



Tillitsramverk för RA

PoSC Net iD SweID

Classification:	Public
Publication No.:	PSC-Rd22-04
Document version:	2.0
Document status:	Final
Date:	11 Sep 2023

Table of Contents

1	Inledning	1
1.1	Bakgrund och syfte.....	1
1.2	Målgrupp.....	1
1.3	Identifiering.....	1
1.4	Termer och begrepp.....	2
2	Organisation och styrning	2
2.1	Övergripande krav	2
2.1.1	Regelverk	2
2.1.2	Förvaltning	2
2.2	Tjänstens övergripande dokumenthierarki.....	2
3	Säkerhet och revision.....	3
3.1	Revision från Pointsharp	3
3.2	Informationssäkerhet.....	4
3.2.1	Riskhantering.....	4
3.2.2	Internrevision	4
3.2.3	Informationssäkerhetsincidenter.....	5
3.2.4	Fysisk säkerhet	5
3.2.5	Administrativ säkerhet	5
3.2.6	Kontinuitetsplan	6
3.2.7	Spårbarhet, gallring och bevarande av information.....	6
4	RA-organisationen.....	6
4.1	RA Security Officer	7
4.1.1	Krav på RA Security Officer.....	7
4.1.2	Bakgrundskontroll av RA Security Officer	7
4.1.3	RA Security Officers skyldigheter	7
4.2	RA Auditor och RA Officer	8
4.2.1	Krav på RA Auditor och RA Officer	8
4.2.2	Bakgrundskontroll av RA Auditor och RA Officer.....	8
4.2.3	RA Auditors skyldigheter	9
4.2.4	RA Officers skyldigheter	9
5	Avveckling av RA-domän	9

6	E-legitimationer	10
6.1	Användningsområden.....	10
6.2	Villkor	10
6.3	Giltighetstid för e-legitimation	10
6.4	Ansökan om e-legitimation	10
6.4.1	Förutsättningar	10
6.5	Beställning av e-legitimation	11
6.5.1	Kontroll av personuppgifter.....	11
6.5.2	Identifiering vid beställning.....	11
6.6	Uthämtning av e-legitimation	11
6.6.1	Identifiering vid uthämtning.....	11
6.6.2	Uthämtning av e-legitimation vid personligt besök	12
6.7	Spärr av e-legitimation.....	12
7	Appendix A: Termordlista	13

1 Inledning

1.1 Bakgrund och syfte

PoSC Net iD SweID (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, PoSC Net iD SweID Tillitsramverk för RA (hädanefter kallad "Tillitsramverk för RA"), beskriver det tillitsramverk för Tjänsten som alla anslutna RA-organisationer skall uppfylla och är baserat på valda delar av DIGGs 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 skall ansluta sig till Tjänsten skall lämna in en tillitsdeklaration till Pointsharp och efter anslutning skall ny tillitsdeklaration lämnas in var 12:e månad. Tillitsdeklarationens frågor som skall besvaras är baserat på detta 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. Med tillitsnivå menas graden av säkerhet och tillförlitlighet. Ju 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 skall uppfyllas. LoA3 är den näst högsta nivån i standarden ISO/IEC 29115, vilken också beskrivs i DIGG:s Tillitsramverk för Svensk e-legitimation.

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

Namn	Objektidentifierare (OID)	Beskrivning
PoSC Net iD SweID 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, skall 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 utföra granskning av de underleverantörer som de anlitar i Tjänsten.

En RA Officer skall 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 skall 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 samlade dokumentstruktur. Varje RA-organisation som ansluter sig skall lämna in en tillitsdeklaration, en självskattning av organisationens överensstämmelse med Tillitsramverket och Tjänstens CP och CPS inom sin RA-domän.

