



Rutin och handledning för Ansvarig utgivare

Identifieringstjänst SITHS



Innehåll

1. Dokumentets syfte	3
2. Termer och begrepp.....	3
3. Tillitsramverk	4
4. Tillitsdeklaration	4
4.1 Vägledning för att besvara tillitsfrågor	4
5. Uppdatera SITHS kontaktuppgifter vid förändring	5
6. Easy	5
6.1 Konto och inloggning i Easy	5
6.2 Handledning Easy	5
7. Rutin för personkontroller	9
7.1 Lämplighet och anställning	9
7.2 Legal lämplighet	10
7.3 Finansiell lämplighet	10
7.4 Utbildning.....	10
8. Intern revision och förbättringsarbete	10
9. Riskanalys	11
10. Säkerhetsincidenter – rapportering.....	11
11. Utbildning för ID-administratörer.....	11
12. Beskrivning av roller inom SITHS.....	12
Förenklad matris över roller.....	13
12.1 Tilldelning av roll kopplat till ID-administratörens arbetsuppgifter	13
13. Behörighet för ny ID-administratör	14
14. Korttyper	15
15. Konfiguration i SITHS Admin	15
15.1 Konfigurerar organisationsparametrar.....	15
15.2 Konfigurera e-postmallar	16
15.3 Konfigurera kvittensmallar	17
15.4 Tilldela roll i SITHS Admin.....	18
15.5 Ta bort roll i SITHS Admin.....	18
16. Beställa reservkort	19
Återlämning och avregistrering	20
16.1 Ej återlämnade SITHS-kort	20
16.2 Ej utlämnade SITHS-kort.....	20
16.3 Spärr	20



17.	Giltiga kort för borttagna personer	21
18.	Skicka ordinarie kort mellan kontor	22
19.	Arkivering av kvittenser	22
	Funktionscertifikat	23
19.1	Gör så här för att skapa och leverera funktionscertifikat	24
19.2	Arkivera kvittens	25
20.	Domänvalidering	25
20.1	Gör så här för att anmäla domäner	26
21.	Statistik och loggar	26
21.1	Användningsområden för olika rapporter	27
21.1.1	Hitta ordinarie SITHS-kort med status = Skickat	27
22.	Regler vid verksamhetsövergång och ägarbyte	29
22.1	Regler gällande utfärdarnummer	30
22.1.1	Organisationen äger sitt eget utfärdarnummer:	30
22.1.2	När ett ombuds utfärdarnummer har använts vid utfärdande av SITHS-kort:	30
23.	Namnbyte av organisation	30
24.	Lägga ner utgivningsområde	30
25.	Från tredjepartsanslutning till direktanslutning	31
26.	Byte av ombud/Övergång till ombud	31
26.1	Tredjepartsansluten organisation som vill byta ombud	31
26.1.1	Tredjepartsansluten organisation	31
26.1.2	Avgående ombud	31
26.2	Direktansluten organisation som byter till ombud	31
26.2.1	Direktansluten organisation	31
26.2.2	Tillträdande ombud	32
27.	Verksamhetsövergång	32
27.1	Direktansluten organisation övertas men lever kvar med eget organisationsnummer	32
27.2	Direktansluten organisation övertas och upphör	32
27.3	Direktansluten övertar en tredjepartsansluten	32
27.4	Utfärdade SIS-kort	33
28.	Ombud och tredjepartsanslutning	33
29.	Mallar för kvittenser och e-post	33
29.1	E-postutskick	33
29.1.1	Påminnelse av utgående certifikat	34
29.1.2	Beställning av nytt certifikat	34
29.1.3	Misslyckad publicering av certifikat	34



29.2	Kvittenser.....	35
29.2.1	Ordinarie kort.....	35
29.2.2	Funktionscertifikat.....	36
29.2.3	Reservkort	37

Revisionshistorik

Version	Datum	Författare	Kommentar
0.9	2019-01-15	Kerstin Arvedson/Cathrine Andersson	Upprättat dokument
1.0	2019-03-08	SITHS Policy Authority	Fastställt
1.1	2019-04-11	SITHS Policy Authority	Tillagt: Beskrivning av roller inom SITHS Giltiga kort för borttagna personer
1.2	2019-05-14	SITHS Policy Authority	Uppdaterat rutinen för domänvalidering
1.3	2019-10-14	SITHS Policy Authority	Förtydligat information om nivåindelningen i Easy
1.4	2019-11-27	Siths Policy Authority	Förtydligat om avregistrering, spärr och ej utlämnade kort. Förtydligande om utfärdarnummer, personkontroller och kvittenstext

1. Dokumentets syfte

Detta dokument ska vara ett stöd för dig som har rollen Ansvarig utgivare inom Identifieringstjänst SITHS för en eller flera organisationer i ett utgivningsområde. Dokumentet innehåller rutiner och handledningar samt hänvisning till styrande och stödjande dokument för SITHS.

2. Termer och begrepp

<https://www.inera.se/siths/repository>



3. Tillitsramverk

Du som är Ansvarig utgivare ska ha god kännedom om SITHS tillitsramverk

<https://www.inera.se/siths/repository>

4. Tillitsdeklaration

Du som är Ansvarig utgivare besvarar tillitsdeklarationen årligen genom att göra en bedömning av hur väl det egna utgivningsområdet uppfyller kraven i tillitsramverket. Bedömningen blir sedan grund för det egna förbättringsarbetet. Du hanterar tillitsdeklarationen i Easy.

4.1 Vägledning för att besvara tillitsfrågor

Att arbeta med förbättring av ett ledningssystem (riktlinjer, processer, rutiner och roller) blir aldrig klart.

Vid bedömning av nivå vid tillitsdeklaration används en skala Nivå 1 – Nivå 5.

Nivå 1

Inte alls. Vid den här nivån har inte någon aktivitet genomförts för att möta upp mot kravet i Tillitsramverket.

