POINTSHARP

Tillitsramverk för RA

Pointsharp Secure Cloud Net iD SweID

Classification:	Public
Publication No.:	PSC-Rd22-04
Document version:	1.0
Document status:	Final
Date:	03 Jun 2022

Table of Contents

1 Inledning

1.1 Bakgrund och syfte

Pointsharp Secure Cloud Net iD SweID (hädanefter kallad "Tjänsten") ska tillhandahålla e-legitimationer för identifiering och signering för verksamheten och tjänster inom privat och offentlig sektor för användning i Tjänsten i enlighet med Tillitsramverk för kvalitetsmärket Svensk e-legitimation utfärdad av DIGG (hädanefter kallad "DIGGs Tillitsramverk"). I e-legitimationer ingår även de bärare (exempelvis kort, mobiltelefon) som behövs och Pointsharp Secure Cloud Net iD SweID Tillitsramverk för RA (hädanefter kallad Tillitsramverket) gäller även för dessa i tillämpliga delar.

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

För e-legitimationer för personer är kraven fördelade på olika tillitsnivåer. Detta svarar mot olika grader av teknisk och operationell säkerhet hos ansluten organisation som ger olika säkerhet i kontrollen av att en person, som tilldelas en e-legitimation, verkligen är den han eller hon utger sig för att vara. Nivåindelningen motsvarar den som används i den internationella standarden ISO/IEC 29115, eller myndigheten för Digital förvaltning, DIGG, beskrivning som bygger på samma standard. Kraven i detta tillitsramverk gäller tillitsnivå 3 (LoA3), där nivå 3 motsvarar den nästa högsta nivån på processen för fastställande av identitet och skydd av e-legitimationer.

1.2 Översikt

Detta dokument beskriver det Tillitsramverk för Tjänsten som alla anslutna RA organisationer ska uppfylla och är baserat på valda delar av DIGGs Tillitsramverk som även definierar grundkraven för Pointsharp Secure Cloud 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 dokumenthierarkin.

1.3 Målgrupp

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

1.4 Identifiering

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

Namn	Objektidentifierare (OID)	Beskrivning
Pointsharp Secure Cloud Net iD SweID Tillitsramverk för RA	{1.2.752.179.100.1.3}	Detta dokument
Pointsharp Secure Cloud Net iD SweID Certificate Policy and Certification Practice Statement	{1.2.752.179.100.2.3}	Tjänstens CP och CPS

1.5 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. RA-organisationen är ansvarig för att eventuella underleverantörer som utför uppdrag i Tjänsten uppfyller kraven i TIllitsramverket som rör deras verksamhet samt utför granskning av dessa.

Alla 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 måste göras av användaren själv eller annan funktion i organisationen.

2.1.1 Regelverk

Regelverket för Tjänsten ägs och förvaltas av PsPT. Regelverket beskrivs i Tjänstens samlade dokumentstruktur. Varje RA-organisation som ansluter sig ska lämna in en tillitsdeklaration, en självskattning av organisationens överensstämmelse med Tillitsramverket och Tjänstens CP och CPS inom sin RA-domän.