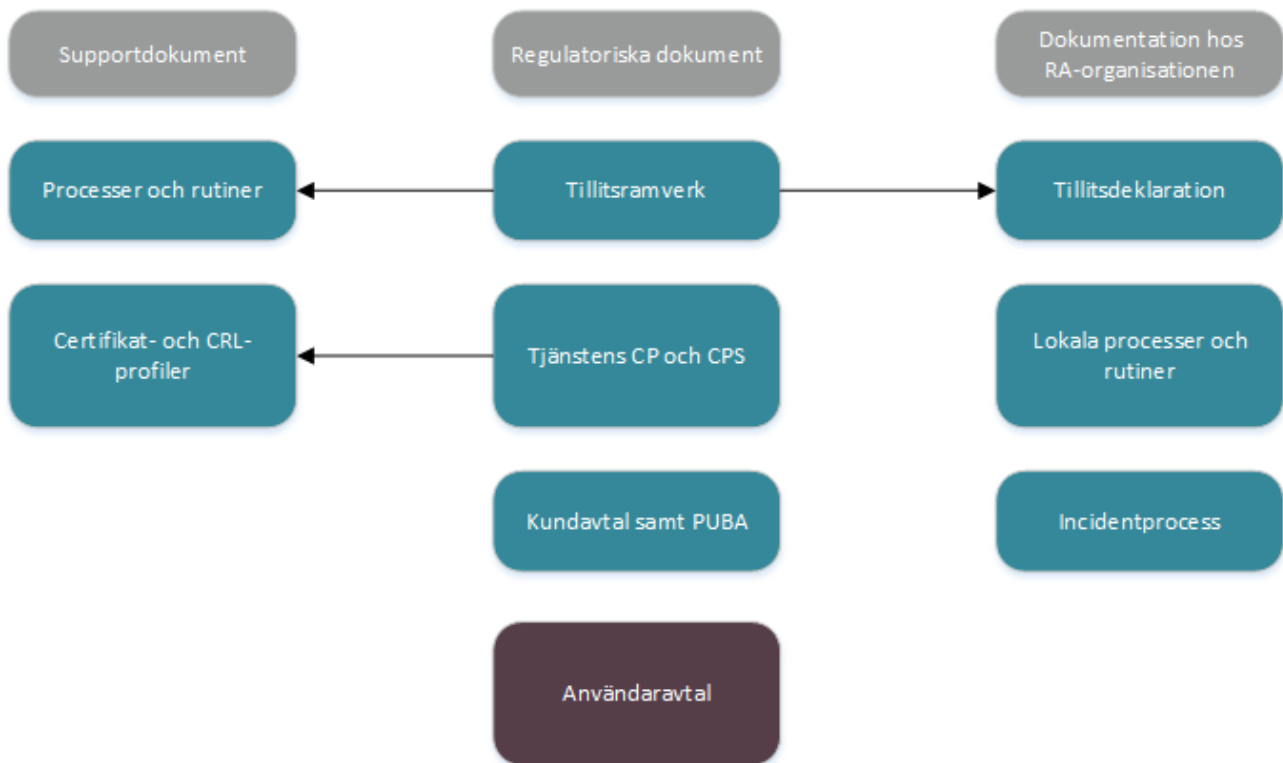
Tillitsdeklarationen skall var 12:e månad fyllas i och lämnas in till Pointsharp, det kan förslagsvis göras i samband med den återkommande internrevisionen som RA-organisationen skall utföra, se stycke [3.2.2 Internrevision](#).

2.1.2 Förvaltning

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

2.2 Tjänstens övergripande dokumenthierarki

Alla regulatoriska och styrande dokument relaterade till Tjänsten ägs och förvaltas av PsPT. Tillitsdeklaration ägs av de anslutna RA-organisationerna, men skall dokumenteras enligt mall från PsPT. RA interna dokument ägs och utformas av de anslutna RA-organisationerna, i vissa fall har PsPT tagit fram exempeldokument som kan användas.



1 Tjänstens dokumentstruktur

3 Säkerhet och revision

Personal hos ansluten RA-organisation skall 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.

Revisionen kommer att genomföras i enlighet med den vid varje tidpunkt gällande processen.