Nivå 2

Initierad. Här har verksamheten initierat ett arbete för att möta upp mot kravet i Tillitsramverket.

Nivå 3

Påbörjad. Verksamheten har satt upp de processer, riktlinjer, roller mm som krävs för att uppnå kravet i Tillitsramverket. Detta kan påvisas genom den dokumentation som Tillitsramverket kräver.

Nivå 4

Mogen. Verksamheten efterlever riktlinjer, processer och rutiner som verksamheten satt upp för att möta upp mot kravet i Tillitsramverket. Det finns även en fungerande process för ständig förbättring. Efterlevnaden kan påvisas genom den dokumentation som Tillitsramverket kräver.

Nivå 5

Världsklass. Verksamheten har väl inarbetade processer för att säkra tilliten. Riktlinjer, rutiner och processer övervakas och mäts regelbundet. Ständig förbättring är väl inarbetad och efterlevs i organisationen. Förbättringar analyseras med avseende på nytta och ledningssystemet är hållbart över tid.

Ej tillämbart

I det fall organisationen inte hanterar utgivning av elektroniska identitetshandlingar för funktion eller agerar ombud besvaras frågan med "Ej tillämbart" vilket motsvarar nivå 0 i spindeldiagrammet.



5. Uppdatera SITHS kontaktuppgifter vid förändring

Förändringar av Ansvarig utgivare, Säkerhetsansvarig och vilka organisationer som ingår i utgivningsområdet ska skyndsamt meddelas till SITHS PA via Inera.

Anmälan om förändringar görs här för att starta hanteringen i Easy:

<https://www.inera.se/tjanster/identifieringstjanst-siths/mer-om-tjansten/#af5e0846-c301-4fa8-8360-ee58cd96460f>

6. Easy

Här dokumenterar du bedömningen i tillitsdeklarationen och uppdaterar SITHS Kontaktuppgifter

6.1 Konto och inloggning i Easy

Ansvarig utgivare behöver ha ett konto i Easy med rollen Verksamhetsansvarig. Om Ansvarig utgivare vill ha ytterligare en eller flera personer som kan hjälpa till och besvara tillitsdeklarationen, ansöker man om rollen Sakkunnig för dessa personer.

Ansökan finns här:

<https://www.inera.se/kundservice/bestall--andra/bestall-easy/>

Logga in i Easy:

<https://www.inera.se/tjanster/kvalitetssystem-easy/Easy/#c287ee54-9454-4cec-8e13-27dd7a8644a5>

6.2 Handledning Easy

I Easy kommer du som Ansvarig utgivare att hantera tillitsdeklarationen samt SITHS kontaktuppgifter för ditt Utgivningsområde. Detta innebär att Ansvarig utgivare kommer att hantera två olika typer av Självdeklarationer enligt nedan.

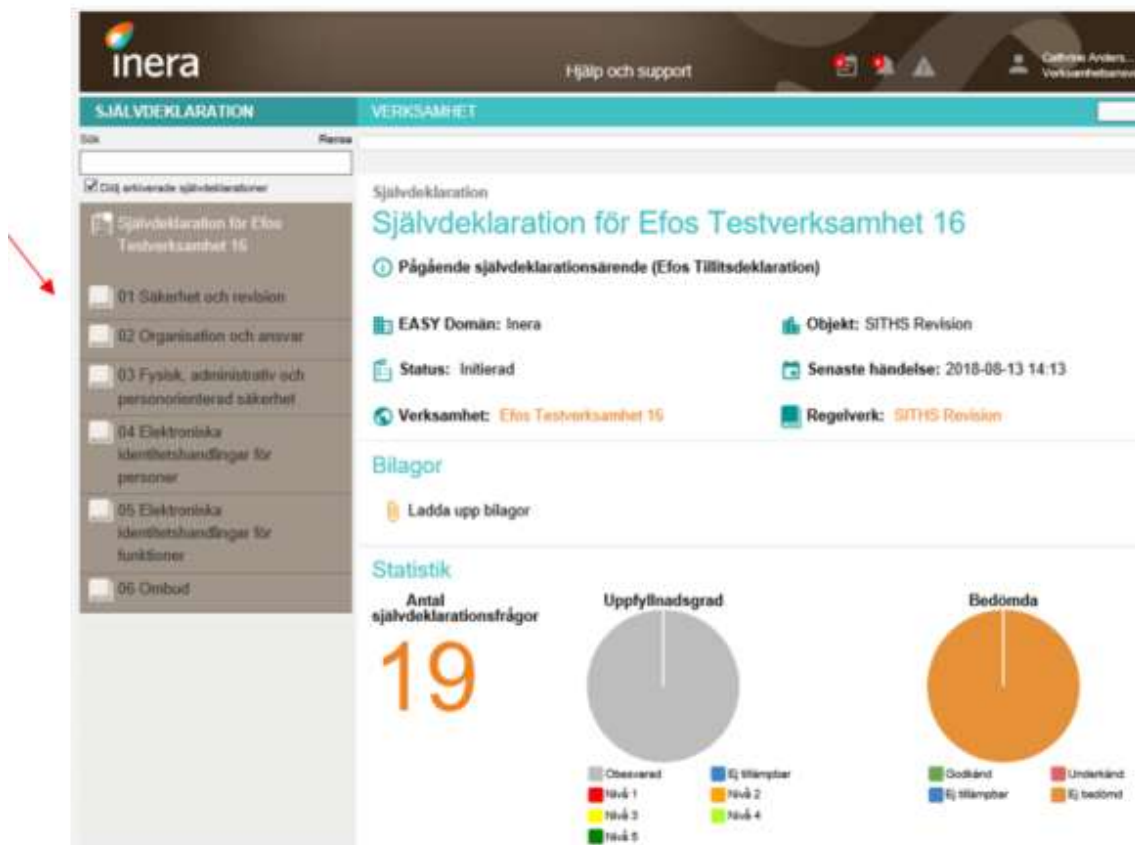




1. Öppna en självdeklaration genom att klicka på Självdeklaration för XXX



2. I menyn till vänster under "Självdeklaration för XXX", finns de frågor som du ska besvara i Självdeklarationen. Frågorna är indelade i olika kategorier. Klicka på valfri kategori (rubrik) och därefter klickar du på den fråga du ska besvara. Du kan själv välja i vilken ordning du vill besvara frågorna, och du kan även lämna frågor obesvarade och logga in vid ett senare tillfälle och fortsätta, men samtliga frågor måste vara besvarade för att du ska kunna skicka in självdeklarationen.