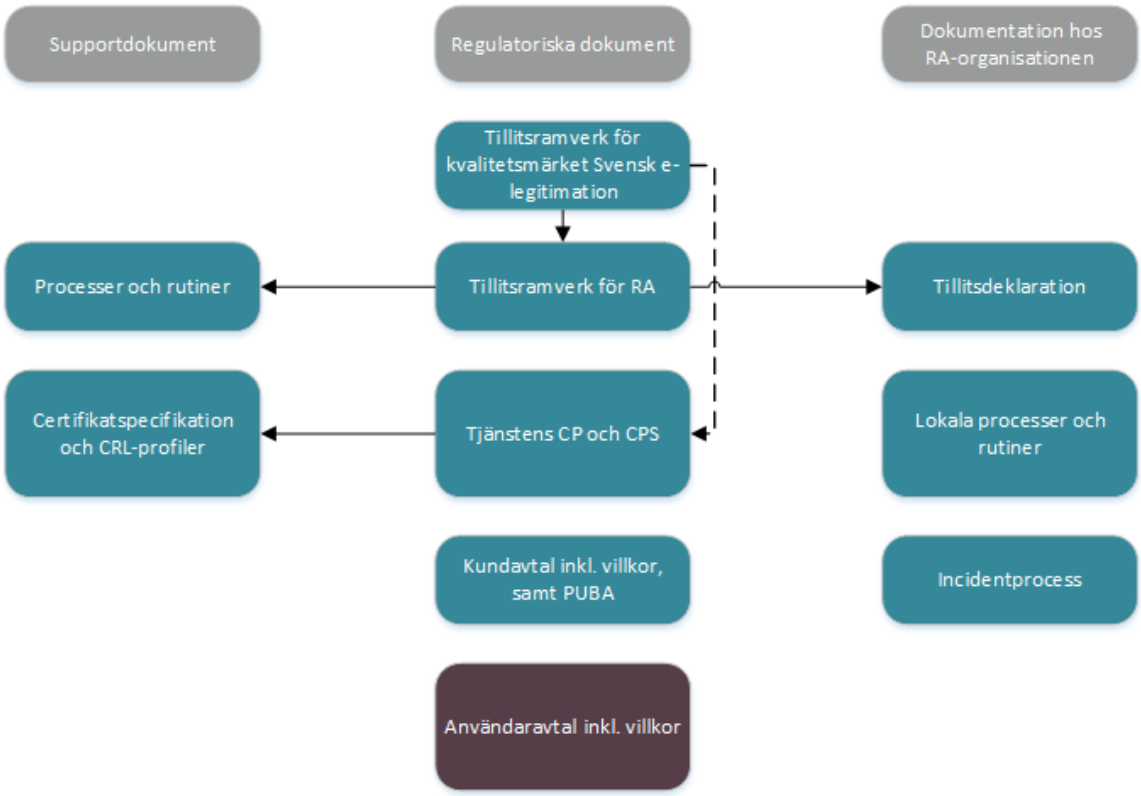
Tillitsdeklarationen skall periodiskt lämnas in till PsPT, det kan förslagsvis göras vid den återkommande internrevisionen, se kapitel 3.4 .

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 övergripande dokumentstruktur

Alla styrande och stödjande dokument ägs och förvaltas av PsPT. Anslutningsdokument ägs av de anslutna RA-organisationerna, men ska tas fram enligt mallar från PsPT. Lokala dokument ägs och formges av de anslutna 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 uppgifter vid revision som PsPT har rätt att utföra hos ansluten organisation,
- vid säkerhetsincidenter,
- vid andra rappporterade fel och brister.

3.1 Informationssäkerhet

Ansluten RA-organisation ska ha ett strukturerat säkerhetsarbete relaterat till sina åtaganden inom Tjänsten som ska omfatta:

- En riskhanteringsprocess som kontinuerligt analyserar hot och sårbarheter i verksamheten relaterat till Tjänsten och bedömer sannolikhet och konsekvens för (skada på) användare och RA-organisationen inom Tjänsten. Resultatet från riskanalysen ska leda till säkerhetsåtgärder som ska balansera riskerna till acceptabla nivåer. Riskanalys och åtgärdsplan ska dokumenteras och kunna visas vid revision.
- En dokumenterad och strukturerad informationssäkerhetshantering:
  - ett dokumenterat informationssäkerhetsarbete med praxis och policyer.
  - ett ledningssystem för informationssäkerhet (ISMS), enligt ISO/IEC 27001 eller motsvarande, finnas på plats för de delar som rör Tjänsten.

- Kontinuerligt genomförda och dokumenterade internrevisioner.
- En upprättad och beprövad kontinuitetsplan.