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

Vid revision skall 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 skall ha ett strukturerat informationssäkerhetsarbete relaterat till sina åtaganden inom Tjänsten som skall omfatta:

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

Resultatet från riskanalysen skall 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 skall minst var 12:e månad ha genomfört en internrevision av organisationens efterlevnad av Tillitsramverk för RA och den egna gällande tillitsdeklarationen.

Avvikelse som hittats under internrevision skall hanteras i en åtgärdsplan som därefter skall genomföras. Internrevision och åtgärdsplan med dess genomförande skall dokumenteras.

Dokumentationen skall minst omfatta:

- Problem/risk/avvikelse
- Orsaker
- Förbättringsförslag
- Slutsats/rekommendation
- Tidpunkt för åtgärden
- Ansvarig för åtgärden
- Mätning av effekt/nytta med förbättringsåtgärd från föregående internrevision.

Genomförda internrevisioner skall kunna redovisas vid revision från Pointsharp. Internrevision skall 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 Officer, eller på annat sätt ansvara för eller delta i utfärdande av e-legitimationerna.

3.2.3 Informationssäkerhetsincidenter

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

I händelse av en incident skall lämpliga åtgärder vidtas i samråd med Pointsharp för att mitigera effekten och förhindra ytterligare skador samt minimera risken för återupprepning av incident.

Perioden för RA-organisationen att genomföra åtgärderna beslutas av Pointsharp och är relaterat till händelsens allvar.

En incidentrapport skall upprättas och rapporteras till Pointsharp via kundsupportverktyget som tillhandahålls av Tjänsten.

Se Kundavtalet för mer information om incidentklassificering och incidenthantering.

RA-organisationen skall föra en incidentlogg där alla säkerhetsincidenter relaterade till Tjänsten noteras.

Incidentloggen skall innehålla följande information men är inte begränsad till:

- utfärdarens namn (rapportör),
- kort beskrivande benämning på händelsen (namn),
- unik referens för händelsen (referens),
- status på händelsen (status),
- kategorisering av händelsen (kategorisering),
- när händelsen inträffade eller den uppskattade tidpunkten för den (tidpunkt),
- när Utfärdaren upptäckte händelsen (upptäckt),
- en översiktlig beskrivning av händelsen (beskrivning), och
- bedömning av händelsens omfattning och konsekvenser samt annan information som kan vara av värde (analys).

3.2.4 Fysisk säkerhet

Nyckelbärare skall skyddas fysiskt mot skada och otillåten åtkomst.

Tillträdeskontroll skall tillämpas så att åtkomst till känsliga utrymmen är begränsad till behörig personal. RA Officer skall ha tillgång till låsbar förvaring för ännu inte uthämtade nyckelbärare. RA Security Officer och annan utpekad personal skall 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 skall ha en dokumenterad process för tilldelning och konfiguration av sådana roller. Processen skall 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 skall ha en kontinuitetsplan med etablerade och testade rutiner för verksamhetskritiska funktioner som rör utfärdande och användande av e-legitimationer som utfärdats i Tjänsten.

Rutinerna skall 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 skall 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 skall de användas.

Information som skall 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
- 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 skall 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 ur integritetssynvinkel och har stöd i lag eller annan författning.

Tiden minst 5 år gäller även om avtalsförhållanden med Pointsharp har avslutats.

4 RA-organisationen

Varje ansluten RA-organisation skall utse en RA Security Officer, en RA Auditor och RA Officers, 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 skall skyndsamt meddelas till Pointsharp.

Varje person som utses till en RA-roll i organisationen skall ha uppvisat sig lämplig för respektive roll. Alla RA Officers skall 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 Officers inom RA-domänen. Utbildning av övriga som skall ha rollen RA Officer är organisationen själv ansvarig för.

RA-organisationen är ansvarig för att utbilda sina RA Officers kring GDPR t.ex. 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 skall RA-organisationen skyndsamt utse ny RA Security Officer som skall 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 skall ha de kvalifikationer och den utbildning som krävs för att på ett tillfredsställande, korrekt och säkert sätt utföra de arbetsuppgifter som följer av rollen.

