstid (maximal)
Ordinarie smartkort eller annan hårdvarubärare	5 år
Tillfälligt smartkort eller annan hårdvarubärare	1 år

Nyckelbärare	Giltighetstid (maximal)
Mobil App	3 år

6.4. Ansökan om e-legitimation

Ansökan om e-legitimation är en begäran om att erhålla en svensk e-legitimation utfärdad av Tjänsten.

6.4.1. Förutsättningar

E-legitimationer kan utfärdas:

- till anställda inom RA-organisationen eller till andra personer med en relation till RA-organisationen, till exempel konsulter.
- till personer som efter kontroll mot betrott internt register hos RA-organisationen samt Skatteverkets SPAR-tjänst har registrerats i Tjänsteportalen.
- på begäran av en person behörig att göra ansökningar i RA-domänen.
- till personer som har fyllt 16 år.
- efter att ansökan har kunnat knytas till giltigt personnummer eller styrkt samordningsnummer.

Ansökan måste innehålla entydiga uppgifter som möjliggör att en RA Officer kan hitta personen som ansökan gäller samt om nödvändigt registrera personen i Tjänsteportalen.

RA Officer ska avslå ansökan om förutsättningarna inte är uppfyllda. RA Officer ska meddela avslag eller godkännande till personen som lämnade in ansökan.

6.5. Beställning av e-legitimation

Beställningen av e-legitimationen omfattar delen av utfärdandeprocessen av e-legitimation, inklusive eventuell hårdvarubärare, för en beviljad ansökan fram till att den kan hämtas ut.

6.5.1. Kontroll av personuppgifter

RA Officer kontrollerar att uppgifterna knutna till ansökan är fullständiga samt stämmer överens med de användaruppgifter som finns registrerade om användaren i Tjänsteportalen.

~~*6.5.2. Identifiering vid beställning*~~

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

~~Nyckelbärare~~	~~Identifieringsprocedur~~
~~Ordinarie personaliserat smartkort från korttillverkare~~	~~Identifiering ska ske på plats genom ett personligt möte med RA Officer enligt av RA fastställda rutiner.~~ ~~Identifiering sker med någon av följande svenska identitetshandlingar:~~ • ~~Körkort~~ • ~~Nationellt id-kort~~ • ~~Pass~~ • ~~SIS-märkt id-kort~~ • ~~Skatteverkets id-kort~~

~~Övriga beställningar av e-legitimationer kräver inte att användaren identifierar sig med en identitetshandling. Användaren identifieras alltid i samband med uthämtning av e-legitimation.~~

6.6. Uthämtning av e-legitimation

6.6.1. Identifiering vid uthämtning

All identifiering ska ske enligt av PsPT fastställda rutiner.

Nyckelbärare	Identifieringsprocedur
Ordinarie personaliserat smartkort från korttillverkare	Identifiering ska ske på plats genom ett personligt möte med en RA Local Officer ~~enligt av RA fastställda rutiner~~. Personer med svenskt personnummer ska identifiera sig med någon av följande svenska identitetshandlingar: ~~Identifiering sker med någon av följande svenska identitetshandlingar:~~ • Körkort • Nationellt id-kort • Pass • SIS-märkt id-kort • Skatteverkets id-kort Personer med styrkt samordningsnummer ska identifiera sig med följande svenska identitetshandling: • Skatteverkets id-kort
Ordinarie smartkort eller annan hårdvarubärare	
Tillfälligt smartkort eller annan hårdvarubärare	
Mobil app	
Mobil app (id-växling)	Vid utfärdande av e-legitimation till mobil applikation (id-växling) sker identifiering mot Tjänsteportalen på distans med en svensk e-legitimation av LoA3 eller LoA4 och som är godkänd av Digg och Pointsharp.

6.6.2. Uthämtning av e-legitimation ~~vid personligt besök~~

Uthämtning av e-legitimationen sker efter identifiering vid personligt möte med RA Officer enligt tidigare beskrivning i stycke 6.6.1 Identifiering vid uthämtning.

Vid uthämtning av e-legitimationen väljer användaren sina egna PIN-koder och signerar elektroniskt kvittensen för mottagen e-legitimation och godkännandet av Användaravtalet. Inmatning av PIN-koder ska ske på ett sätt skyddat från insyn av andra än användaren själv.