3.2 Kontinuitetsplan

RA-organisationen måste ha en etablerad och beprövad kontinuitetsplan som berör Tjänsten. Rutinerna ska innefatta planer för hantering av avbrott i tjänster som hanterar spärrstatus (OCSP och certifikatspärrlistor (CRL)) och utfärdande av e-legitimationer. Varje RA-organisation är ansvarig för möjligheten att komma åt nyckelkomponenter såsom CRL:er.

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 säkerhets- eller tillgänglighetsincidenter som gör att Tjänsten inte är tillgänglig, till exempel översvämning, brand eller andra händelser i kategorin "force majeure".

3.3 Revision från PsPT

Ansluten RA-organisation kommer regelbundet att vara föremål för revision från PsPT. Revisionen kommer att genomföras i enlighet med den vid varje tidpunkt gällande processen. De åtgärder som blir följd av revisionen ska genomföras av RA-organisationen.

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

3.4 Internrevision

Ansluten RA-organisation ska minst var 12:e månad ha genomfört internrevision. Funna avvikelser ska resultera i en åtgärdsplan och denna ska genomföras. Internrevision och åtgärdsplan med genomförande ska dokumenteras. Dokumentationen ska minst omfatta:

- Problem/risk/avvikelse
- Orsaker
- Förbättringsförslag
- Slutsats/rekommendation
- Mätning av effekt/nytta med förbättringsåtgärd från föregående internrevision. Genomförda internrevisioner ska kunna redovisas vid revision från PsPT. Internrevision ska ledas av RA Auditor eller oberoende extern revisor/ kontrollfunktion.
  Med oberoende menas att det inte är någon som inte är RA Officer, eller på annat sätt ansvarar eller deltar i utgivningen av e-legitimationer.

3.5 Säkerhetsincidenter

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

I händelse av en säkerhetsincident måste lämpliga åtgärder vidtas i samråd med PsPT för att mitigera effekten och förhindra ytterligare skador. Perioden för RA-organisationen att genomföra åtgärderna beslutas av PsPT och är relaterat till händelsens allvar.

En incidentrapport ska upprättas och rapporteras till PSPT via kundsupportverktyget som tillhandahålls av Tjänsten. Se Kundavtalet för mer information.

3.6 Spårbarhet, gallring och bevarande av dokumentation

Ansluten RA-organisation ska bevara de dokument 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.

Dokumentation som ska bevaras:

- godkänd tillitsdeklaration
- förteckning av utsedda RA Officer samt deras områden, inklusive historik
- avtal med tredjepartsorganisationer
- kvittenser avseende utfärdade e-legitimationer
- dokumentation av interna revisioner samt åtgärdsplaner
- beställning av e-legitimationer för funktion och kvittens på mottagande

Tiden för bevarande ska inte understiga 10 (tio) 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 10 år gäller även om avtalsförhållanden med Pointsharp har avslutats.

4 RA-organisationen

Varje ansluten RA-organisation måste utse en RA Security Officer, en RA Auditor och RA Officers, samt upprätta en organisation för ansökan, beställning, utdelning, support och spärr av e-legitimationer inom RA-domänen. Förändringar av RA Security Officer och RA Auditor som ingår i RA-domänen ska skyndsamt meddelas till PsPT.

Varje utpekad person med en roll i måste uppvisat sig lämplig för respektive roll.

Organisationen är ansvarig för att utbilda sina handläggare och slutanvändare kring GDPR t.ex. gällande "privacy notice" och rutiner för behandling av persondata.

4.1 Krav på RA Security Officer

4.1.1 Bagrundskontroll

En person i RA-organisationen med mandat att utföra identitetskontroller ska identifiera personen som tilldelas rollen RA Security Officer med hjälp av en svensk id-handling. Detta kan också ske på uppmaning av PsPT.

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

RA Security Officer ska ha tillräcklig med tid avsatt för att klara sitt uppdrag.