4.1.2 Bakgrundskontroll av RA Security Officer

Det skall utföras en bakgrundskontroll på personen som skall 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 skall ha en process för bakgrundskontroll av RA Security Officer med lämplighetsprövning.

Bakgrundskontrollen skall 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 brottregistret.

4.1.3 RA Security Officers skyldigheter

RA Security Officer skall:

- 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 och funktioner;
- 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 Officers inom RA-domänen och att delar av bakgrundskontrollerna återupprepas med en bestämd periodicitet;
- ansvara för att RA Auditor samt RA Officers 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

4.2.1 Krav på RA Auditor och 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 Officers skall ha adekvat kunskap och förmåga. RA Security Officer skall 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 Officers skall 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 och RA Officer

Innan en person tilldelas en roll inom RA-organisationen skall 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.

Alla RA-organisationer skall upprätta sin egen process för bakgrundskontroll av RA Auditor och RA Officers med lämplighetsprovning.

Bakgrundskontrollen skall inkludera men är inte begränsad till:

- identifiering vid ett fysiskt möte,

- kontroll av nuvarande anställning,
- lämplighetsbedömning för rollen,
- genomgått relevant utbildning,
- en finansiell riskbedömning och
- kontroll mot brottregistret.

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 skall 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.

5 Avveckling av RA-domän

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

Den anslutna organisationen skall:

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 skall 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 underrättats om och accepterat Användaravtalet, det vill säga villkoren för användningen av e-legitimationen. Villkoren skall distribueras till användaren innan besöket för uthämtning av e-legitimationen så att användaren har tid på sig att läsa igenom avtalet.

Användaren skall informeras om att förvara koder och nyckelbärare så att obehöriga inte får tillgång till dessa samt att koder och nyckelbärare skall 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.

Tillitsnivå	Nyckelbärare	Giltighetstid (maximal)
LoA3	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 och konsulter inom RA-organisationen eller till andra personer med en relation till RA-organisationen.

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

6.5 Beställning av e-legitimation

Beställningen av e-legitimationen innefattar 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 skall ske enligt av PsPT fastställda rutiner.

Nyckelbärare	Identifieringsprocedur
Ordinarie personaliserat smartkort från korttillverkare	Identifiering skall ske på plats genom ett personligt möte med RA Officer enligt av RA fastställda rutiner. Identifiering sker med någon av följande svenska identitetshandlingar: <ul style="list-style-type: none">• 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 skall ske enligt av PsPT fastställda rutiner.

Nyckelbärare	Identifieringsprocedur
Ordinarie personaliserat smartkort från korttillverkare	Identifiering skall ske på plats genom ett personligt möte med RA Officer enligt av RA fastställda rutiner. Identifiering sker med någon av följande svenska identitetshandlingar: <ul style="list-style-type: none"> • Körkort • Nationellt id-kort • Pass • SIS-märkt id-kort • 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 uthämtning 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 skall skyndsamt verkställas av auktoriserad personal inom RA-domänen.

Spärr kan utföras av användaren eller behörig RA Officer.

Spärr skall 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 misstänks vara röjda.
- Vid misstanke om otillåten användning.
- 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		
assymetrisk kryptering		krypteringssystem där olika nycklar används för kryptering respektive dekryptering		
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. <ul style="list-style-type: none"> • namn och lösenord • certifikat • engångslösenord 	

Term	Synonym	Definition	Anmärkning	Avrådda termer
beställning		delen av utfärdandeprocessen av e-legitimation för en beviljad ansökan fram till att den kan hämtas ut		
biometrisk identifiering		verifiering av en persons identitet baserad på dennes fysiologiska eller beteendemässiga egenskaper		
CA		betrodd instans som har till uppgift att skapa och utge certifikat, kan vara en organisatorisk enhet i ett	en-US: certification authority, certificate authority	