Vid uthämntning av personaliserat smartkort ska RA-officer kontrollera namnet på kortet mot personens identitetshandling.

6.7. Spärr av e-legitimation

Spärrbegäran kan komma från användaren, verksamheten eller utfärdande organisation. Spärrbegäran ska skyndsamt verkställas av auktoriserad personal inom RA-domänen.

Spärr kan utföras av användaren eller behörig RA Officer.

Spärr ska göras om något av följande har inträffat:

- Förhållanden som kan påverka certifikatsinnehållet har ändrats, t.ex. namnbyte.
- Någon uppgift i e-legitimationen är eller misstänks vara felaktig.
- Användaren har förlorat nyckelbäraren.
- Koderna är, eller misstänks vara, röjda.
- Vid otillåten användning eller misstanke om sådan.
- När nyckelbäraren återlämnas.
- När e-legitimationen inte längre behövs.
- När e-legitimationen har använts i strid med de regler som anges i Användaravtalet.
- När användaren inte längre har någon relation till utfärdande organisation.

7. Appendix A: Termordlista

Term	Synonym	Definition	Anmärkning	Avrådda termer
AIA		plats där utfärdarcertifikat kan hämtas för att verifiera certifikatskedjan	en-US: authority information access	
ansökan		begäran om att erhålla en svensk e-legitimation utfärdad av Tjänsten		
autentisering		att verifiera identiteten på en användare, enhet eller en del av ett datorsystem	Autentisering sker ofta innan åtkomst beviljas till resurserna i ett system. Det kan även användas för att styrka integriteten i specifik information. Autentisering av meddelande involverar fastställande av dess källa och verifiering att det inte har modifierats eller ersatts under överföringen.	
autentiseringsmetod		säkerhetsmetod som kontrollerar identiteten på en användare, klient eller server	T.ex. • namn och lösenord • certifikat • engångslösenord	
beställning		delen av utfärdandeprocessen av e-legitimation för en beviljad ansökan fram till att den kan hämtas ut		

Term	Synonym	Definition	Anmärkning	Avrådda termer
certifikat		(i samband med e-legitimationer) elektroniskt intyg som innehåller uppgifter som möjliggör identifiering av e-legitimationens innehavare vid legitimering, underskrift eller bådadera	Det finns bland annat certifikat som bekräftar innehavarens identitet vid legitimering och certifikat som bekräftar innehavarens identitet vid underskrift. E-legitimationernas certifikat innehåller även andra uppgifter, såsom uppgift om certifikatutfärdare (CA), giltighet och eventuell organisationstillhörighet. Innehavaren kan vara en fysisk person, en organisationer eller en maskin. **Anmärkning språkbruk:** Använd inte termen e-legitimation istället för *certifikat* när det är väsentligt att det framgår att det är certifikatet som avses.	e-legitimation

Term	Synonym	Definition	Anmärkning	Avrådda termer
certifikatutfärdare	CA, utfärdare	organisation eller organisatorisk enhet som har till uppgift att skapa, tillhandahålla och spärra certifikat	en-US: certificate authority En certifikatutfärdare kan utfärda certifikat antingen till en sluten grupp av användare (till exempel anställda i en organisation) eller till allmänheten (till exempel för nyttjande av tjänster). Vissa certifikatutfärdare utfärdar också certifikat till andra certifikatutfärdare så att dessa i sin tur får rätt att utfärda certifikat. Certifikatutfärdaren har också till uppgift att hålla och sprida spärrlistor. Certifikatutfärdaren går i god för att informationen i certifikatet är korrekt. **Anmärkning språkbruk:** Kortformen *utfärdare* bör endast användas när det inte finns risk för missförstånd. Är det oklart vilken sorts utfärdare som avses, bör den rekommenderade termen *certifikatutfärdare* användas. Använd *CA* (som är en förkortning av det engelska *certification authority*) endast i rent tekniska sammanhang.	