Det ska utföras en bakgrundskontroll på RA Security Officer enligt nedanstående lista. 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 måste inrätta sin egen process för bakgrundskontroll av RA Security Officer med lämplighetsprövning. Bakgrundskontrollen måste inkludera men är inte begränsad till:

- identifiering vid ett fysiskt möte,
- kontroll av nuvarande anställning,
- lämplighetsbedömning för tjänsten,
- genomgått relevant utbildning, och
- en finansiell riskbedömning.

4.2 RA Security Officers skyldigheter

RA Security Officer ska:

- ha det övergripande ansvaret för att upprätta ett RA-ansvarsområde med tillräckliga personella resurser för att uppfylla organisationens åtaganden;
- ansvara för att RA-domänen följer Tjänstens regler och rutiner om ansökan, beställning, utlämnande och spärr av e-legitimationer till personer och funktioner;
- ansvara för att lämna in tillitsdeklarationen till PsPT;
- ansvara för att personkontroller utförs på alla personer som är RA Officer inom RA-domänen;
- ansvara för att RA Officer har adekvat kunskap och kompetens för att upprätthålla organisationens åtagande över tid;
- ansvara för att utvärdera RA-domänens efterlevnad av utgivningsprocesser för e-legitimationer. I detta ingår ansvar för att riskanalyser genomförs;
- ansvara för hantering av roller inom organisationen för åtkomst till Tjänsteportalen;
- ansvara för att säkerhetsincidenter och fel i Tjänsten rapporteras till Pointsharp;
- 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.

Om RA Security Officer lämnar rollen ska RA-organisationen skyndsamt utse ny RA Security Officer som ska kommuniceras till och godkännas av PsPT. Under tiden som RA Security Officer saknas övertar RA-organisationens ordinarie säkerhetsansvarige temporärt de skyldigheter som normalt åligger RA Security Officer, dock kan inte Säkerhetsansvarig få motsvarande behörigheter i systemen.

4.2.1 Bakgrundskontroll av RA Auditor och RA Officers

Innan en person tilldelas en roll inom RA-organisationen ska RA Security Officer, eller en områdesansvarig som denna delegerat ansvaret till, ha genomfört en identitetskontroll med hjälp av godkänd id-handling samt gjort 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.

Personen får inte ha annat uppdrag som kan bedömas stå i konflikt med arbetet inom RA-domänen.

Alla RA-organisationer måste inrätta sin egen process för bakgrundskontroll av RA Auditor och RA Officers med lämplighetsprövning. Bakgrundskontrollen måste inkludera men är inte begränsad till:

- identifiering vid ett fysiskt möte,
- kontroll av nuvarande anställning,
- lämplighetsbedömning för tjänsten,
- genomgått relevant utbildning, och
- en finansiell riskbedömning.

4.2.2 Utbildning av RA Auditor och RA Officers

RA Auditor samt alla RA Officers måste 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 säkras. Uppföljning av utbildning av administratörer ska genomföras så att kvalité upprätthålls inom RA-organisationen.

4.3 RA Auditors skyldigheter

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

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

Om RA Auditor lämnar rollen ska RA Security Officer skyndsamt tillse att en ny RA Auditor utses. Under den tid som RA Auditor saknas övertar RA Security Officer temporärt de skyldigheter som normalt åligger RA Auditor. Dock kan inte RA Security Officer få motsvarande behörigheter i systemen.

4.4 Krav på kontinuitetsplan

Respektive organisation är skyldig att upprätta en kontinuitetsplan. Se stycke 3.2.

5 Avveckling av RA-domän

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

Den anslutna organisationen som står som ansvarig för tillitsdeklarationen 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 3.6.

6 Fysisk och administrativ säkerhet

6.1 Fysisk säkerhet

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

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

6.2 Administrativ säkerhet

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

7 E-legitimationer

7.1 Användningsområden

E-legitimationer utfärdade inom Tjänsten skall användas:

- för personligt bruk, samt
- för att identifiera fysiska personer verksamma i privat eller offentlig sektor vid legitimering och underskrift.