3. Frågorna besvaras genom att du gör en bedömning av hur väl din verksamhet uppfyller Tillitsramverket för aktuell fråga.
 - a. Bedömningen görs på en skala från 1–5, se punkt 4.1 för vägledning om nivåindelningen
 - b. Välj Nivå
 - c. Klicka på Spara
 - d. För vägledning samt hänvisning till Tillitsramverket, klicka på relaterad regel.

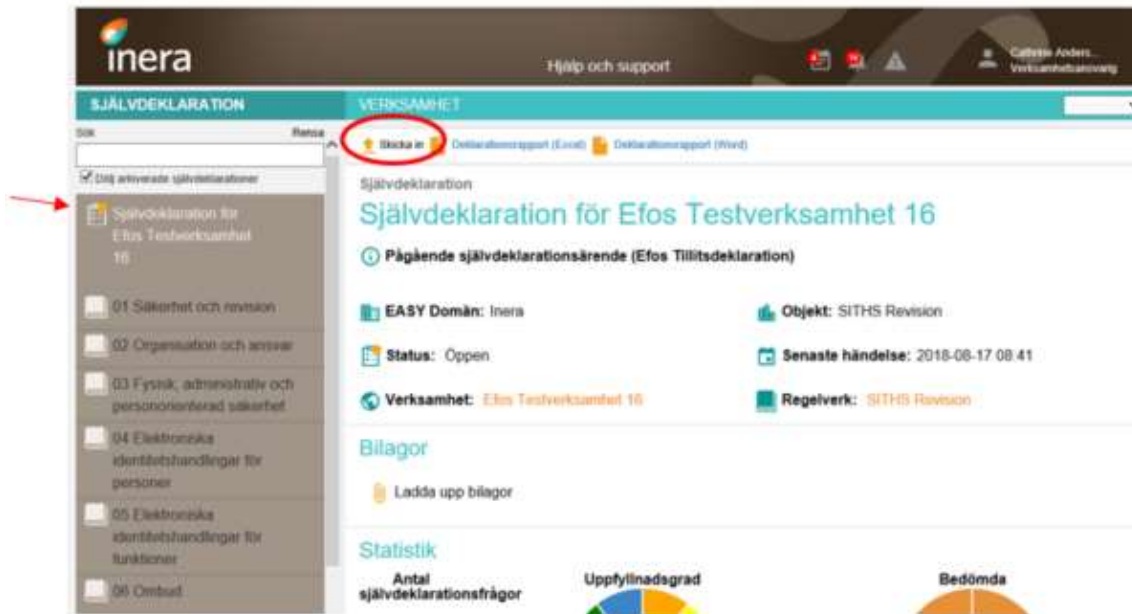
The screenshot shows the Inera web interface for a self-declaration. The main heading is 'Självdokumentation' and 'VERKSAMHET'. The current section is '01.1 Riskhantering'. The status is 'Obedömd'. A red circle highlights the 'Relaterad regel' link. A red arrow points from a text box containing guidance to this link. The text box contains the following text: 'Vägledning. Tillitsramverket kapitel 3.1 Informations säkerhet samt 3.3 Informations... Deklarationsfråga: Bedöm i vilken utsträckning process för riskhantering är implementerad i verksamheten (1-5) där 1 = Inte alls och 5 = Fullständig. Svarsfält: Uppfyllnadsgrad: Nivå 1, Nivå 2, Nivå 3, Nivå 4, Nivå 5, Ej tillämplig. Avbryt, Spara. Bilagor.

4. Du kan bifoga filer och skriva kommentarer i svarsfältet, men inget av detta är obligatoriskt i den Självdokumentation som hanterar **Tillitsdeklarationen**, men om behov finns så kan man använda funktionen för att förtydliga sitt svar och en förklaring till den bedömningen du gjort i aktuell fråga.

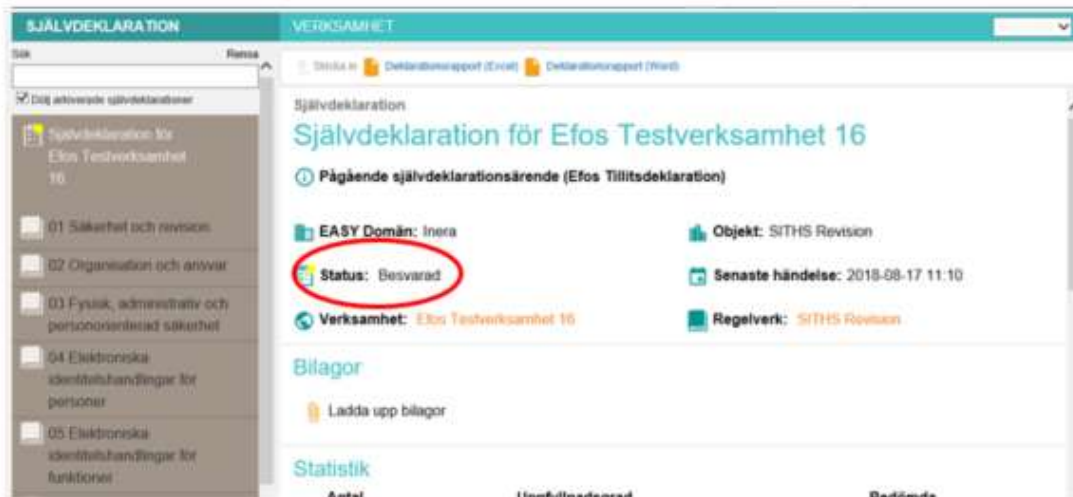
I Självdokumentation som hanterar **SITHS Kontaktuppgifter** är det obligatoriskt att ladda upp bilagor i de fall det efterfrågas i deklarafrågan.