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	<p>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.</p> <p>Anmärkning språkbruk: Använd inte termen e-legitimation istället för <i>certifikat</i> när det är väsentligt att det framgår att det är certifikatet som avses.</p>	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	<p>en-US: certificate authority</p> <p>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 spärllistor. Certifikatutfärdaren går i god för att informationen i certifikatet är korrekt.</p> <p>Anmärkning språkbruk: Kortformen <i>utfärdare</i> bör endast användas när det inte finns risk för missförstånd. Är det oklart vilken sorts utfärdare som avses, bör den rekommenderade termen <i>certifikatutfärdare</i> användas. Använd <i>CA</i> (som är en förkortning av det engelska <i>certification authority</i>) endast i rent tekniska sammanhang.</p>	

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	<p>En e-legitimation innehåller flera delar, varav certifikaten (tillsammans med s.k. nycklar) utgör en förutsättning för legitimering och underskrift. E-legitimationen kan till exempel lagras på ett kort eller i en dator.</p> <p>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 <i>e-id</i> inte ska utläsas <i>elektronisk identitet</i>. Jämför identitet.</p>	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 [<i>sic!</i>] 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 <i>person-id</i> händer det att förkortningen <i>id</i> utläses som <i>identitet</i> . I sådana uttryck bör dock <i>id</i> utläsas som <i>identitetsbeteckning</i> . Undvik uttrycket <i>elektronisk identitet</i> . 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	<p>Identiteten uttrycks genom någon typ av representation, t.ex. personnummer eller annan identitetsbeteckning.</p> <p>Anmärkning språkbruk: Termen <i>autentisering</i> används synonymt med <i>identifiering</i> i tekniska sammanhang, men bör undvikas i dokument som riktar sig till allmänheten. Uttrycket <i>verifiering av identitet</i> kan också uppfattas som alltför tekniskt i texter riktade till allmänheten. Notera att verbet som hör ihop med <i>är identifiera</i> och inte <i>identifiera sig</i>. Mer tekniska synonymer till <i>identifiera</i> är <i>verifiera identitet</i> och <i>autentisera</i>.</p>	

Term	Synonym	Definition	Anmärkning	Avrådda termer
identitetshandling	legitimationshandling, legitimation	handling som innehåller uppgifter som är tillräckliga för en direkt eller indirekt identifiering av innehavaren	<p>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.</p> <p>Innehavaren av en identitetshandling kan vara en fysisk eller en juridisk person.</p> <p>Identitetshandlingar kan vara fysiska (identitetskort, pass) eller elektroniska (e-legitimation).</p>	
kryptering		omvandling av klartext till kryptotext i syfte att förhindra obehörig åtkomst av information		
LDAP		protokoll som används för kommunikation med en certifikatkatalog över Internet	en-US: lightweight directory access protocol	
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 <i>behörighetskontroll</i>) 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: SE999999999901 , 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	online certificate status protocol	protokoll till vilket man kan ställa frågan om ett visst certifikat är giltigt		

Term	Synonym	Definition	Anmärkning	Avrådda termer
PIN-kod		lösenord oftast bestående enbart av siffror	<p>en-US: personal identification number</p> <p>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.</p>	

Term	Synonym	Definition	Anmärkning	Avrådda termer
PKI		infrastruktur för kryptering med publik nyckel	<p>en-US: public key infrastructure</p> <p>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.</p> <p>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.</p>	
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	
S/MIME		standard för säker e-post via Internet	en-US: secure multipurpose internet mail extensions	
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		

Term	Synonym	Definition	Anmärkning	Avrådda termer
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
verifiering		kontroll av certifikat, giltighet m.m.	Vid till exempel elektronisk identifiering eller elektronisk signering	
X.509		standard för hur certifikat ska se ut och vad de ska innehålla		



Website

<https://www.pointsharp.com>

Copyright

© 2023, Pointsharp AB. All rights reserved worldwide.

Disclaimer

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

Classification: Public
Publ. No.: PSC-Rd22-04
Document version: 2.0
Document status: Final
OID: 1.2.752.179.100.1.3
Published: 11 Sep 2023