7.2 Villkor

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

Användaren ska informeras om att förvara pin- och eventuella pukkoder, bärare så att obehöriga inte får tillgång till dessa samt att koder och bärare ska förvaras fysiskt åtskilda.

7.3 Giltighetstid för e-legitimation

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

Tillitsnivå	Nyckelbärare	Giltighetstid (maximal)
LoA3	Ordinarie smartkort eller annan hårdvarubärare	5 år
	Tillfälligt smartkort eller annan hårdvarubärare	1 år

Tillitsnivå	Nyckelbärare	Giltighetstid (maximal)
	Mobil App	3 år

7.4 Ansökan om e-legitimation

7.4.1 Förutsättningar

E-legitimationer kan utfärdas:

- till anställda och konsulter inom RA-organisationen eller till andra personer med en relation till RA-organisationen.
- på begäran av användaren eller genom annat likvärdigt acceptförfarande.
- till personer som har fyllt 16 år.
- efter att ansökan har kunnat knytas till personnummer eller styrkt samordningsnummer samt till de uppgifter som i övrigt är nödvändiga för att kunna tillhandahålla e-legitimation.

RA Officer ska neka utfärdande om förutsättningarna inte är uppfyllda.

7.5 Beställning av e-legitimation

7.5.1 Kontroll av personuppgifter

RA Officer ska kontrollera att uppgifterna knutna till ansökan är fullständiga och stämmer överens med de uppgifter som finns registrerade i Skatteverkets SPAR-tjänst.

7.5.2 Identifiering vid beställning

All identifiering ska ske enligt av PsPT fastställda rutiner.

Användarens identitet ska verifieras mot ett Skatteverkets SPAR-tjänst samt visa giltig svensk id-handling.

Tillitsnivå	Nyckelbärare	Identifieringsprocedur
LoA3	Ordinarie smartkort eller annan hårdvarubärare	Personligt besök och giltig svensk id-handling krävs vid utgivning.
	Tillfälligt smarkort eller annan hårdvarubärare	Personligt besök och giltig svensk id-handling krävs vid utgivning.
	Mobil app	Personligt besök och giltig svensk id-handling krävs vid utgivning.
	Mobil app (id-växling)	En annan giltig e-legitimation med minst LoA3 måste användas innan utfärdande och mottagande.

7.6 Utlämning av e-legitimation

Vid utlämning ska RA Officer genomföra en identitetskontroll. Identifieringssättet ska dokumenteras.

7.6.1 Identifiering vid personligt möte

All identifiering ska ske enligt av PsPT fastställda rutiner.

Tillitsnivå	Utlämningsprocess	Identifieringsprocedur
LoA3	Personligt möte med RA Officer	Identifiering av en användare sker vid ett personligt möte där användaren presenterar en giltig svensk id-handling för en behörig RA Officer.
	Mobila applikationer (derived)	I de fall ett personligt besök inte kan ske är även följande identifieringssätt godkända: • Befintlig e-legitimation godkänd av PsPT

7.6.2 Utlämning vid personligt möte

RA Officer ska, vid personligt besök och efter utförd identitetskontroll, lämna ut e-legitimation mot undertecknad elektronisk kvittens. I samband med detta måste användaren läsa och acceptera Användaravtalet för Pointsharp Secure Cloud Net iD SweID.

Användaren väljer sin egen PIN-kod och undertecknar elektroniskt kvittot för e-legitimation och godkännandet av Användaravtalet.

Tillitsnivå	Identifieringsprocedur
LoA3	Användaren ska kvittera e-legitimationen med egen angiven PIN-kod. Personen verifieras i betrott register (SPAR). Legitimering med en giltig svensk id-handling krävs. Användaren väljer själv sin PIN-kod.