Bilagorna ska namnges enligt den instruktion som finns i deklarafrågan

5. För att kunna skicka in en Självdokumentation måste alla frågorna vara besvarade
 - a. Klicka på "Självdokumentation för XXX".
 - b. Klicka på Skicka in.



6. Kontrollera att Självdeklarationen blivit inskickad
 - a. Klicka på ”Självdeklaration för XXX”.
 - b. Se statusen i rutan till höger, se figur nedan.



Status på självdeklaration: **Besvarad** = Självdeklarationen är inskickad.

Status på självdeklaration: **Öppen** = Självdeklarationen är ej inskickad.



7. Begäran om komplettering av Självdeklaration
I de fall något saknas eller du behöver utföra justeringar i dokumenten får du ett mejl från: no-reply@easy.sjunet.org.
 - a. Då måste du logga in i Easy och öppna din självdeklaration se rubriken Hantera Tillitsdeklarationen och kontaktuppgifter i Easy ovan.
 - b. Klicka på den rubrik där det är en röd cirkel.
 - c. I kommentarsfältet till höger, längst ner på sidan, finns information från granskaren om vad som behöver åtgärdas.

8. Godkänd Självdeklaration
När Självdeklaration är godkänd får du ett mail från: no-reply@easy.sjunet.org.
 - a. Du måste då logga in i Easy och ta del av godkännandet.
 - b. Klicka på ”Självdeklaration för XXX ”.
 - c. Statusen ska vara Godkänd
 - d. Se kommentaren i rutan till höger längst ner på sidan.

7. Rutin för personkontroller

Kontrollerna nedan görs med hänvisning till stycke 4.1 i Tillitsramverket

- Nuvarande anställning
- Lämplighet för tjänsten
- Legal lämplighet
- Finansiell lämplighet
- Genomförd utbildning för Ansvarig utgivare respektive Säkerhetsansvarig

7.1 Lämplighet och anställning

Använd mallen nedan för att skriva intyg om att du som Ansvarig utgivare är lämplig för rollen. Intygsgivare ska vara nivån direktör, kommunchef, vd eller motsvarande som kan representera organisationen.

Namnge dokumentet enligt följande: Förnamn_Efternamn_HSA-id_Lämplighet

”Härmed intygas att XX som är (ska bli) Ansvarig utgivare för organisation Y, är anställd hos oss samt är pålitlig och noggrann. Personen är väl lämpad för rollen som ansvarig för att organisation Y följer tillitsramverket och den kvalitetssäkrade utgivningsprocessen enligt det gemensamma regelverket.

Vi är införstådda med att med ansvaret följer administrativa och operativa arbetsuppgifter. Organisationen inser att rollen som Ansvarig utgivare omfattar ansvaret för utgivning av Elektroniska identitetshandlingar och att identifieringsprocessen följs inom vår organisation.”

XX=namn samt HSA-id eller personnummer

Intygsgivarnas underskrift



7.2 Legal lämplighet

Du som Ansvarig utgivare ska beställa ett registerutdrag ur belastningsregistret enligt 9§ 1st lagen om belastningsregister (1998:620). Du ska öppna utdraget i närvaro av säkerhetsansvarig för organisationen. Ansvarig utgivare visar upp samtliga sidor i utdraget så att säkerhetsansvarig kan läsa dem.

Du som Ansvarig utgivare behåller utdraget.

Använd mallen nedan för att visa att du som Ansvarig utgivare inte är legalt olämplig för rollen.

Intygsgivare ska vara Säkerhetsansvarig.

Namnge dokumentet så här: Förnamn_Efternamn_HSA-id_Belastningsregister

”Jag intygar att jag tagit del av registerutdraget för XX och intygar att utdraget inte innehöll något som gör XX olämplig som Ansvarig utgivare.”

XX=namn samt HSA-id eller personnummer

Säkerhetsansvarigs underskrift

7.3 Finansiell lämplighet

Inera kontrollerar, på uppdrag av SITHS PA, att du som Ansvarig utgivare inte har någon finansiell anmärkning som kan påverka tilliten.

Kontrollen görs hos Kronofogdemyndigheten och dokumenteras i Easy

7.4 Utbildning

Du som Ansvarig utgivare måste genomgå en utbildning innan du får din roll tilldelad.

Ett intyg på att du har genomgått en utbildning ska skickas in genom att i Easy ladda upp en kopia på kursintyget.

Följande utbildningsinstanser är godkända:

- Secure State AB
- Tjänsteansvarig SITHS

Namnge dokumentet enligt följande: Förnamn_Efternamn_HSA-id_Utbildning

8. Intern revision och förbättringsarbete

Ansvarig utgivare ansvarar för följsamheten till Tillitsramverket. För att följa upp detta ska den Säkerhetsansvarige för en direktansluten organisation ansvara för att det minst var 13:e månad genomförs en internrevision. Säkerhetsansvarige leder arbetet. Även eventuella tredjepartsanslutna ska omfattas av revision och under en treårsperiod ska samtliga tredjepartsanslutna ha blivit reviderade. De avvikelser som upptäcks ska resultera i en åtgärdsplan och ska planeras in och genomföras. Internrevision, åtgärdsplan och uppföljning ska dokumenteras och kunna visas upp vid en revision.

Använd gärna Ineras process för Risk, revision och förbättring samt de stöddokument och metoder som är beskrivna.

