POINTSHARP

Tillitsramverk för RA

Pointsharp Net iD svensk e-legitimation

Classification:	Public
Publication No.:	PSC-Rd22-04
Document version:	2.2
Document status:	Final
Date:	19 Nov 2024

Table of Contents

Revisionshistorik

Version	Datum	Författare	Beskrivning
2.2	19 Nov 2024	PsPT	Förtydligat, tagit bort eller lagt till i stycke: • 1.4. Termer och begrepp • 3.2.7. Spårbarhet, gallring och bevarande av information • 4.2.2. Bakgrundskontroll av RA Auditor samt RA Officer • 6.5.1. Kontroll av personuppgifter • 6.6.1. Identifiering vid uthämtning • 6.6.2. Uthämtning av e-legitimation Borttagna stycken: • 7. Appendix A: Termordlista
2.1	13 Sep 2024	PsPT	Förtydligat eller lagt till 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.

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. 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
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 termordlista på Tjänstens hemsida.

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-organisationen är ansvarig 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.

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*.

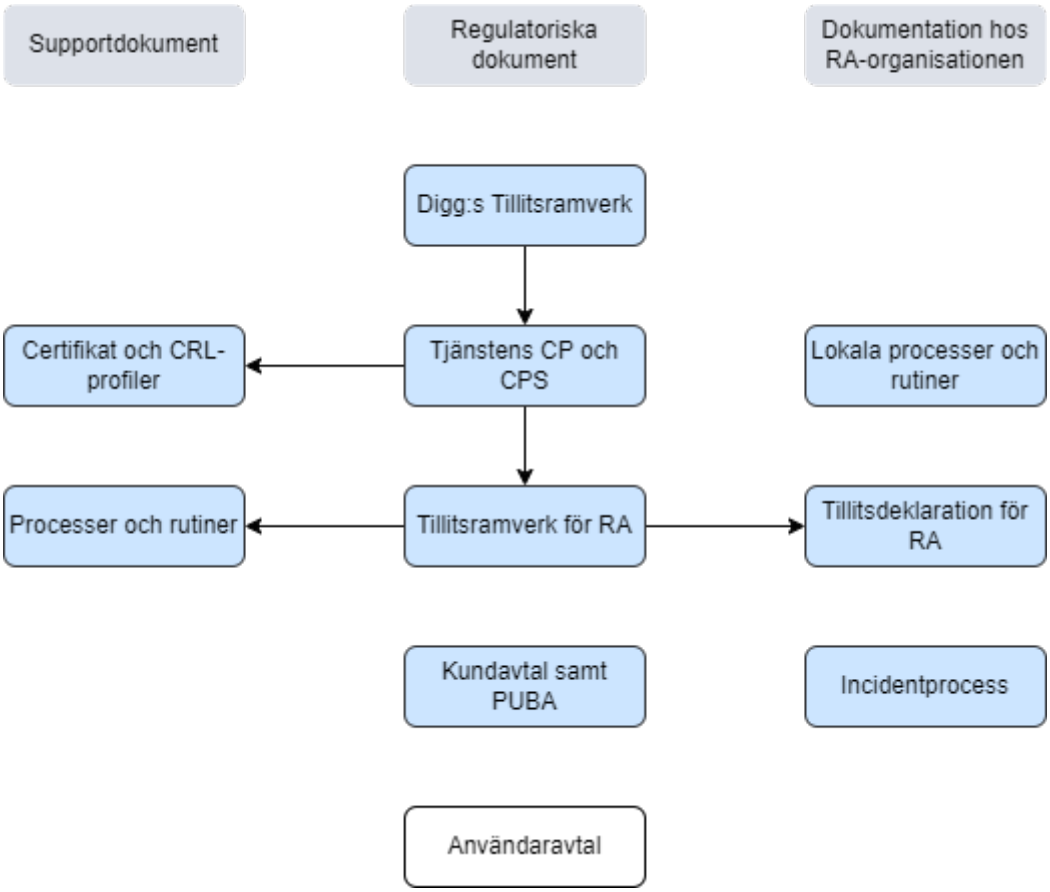
2.2.2. Tillitsramverk för RA

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 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 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
- 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 kvartalet 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 implementation 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

För att bistå RA-organisationen finns inom Tjänsten olika stöd framtagna i Tjänsteportalen såsom loggar, kontroll av id-nummer, signerade användarvillkor, handläggarkvittenser med mera. Och finns dessa ska de användas.

Följande information ska bevaras men är inte begränsad till:

- 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, inklusive historik; och
- avtal med eventuella underleverantörer relaterat till genomförande 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 beslastningregistret 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 deras arbete 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 beslastningregistret 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.

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
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 samt betrott register.

6.6. Uthämtning av e-legitimation

6.6.1. Identifiering vid uthämtning

All identifiering ska ske enligt av PsPT ~~fastställda~~ godkända rutiner. Användarens identitetshandling ska också kontrolleras mot personuppgifterna i Tjänsteportalen.

Nyckelbärare	Identifieringsprocedur
Ordinarie personaliserat smartkort från korttillverkare	Identifiering ska ske på plats genom ett personligt möte med en RA Local Officer. Personer med svenskt personnummer ska identifiera sig 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	

Nyckelbärare	Identifieringsprocedur
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

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

Hanteringen av uthämtning av e-legitimationer ska ske på en plats fri från yttre störningar.

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 uthämtning av personaliserat smartkort ska RA-officer kontrollera namnet på smartkortet 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~~

POINTSHARP

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:	2.2
Document status:	Final
OID:	1.2.752.179.100.1.3
Published:	19 Nov 2024