7.7 Spärr av e-legitimation

Spärrbegäran kan komma från användaren, verksamheten eller utgivande organisation. Spärrbegäran måste omedelbart och säkert verkställas av auktoriserad personal inom RA-domänen eller CA.

Spärr kan utföras av användaren eller behörig RA Officer. Användarens identitet verifieras med någon av dess unika identifierare.

Spärr kan göras om något av följande har inträffat:

- Förhållanden som kan påverka certifikatsinnehållet har ändrats.
- Någon uppgift i e-legitimationen är eller misstänks vara felaktig.
- Användaren har tappat kontrollen över bäraren eller koderna.
- Vid misstanke om otillåten användning.

- När bäraren återlämnas.
- När den e-legitimationen inte längre behövs.
- När e-legitmiationen har använts i strid med de regler som anges i Användaravtalet.
- När användaren inte längre har någon koppling till utgivande organisation.

8 Appendix A: Termordlista

Term	Synonym	Definition	Anmärkning	Avrådda termer
assymetric encryption	public-key cryptography	krypteringssystem där olika nycklar används för kryptering respektive dekryptering		
auktorisering		tillåtelse för en användare, ett program eller en process att använda ett eller flera objekt		
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		
authority information access	AIA	plats där utfärdarcertifikat kan hämtas för att verifiera certifikatskedjan		

Term	Synonym	Definition	Anmärkning	Avrådda termer
avancerad elektronisk signatur		elektronisk signatur som • är knuten uteslutande till en undertecknare • gör det möjligt att identifiera undertecknaren • är skapad med hjälpmedel som endast undertecknaren kontrollerar • är knuten till andra elektroniska data på ett sådant sätt att förvanskningar av dessa data kan upptäckas		
behörighets-kontrollsystem		system som anger en användares behörighet, dvs. tillgång till system eller data	Behörighetskontrollsystem kombinerat med elektronisk identifiering ger ett effektivt sätt för accesskontroll.	
biometrisk identifiering		verifiering av en persons identitet baserad på dennes fysiologiska eller beteendemässiga egenskaper		
CA	certification authority certificate authority	betrodd instans som har till uppgift att skapa och utge certifikat, kan vara en organisatorisk enhet i ett		

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
CP	certificate policy	dokument som redogör för under vilka förhållanden ett certifikat är utfärdat av en CA		
spärrlista	CRL, certificate revocation list	spärrlista över certifikat som inte längre är giltiga		revokeringslista

Term	Synonym	Definition	Anmärkning	Avrådda termer
certifikatutfärdare	CA, utfärdare	organisation eller organisatorisk enhet som har till uppgift att skapa, tillhandahålla och spärra certifikat	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
CPS	certification practice statement	dokument i vilket en CA beskriver de rutiner vilka tillämpas vid utgivning av certifikat		
dekryptering		avkodning av kryptotext		
e-id-kort	e-legitimationskort	aktivt kort på vilket det lagras en elektronisk legitimation		

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		
hårt certifikat		privat nyckel som är hårdvaruskyddad, dvs. lagras i chip på ett smartkort		

Term	Synonym	Definition	Anmärkning	Avrådda termer
hash	hash-funktion	algoritm som avbildar eller översätter en uppsättning av bitar till en annan uppsättning på ett sådant sätt att • ett meddelande ger samma resultat varje gång algoritmen exekveras med inmatning av samma meddelande. • det är datamässigt omöjligt att härleda eller rekonstruera Ett meddelande från Det resultat som produceras av algoritmen. • det är datamässigt omöjligt att hitta två olika meddelanden som producerar samma hash resultat med användning av samma algoritm.		
hashsumma	kondensat	kontrollsumma som skapas utifrån det digitala dokumentets innehåll när man vill utföra en digital signatur		
HSM	hardware security module	skyddar nycklar till CA i en extern hårdvara		