<https://www.inera.se/tjanster/identifieringstjanst-siths/mer-om-tjansten/#7b121e93-2205-497b-8bd8-4d93500d93a8>



Din organisation ingår i SITHS revisionsprogram av anslutna organisationer som är systematiskt och riskbaserat. Alla anslutna organisationer finns med i programmet och kommer att bli reviderade av Inera vid en på-platsen-revision.

9. Riskanalys

Ansvarig utgivare ska medverka i organisationens säkerhetsarbete och följa den process för riskhantering som används i organisationen. Du som Ansvarig utgivare ska säkerställa att riskanalyser genomförs inom ditt utgivningsområde och att identifierade risker leder till att förbättringsåtgärder vidtas och att önskad förbättring uppnås.

Riskanalys med åtgärdsförslag och uppföljning ska dokumenteras och kunna visas upp vid en revision.

Använd gärna Ineras process för Risk, revision och förbättring samt de stöddokument och metoder som är beskrivna.

<https://www.inera.se/tjanster/identifieringstjanst-siths/mer-om-tjansten/#7b121e93-2205-497b-8bd8-4d93500d93a8>

10. Säkerhetsincidenter – rapportering

Ansvarig utgivare ska agera vid misstanke eller bekräftat missbruk av certifikat.

Vid en säkerhetsincident, dvs. misstanke om eller bekräftat missbruk av elektronisk identitetshandling ska Ansvarig utgivare se till att:

- Spärra de inblandade certifikaten
- Starta en utredning om missbrukets omfattning
- Anmäla misstanke om, eller bekräftat missbruk av certifikat till Kundservice på telefon 0771-251010 eller via kundservice@inera.se
- Händelsen ska upprättas i en incidentrapport

11. Utbildning för ID-administratörer

Du som Ansvarig utgivare ansvarar för att säkerställa att ID-administratörer har relevant utbildning och den ska omfatta minst följande:

- Bakgrund översikt om SITHS regelverk
- Identifieringsprocessen inklusive genomgång av De sju stegen
- Kännedom om personer med skyddade personuppgifter
- Genomgång av flödet i SITHS Admin
- Genomgång av flödet i SCS
- Rutiner normalflöden SITHS
- Översiktligt om hur man blir godkänd som ID-administratör
- Översiktligt om revision enligt Revision, risk och förbättring

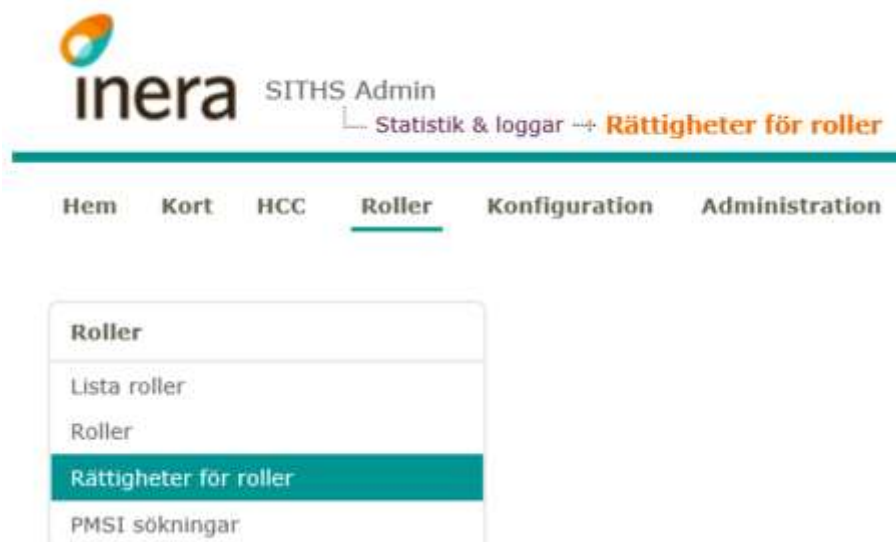


Utbildningen av ID-administratörer ska dokumenteras och kunna visas upp vid en revision. Utöver utbildning ska även personkontroller göras av blivande ID-administratörer enligt 4.2.1 i Tillitsramverket.

12. Beskrivning av roller inom SITHS

Beskrivning av ansvarsroller inom Identifieringstjänst SITHS så att du som Ansvarig utgivare ska kunna tilldela rätt roll i SITHS Admin.

Komplett matris med alla rättigheter för respektive roll finns i Statistik & Loggar





Förenklad matris över roller

Ansvarsroll inom SITHS	Ansvarig utgivare	Biträdande utgivare	ID-administratör	ID-administratör	Tilläggsroll För skyddade personuppgifter	Tilläggsroll För att läsa Korthistorik	Läs - Revisor
Tilldelas systemroll i SITHS Admin	RA	ORA	KRA	LRA	KUR	AO	ROA
Administrera reservkort	✓	✓		✓			
Administrera ordinarie kort och puk	✓		✓				
Administrera roller	✓	✓					
Administrera funktionscertifikat	✓	✓					
Administrera personer med skyddade personuppgifter	✓				✓		
Se rapporten korthistorik	✓					✓	✓
Se statistik och loggar	✓	✓	✓	✓	✓	✓	✓
Läsa ej administrera all information							✓

12.1 Tilldelning av roll kopplat till ID-administratörens arbetsuppgifter

Beroende på vad som ska ingå i ID-administratörens arbetsuppgifter kan man behöva kombinera flera systemroller. Matrisen ovan beskriver vad respektive systemroll har för behörighet.

Den ID-administratör som ska hantera användare med skyddade personuppgifter ska tilldelas tilläggsrollen KUR.

Exempel på kombinationer av systemroller beskrivs nedan.

1. ID-administratör som arbetar med utgivning av ordinarie kort och reservkort

- För att administrera ordinarie kort, tilldela
 - KRA
- För att administrera reservkort, tilldela
 - LRA

2. Biträdande utgivare som också arbetar med kortutgivning

- För att administrera reservkort, roller och funktionscertifikat, tilldela
 - ORA
- För att administrera ordinarie kort tilldela
 - KRA



- För att läsa rapporten korthistorik tilldela
 - AO

Tillgång till rapporten Korthistorik ger en utökad möjlighet till felsökning och att göra logguppföljningar.