Term	Synonym	Definition	Anmärkning	Avrådda termer
CP	certifikatpolicy	dokument som redogör för under vilka förhållanden ett certifikat är utfärdat av en CA	en-US: certificate policy	
CPS	utfärdardeklaration	dokument i vilket en CA beskriver de rutiner som tillämpas vid utfärdande av certifikat	en-US: certification practice statement	

Term	Synonym	Definition	Anmärkning	Avrådda termer
e-legitimation	elektronisk legitimation, elektronisk identitetshandling, eID och e-id	identitetshandling i elektronisk form, som vid elektronisk kommunikation används för legitimering, underskrift eller bådadera	En e-legitimation innehåller flera delar, varav certifikaten (tillsammans med s.k. nycklar) utgöt en förutsättning för legitimering och underskrift. E-legitimationen kan till exempel lagras på ett kort eller i en dator. **Anmärkning språkbruk:** Eftersom ett och samma kort ibland kan innehålla flera e-legitimationer, bör man undvika att kalla själva kortet för e-legitimation när man vill vara precis. För kortet förekommer istället benämningar som e-legitimationskort och e-id-kort. Observera att termen *e-id* inte ska utläsas *elektronisk identitet*. Jämför identitet.	e-ID och eid

Term	Synonym	Definition	Anmärkning	Avrådda termer
			Observera: Vi har dock valt att använda termen eID trots TNCs avrådan. Dels då den är och har varit vanligt förekommande sedan tidigt och fortfarande är det av flera av våra konkurrenter (Inera/SITHS, Freja eID [*sic!*] m.fl.). Dessutom ser den ganska bra och tydlig ut i text. Både ur ett tekniskt informations- och marknadsmässigt perspektiv.	
elektronisk signatur		data i elektronisk form som är fogade till eller logiskt knutna till andra elektroniska data och som används för att kontrollera att innehållet härrör från den som framstår som utställare och att det inte har förvanskats		
HSM		skyddar nycklar till CA i en extern hårdvara	en-US: hardware security module	
hårdvarubärare		nyckelbärare i form av smartkort eller USB-minne, t.ex. YubiKey, som kan lagra och skydda användares digitala certifikat och privata nycklar		

Term	Synonym	Definition	Anmärkning	Avrådda termer
identitet		ställning såsom varande viss, entydigt bestämd fysisk eller juridisk person eller visst entydigt bestämt objekt	I uttryck som *person-id* händer det att förkortningen *id* utläses som *identitet*. I sådana uttryck bör dock *id* utläsas som *identitetsbeteckning*. Undvik uttrycket *elektronisk identitet*. Det är ett oklart uttryck, som kan ge sken av att man skulle ha en annan identitet "på nätet" än annars.	

Term	Synonym	Definition	Anmärkning	Avrådda termer
identifiering	verifiering av identitet, autentisering	(i samband med legitimering) process varigenom en persons eller ett objekts uttryckta identitet bekräftas	Identiteten uttrycks genom någon typ av representation, t.ex. personnummer eller annan identitetsbeteckning. **Anmärkning språkbruk:** Termen *autentisering* används synonymt med *identifiering* i tekniska sammanhang, men bör undvikas i dokument som riktar sig till allmänheten. Uttrycket *verifiering av identitet* kan också uppfattas som alltför tekniskt i texter riktade till allmänheten. Notera att verbet som hör ihop med är *identifiera* och inte *identifiera sig*. Mer tekniska synonymer till *identifiera* är *verifiera identitet* och *autentisera*.	

Term	Synonym	Definition	Anmärkning	Avrådda termer
identitetshandling	legitimationshandling, legitimation	handling som innehåller uppgifter som är tillräckliga för en direkt eller indirekt identifiering av innehavaren	Vid en indirekt identifiering innehåller identitetshandlingen i sig inte tillräckliga uppgifter för identifiering, utan uppgifterna utgörs t.ex. av en referens (ett nummer eller dylikt) till ett register där de "verkliga" uppgifterna finns. Innehavaren av en identitetshandling kan vara en fysisk eller en juridisk person. Identitetshandlingar kan vara fysiska (identitetskort, pass) eller elektroniska (e-legitimation).	
legitimera sig		uttrycka sin identitet i syfte att utföra en eller flera aktiviteter	Identiteten uttrycks genom någon typ av representation, t.ex. personnummer eller annan identitetsbeteckning.	identifiera sig

Term	Synonym	Definition	Anmärkning	Avrådda termer
legitimering		process varigenom person eller objekt anger sin identitet i syfte att utföra en eller flera aktiviteter	Den angivna identitets måste sedan i nästa led kontrolleras och bekräftas av motparten, se identifiering. Samma motpart avgör också (efter identifieringen) vilka aktiviteter som personen eller objektet har rätt att utföra (i e-legitimationssammanhang till exempel rätt att ta del av information eller elektroniskt skriva under dokument). Detta är dock en egen process (ofta benämnd *behörighetskontroll*) och ingår inte i själva identifieringen.	