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.	
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 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).	
kryptering		omvandling av klartext till kryptotext i syfte att förhindra obehörig åtkomst av information		
kvalificerad elektronisk signatur		avancerad elektronisk signatur som är baserad på ett kvalificerat certifikat och som är skapat av en säker anordning för signaturframställning		
kvalificerat certifikat		certifikat som uppfyller kraven i 6 § eller 7 §, Lag om kvalificerade elektroniska signaturer (SFS 2000:832)	SFS 2000:832	

Term	Synonym	Definition	Anmärkning	Avrådda termer
LDAP	lightweight directory access protocol	protokoll som används för kommunikation med en certifikatkatalog över Internet		
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. **Anmärkning språkbruk:** Se figur 1 som visar relationen mellan att identifiera (någon) och att legitimera sig.	identifiera sig
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			eng: VAT registration number	
mjukt certifikat		privata nyckel som är mjukvaruskyddad d.v.s. lagras på diskett, hårddisk eller CD		
Net iD		PKI klient (CSP) som används för att kommunicera med det smarta kortet		
Net iD Card Portal	NiCP	används för att ställa ut certifikat till användarnas smarta kort samt att administrera och hantera utgivningen av dessa kort		
nyckel	krypteringsnyckel	varierbar information som styr en krypteringsalgoritms omvandling av klartext till kryptotext		
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	personal identification number	lösenord oftast bestående enbart av siffror	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.	
PKCS	public key cryptography standard	rekommendationer för kryptering, utgivna av RSA, vilka betecknas PKCS med ett löpnummer		

Term	Synonym	Definition	Anmärkning	Avrådda termer
PKI	public key infrastructure	kombination av teknik, standarder och juridik som möjliggör säker kommunikation. En teknik och metod som gör det möjligt att utföra grundfunktionerna elektronisk identifiering, elektronisk signering och kryptering. 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. Myndigheter och företag kan nå ut brett med individbaserade tjänster som aldrig stänger, vare sig helger eller nätter. PKI utnyttjar avancerad kryptografi och teknik, men användaren behöver inte veta något om det eller vidta några extra åtgärder. Allt sker med automatik. Metoden växte fram mot slutet av 1970-talet och är sedan länge förhärskande för säker kommunikation över publika nät.	sv-SE: infrastruktur för kryptering med öppen nyckel	
PKI	public key infrastructure	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 tillåter användare av internet och andra offentliga nätverk att engagera sig i säker kommunikation, datautbyte och pengautbyte genom offentliga och privata kryptografiska nyckelpar som tillhandahålls av en certifikatutfärdare.	

Term	Synonym	Definition	Anmärkning	Avrådda termer
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		
PUK-kod	personal unblocking key	används för att låsa upp ett kort som har spärrats, t.ex. då användaren har angivit fel PIN-kod tre gånger i rad		
registration authority	RA	authority in a network that verifies user requests for a digital certificate and tells the certificate authority to issue it		
revokering		Ett annat begrepp för spärrhantering. Om användaren tappar sitt certifikat eller någon missbrukar det så kan certifikatet spärras.		
RSA		asymmetrisk krypteringsalgoritm	uppkallad efter upphovsmännen Rivest, Shamir och Adleman	

Term	Synonym	Definition	Anmärkning	Avrådda termer
S/MIME	secure multipurpose internet mail Extensions	standard för säker e-post via Internet		
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		
TSS	time stamping service	tjänst som tidstämplar en elektronisk handling, till exempel elektronisk signering av ett elektroniskt dokument		
TTP	trusted third party	roll som innebär att ett företag eller en organisation är betrodd som till exempel certifikatutgivare	sv-SE: betrodd tredje part	
verifiering		kontroll av certifikat, giltighet etc., vid till exempel elektronisk identifiering eller elektronisk signering		

Term	Synonym	Definition	Anmärkning	Avrådda termer
X.509		standard för hur certifikat ska se ut och vad de ska innehålla etc.		

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: 1.0
Document status: Final
OID:
Published: 03 Jun 2022