3. Person i supportfunktion som arbetar med service till användare så som reservkortshantering och puk-beställningar

- För att administrera reservkort dvs, utfärda och avregistrera reservkort, tilldela
 - LRA
- För att beställa PUK, tilldela
 - KRA
- För att avregistrera ordinarie kort, tilldela
 - KRA

4. Revisor och Säkerhetsansvarig

För att en revisor, Säkerhetsansvarig eller annan lämplig person som ska följa upp att tilliten efterlevs eller att en supportroll har behov av att se uppgifter om användare, kort och certifikat

- För läsfunktion till hela utgivningsområdet, tilldela
 - ROA

13. Behörighet för ny ID-administratör

När ny ID-administratör ska få behörigheter behöver följande steg genomföras.

- Fyll i Bilaga 1.3 med information om:
 - Korttyper som ID-administratören ska vara behörig att beställa
 - Vilket/vilka kontor ID-administratören ska vara behörig att beställa till
 - Vilket/vilka kundnummer ID-administratören ska vara behörig att beställa på
 - Gäller det SIS godkända kort meddelas även DNV som uppdaterar organisationens tillstånd med den nya ID-administratören
- Skicka med e-post till siths@cygate.se

Cygate och Gemalto sätter upp rätt konfiguration för ovanstående beställning. DNV uppdaterar organisationens tillstånd och skickar till kunden. Detta kan ta ett par veckor.

- Ansvarig utgivare/Biträdande utgivare tilldelar rätt roll i SITHS Admin till den nya ID-administratören för aktuell organisation
- ID-administratören måste ha en e-postadress i certifikatet
- ID-administratören kan nu förbereda beställning i SITHS Admin
- För att kunna skicka iväg en beställning måste ID-administratören logga in med sitt personnummertcertifikat i SIS Capture station – SCS och ”hämtar kunduppgifter”. När



kunduppgifterna är hämtade enligt den uppdaterade konfigurationen ovan så har ID-administratören fått rättigheter att skicka iväg en elektronisk beställning med

- Korttyper enligt bilaga 1.3
- Organisation/kund enligt bilaga 1.3
- Till kontor enligt bilaga 1.3

14. Korttyper

Det finns ett antal beställningsbara korttyper. Deras grafiska och tekniska egenskaper beskrivs i SITHS Kortbilaga som återfinns här: <https://www.inera.se/kundservice/dokument-och-lankar/tjanster/identifieringstjanst-siths/>

Nya korttyper beställs via blankett Bilaga 1.1.1.

<https://www.inera.se/kundservice/dokument-och-lankar/tjanster/identifieringstjanst-siths/>

En ny korttyp enligt Bilaga 1.1.1 måste vara kopplad till behörighet för minst en ID-administratör enligt Bilaga 1.3.

15. Konfiguration i SITHS Admin

Förutsättningar

- Ansvarig utgivare är godkänd enligt uppdaterad SITHS kontaktuppgifter
- Har fått sitt första kort
- Behörighet i SITHS Admin tilldelade av Förvaltningsadministratör på Inera
- Innan kort- och certifikatbeställningar kan genomföras ska Ansvarig utgivare
 - Konfigurera organisationsparametrar
 - Konfigurera E-postmallar
 - Konfigurera kvittensmallar
 - Tilldela roller

15.1 Konfigurerar organisationsparametrar

Välj din organisation genom att klicka och markera organisationen i trädet





Ange uppgifter i respektive textfält:

- Rekommenderad giltighetstid för reservkort
 - Maximalt = 90 dagar (max 180 kan anges)
 - Standard = 30 dagar

Detta blir den giltighetstid som föreslås av SITHS Admin för HCC till reservkort. Det förvalda värdet bör vara lågt för att sen kunna ändras vid behov.

- Tid för påminnelse av SITHS certifikaten som är på väg att gå ut
 - Påminnelse om att certifikat som går ut sätts till ett lämpligt antal dagar så att medarbetaren hinner förnya sitt certifikat (kort).
- e-postadress till funktionsbrevlåda för utgivningsområdet

15.2 Konfigurera e-postmallar

För respektive e-postmall ange:

- e-postadress till funktionsbrevlåda för utgivningsområdet
- Ämne
- Meddelande

Se exempel på Ämne och Meddelande under punkt 30 i detta dokument ”Mallar för kvittens och e-post”.

Upprepa detta med samtliga e-postmallar.

Klicka på:

KONFIGURERA E-POSTMALLAR



Telia SITHS Admin v2.12.2.29

HCC Administration | Statistik & Loggar | HCS Beställningar

Organisation: Inera AB
Organisationsnummer: 556559-4230

HSA-id: SE165565594230-1000
E-postadress:

E-postmallar:

- Mail för påminnelse av utgående HCC
- Mail för e-post till NI vid massutbyte
- Mail för påminnelse massutbyte
- Mail för e-post till NI vid utbyte av HCC
- Mail för beställning av POCSE LE
- Mail för publikationenssläckande
- Mail för e-post till NI vid beställning av HCC

Avsändaradress:
infunktionen@inera.se

Ämne:
Påminnelse om SITHS kortets giltighetstid

Meddelande:
Hej!
Du har ett SITHS-kort med certifikat som ger dig tillgång till ett eller flera av Ineras verksamhetsstödande system. Ditt certifikats giltighetstid löper ut om

SPARA OCH SÖKA STÄNG

15.3 Konfigurera kvittensmallar

Klicka på konfigurerar kvittensmall

- Bläddra och Ladda upp logotyp
 - Logotypen skall vara av JPEG format och understiga 100 kb.
- Ämne
- Meddelande

Se exempel på Ämne och Meddelande i under punkt 30 i detta dokument ”Mallar för kvittens och e-post”

Upprepa detta med samtliga kvittensmallar.