Term	Synonym	Definition	Anmärkning	Avrådda termer
momsregistreringsnummer		unikt serienummer som i EU tilldelas alla som registreras för redovisning av moms av medlemsstatens skattemyndighet	en-US: VAT registration number Ett svenskt momsregistreringsnummer är baserat på ett 10-siffrigt personnummer eller organisationsnummer. Det inleds med den svenska landskoden SE och avslutas alltid med 01. Eftersom varken bindestreck eller mellanrum skall förekomma är svenska momsregistreringsnummer alltid 14 tecken: **SE**999999999**01**, där de tio niorna ersätts med personnummer eller organisationsnummer.	
nyckel	krypteringsnyckel	varierbar information som styr en krypteringsalgoritms omvandling av klartext till kryptotext		
nyckelbärare		enhet som kan lagra och skydda användares digitala certifikat och privata nycklar	Enheter kan vara t.ex. smartkort, YubiKey, mobilapp eller en så kallad trusted platform module (TPM).	
OCSP		protokoll till vilket man kan ställa frågan om ett visst certifikat är giltigt	en-US: online certificate status protocol	

Term	Synonym	Definition	Anmärkning	Avrådda termer
PIN-kod		lösenord oftast bestående enbart av siffror	en-US: personal identification number En PIN-kod används när den privata nyckeln hörande till certifikatet används för identifiering eller signering, men också i vissa fall kryptering. Om användaren har två certifikat, ett för identifiering och kryptering och ett för signering så finns två PIN-koder, en identifierings PIN-kod och en signerings PIN-kod.	

Term	Synonym	Definition	Anmärkning	Avrådda termer
PKI		infrastruktur för kryptering med publik nyckel	en-US: public key infrastructure En uppsättning roller, policyer och procedurer som behövs för att skapa, hantera, distribuera, använda, lagra och återkalla digitala certifikat och hantera kryptering med publik nyckel. PKI är en asymmetrisk krypteringsteknik där ett nyckelpar genereras; en privat och en publik nyckel. Med PKI kan användare på ett säkert sätt utbyta data över ett i grunden osäkert publikt nät som Internet. Utan risk för obehörig insyn kan man utväxla information och besvara frågor som enbart berör en enskild person.	
privat nyckel		hemlig nyckel i ett asymmetriskt kryptosystem som kan användas vid elektronisk identifiering, elektronisk signering och kryptering		
publik nyckel		nyckel i ett asymmetriskt nyckelpar som kan göras allmänt känd i till exempel en katalog för att användas vid elektronisk identifiering, elektronisk signering och kryptering		

Term	Synonym	Definition	Anmärkning	Avrådda termer
PUK-kod		kod för att låsa upp ett kort som har spärrats	en-US: personal unblocking key	
RA		enhet i ett nätverk som verifierar användarnas förfrågningar om digitala certifikat och säger till certifikatutfärdaren att utfärda det	en-US: registration authority	
RSA		asymmetrisk krypteringsalgoritm	uppkallad efter upphovsmännen Rivest, Shamir och Adleman	
signering		skapande av elektronisk signatur för att säkerställa att elektroniskt överförd information inte har förändrats, dels för att säkerställa vem som är informationens avsändare och slutligen för att förhindra att avsändaren sedan förnekar informationen		
smartkort	chipkort, integrated circuit card (ICC)	kort med inbyggd mikroprocessor		
spärra		radera certifikat på nyckelbärare	Kan ske om en användare förlorar sin nyckelbärare, avslutar sin relation med sin RA, eller om någon käslig information rörande e-legitimationen misstänks vara röjd.	revokera
spärrlista	CRL	spärrlista över certifikat som inte längre är giltiga	en-US: certificate revocation list	revokeringslista

Term	Synonym	Definition	Anmärkning	Avrådda termer
verifiering		kontroll av certifikat, giltighet m.m.	Vid till exempel elektronisk identifiering eller elektronisk signering	

Website
https://www.pointsharp.com

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

Classification:	Public
Publ. No.:	PSC-Rd22-04
Document version:	2.1
Document status:	Final
OID:	1.2.752.179.100.1.3
Published:	13 Sep 2024