Klicka på:

KONFIGURERA KVITTENSMALLAR

Telia SITHS Admin v2.12.2.29

HCC Administration | Statistik & Loggar | HCS Beställningar

Organisation: Inera AB
Organisationsnummer: 556559-4230

HSA-id: SE165565594230-1000
E-postadress:

Kvittensmallar:

- Mail för HCC Person
- Mail för HCC Org/Punk
- Mail för reservkort

Ladda upp logotyp (max 100kb):
Bläddra...

Nuvarande logotyp: 

Ämne:
Kvittens: Mottagande av SITHS kort

Meddelande:
Jag har mottagit mitt SITHS kort med e-legitimationer med korrekta uppgifter från Inera. Jag har också kontrollerat att uppgifterna på kortet överensstämmer och är sanningsenliga


SPARA OCH SÖKA STÄNG



15.4 Tilldela roll i SITHS Admin

Förutsättningar

Varje roll kan endast delegeras nedåt i en hierarkisk ordning. Rollen RA kan tex tilldela ORA, KRA LRA och KUR inom sin organisation. En ORA kan tex tilldela KRA och LRA. Olika roller kan tilldelas för olika organisationer.

- Sök person
- Klicka på:

- Leta upp och markera aktuella grenar
 - Välj roll/roller
- Signera och skicka
- Stäng

Person: Kerstin Arvedson



Anställda
Förnamn: Kerstin
Mellannamn:
Efternamn: Arvedson
Personnummer: ██████████
Yrkestitel:
Anställd fr.o.m. / t.o.m.: - / Tillsvidare
HSA-id: SE165565594230-12CF
E-postadress: kerstin.arvedson@inera.se



Tilldela/neka roll för administratör:
Välj en organisation i trädet till vänster

Välj organisationer i trädet:
Enhet Infrastruktur

TA BORT REHSA

Roll:
 RA AO ORA LRA KUR KRA LÄS

SIGNERA OCH SKICKA STÄNG

RA AO ORA LRA KUR KRA LÄS

Tips: Det går även att tilldela roll utifrån organisation

15.5 Ta bort roll i SITHS Admin

- Sök person
- Klicka på:

- Klicka på soptunnan för att ta bort roll för en person
- Signera och skicka
- Stäng

Kom ihåg att avbeställa ID-administratörens behörighet hos leverantören via bilaga 1.3, leverantören kommer i förekommande fall meddela DNV.



Tilldela/neka roll för administratör:
Valj en organisation i trädet till vänster

Valda organisationer i trädet:

TA BORT **RENSA**

Roll:
 RA AO ORA LRA KUR KRA LÄS

SIGNERA OCH SKICKA **STÄNG**

	RA	AO	ORA	LRA	KUR	KRA	LÄS
Inera AB				✓		✓	

Tips: Det går även att ta bort roll utifrån organisation

16. Beställa reservkort

Rollerna RA och ORA kan beställa reservkort

- Ange antal reservkort som skall beställas
- Välj Korttyp och ange Reservkort
- Ange aktuell kontorskod – dvs. motsvarande den adress som reservkortet ska levereras till
- Signera och skicka

Reservkortet med pinkoder levereras till utpekat kontor inom 5 dagar

Organisation: Inera AB
Organisationsnummer: 556559-4230

HSA-id: SE165565594230-1000
E-postadress:

Beställ reservkort

Antal kort:

Korttyp:

Kontorskod:

SIGNERA OCH SKICKA **STÄNG**



Återlämning och avregistrering

I samband med att ett SITHS-kort lämnas ut ska ID-administratören informera om att kortet ska återlämnas när personen slutar sin anställning/sitt uppdrag inom organisationen.

Kortinnehavaren ansvarar för att kortet återlämnas ituklippt genom chippet till ansvarig person enligt era lokala rutiner, t.ex. närmaste chef, så att kortet kan lämnas till ID-administratör för avregistrering. Kortinnehavaren kan också själv begära avregistrering av kortet genom att kontakta en ID-administratör.

Kortinnehavare som byter arbetsplats inom organisationen får behålla sitt SITHS-kort.

16.1 Ej återlämnade SITHS-kort

I de fall korten inte återlämnas ska kort och certifikat skyndsamt spärras av ID-administratör, dock senast inom 30 dagar efter anställningens avslut.

Använd gärna rapporten ”Giltiga kort för borttagna personer” under fliken Administration i statistik och loggar för att få fram personer som avslutat sin anställning/uppdrag. Gärna i kombination med kontrollkörning i HSA-portalen.

Alternativt används lokala rutiner för att hantera detta.

Kortet avregistreras som **Ej återlämnat**.

16.2 Ej utlämnade SITHS-kort

ID-administratörerna ska kontinuerligt gå igenom de SITHS-kort som ännu inte har lämnats ut och skicka påminnelse till berörda personer.

SITHS-kort som efter 3 månader fortfarande har status **Skickat** ska avregistreras med orsak **Ej utlämnat** och destrueras.

16.3 Spärr

I Tillitsramverket anges följande orsaker till spärr:

- Förhållanden som kan påverka certifikatsinnehållet har ändrats
- Någon uppgift i den elektroniska identiteten är eller misstänks vara felaktig
- Användaren har tappat kontrollen över bäraren eller koderna
- När bärare återlämnas
- När användaren inte längre har någon koppling till utgivande organisation
- När den elektroniska identiteten inte längre behövs

Exempel på när spärr ska göras:

- Ett pin/puk-brev upphittas av annan än kortinnehavaren
- Ett SITHS-kort upphittas av annan än kortinnehavaren



17. Giltiga kort för borttagna personer

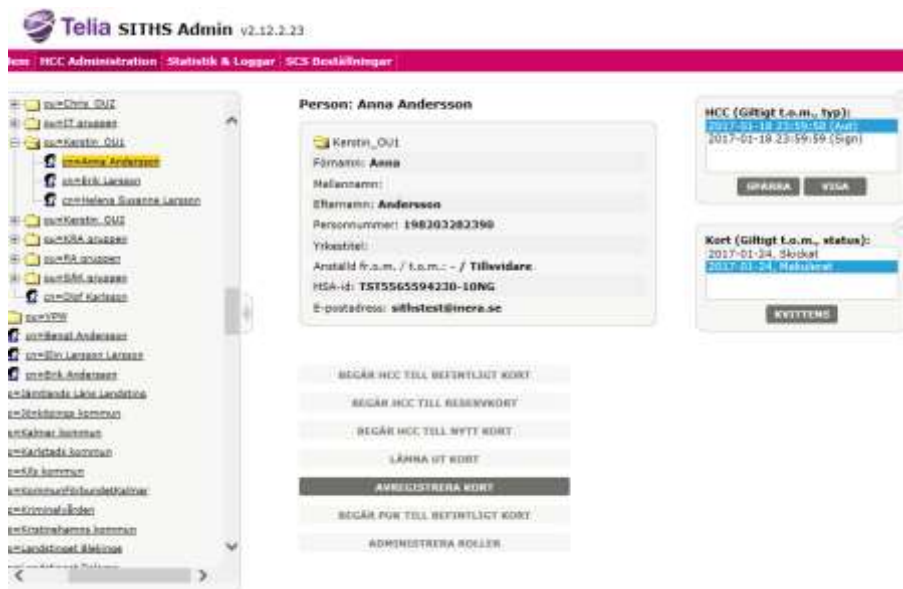
En persons objekt ska tas bort från HSA direkt när personen slutar, men då kan man inte se personobjektet i SITHS längre och därmed inte heller spärra certifikat eller avregistrera SITHS-kort.

För att underlätta en korrekt hanteringen finns det möjlighet att avregistrera SITHS-kort och certifikat i Statistik och Loggar (SoL) för personer som är borttagna i HSA.

För mer information om hanteringen i HSA för den här funktionen, se dokumentet ”Hantering av borttagna personer med giltiga HCC” som finns här:

<https://www.inera.se/kundservice/dokument-och-lankar/tjanster/hsa/>

Så här ser en person ut i SITHS Admin som har fått objektsklassen hsadeletedperson i HSA

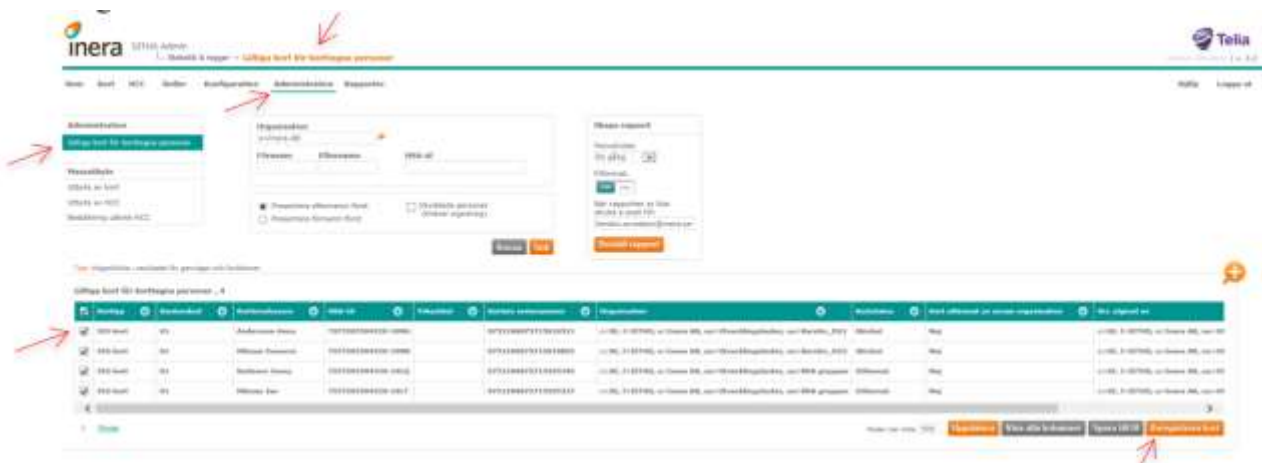


Du kan nu göra avregistreringar för flera personer samtidigt från den nya rapporten Giltiga kort för borttagna personer som ligger under fliken Administration

Välj din organisation och gör en sökning

Markera med kryssruta de personer som du vill avregistrera kort och HCC för.

Signera och skicka





Korrekt information syns i SITHS Admin direkt och dagen därpå i SoL

18. Skicka ordinarie kort mellan kontor

Förutsättningar

När ordinarie kort behöver transporteras mellan kontor och/eller ID-administratörer

- Korten ska skickas i ogenomskinligt och väl förslutet emballage vilket ska vara unikt identifierbart.
- Avsändaren är ansvarig intill att bekräftelse på mottagande kommit avsändaren tillhanda.
- Avsändaren är skyldig att föra förteckning över skickade kort vilka ännu inte är levererade och mottagningskvitterade.
- Mottagare är ansvarig för att postlåda eller motsvarande uppfyller SITHS krav på säkerhet, motsvarande ordinarie kortleverans.
- Rutinen dokumenteras i organisationens rutiner

Rutinbeskrivning

- Avsändaren noterar försändelsens identitet samt de förpackade kortens kortnummer
- Avsändaren meddelar mottagaren att en försändelse kommer att skickas med dess identitet samt kortnummer
- Mottagaren bekräftar ovanstående, samt att postlåda eller motsvarande uppfyller samma krav som ordinarie leverans från leverantör.
- Avsändaren skickar försändelsen med organisationens internpost
- Mottagaren kvitterar till avsändaren att försändelsen kommit fram samt att innehållet är identiskt med vad som tidigare uppgetts

Om försändelsen inte bekräftats som mottagen inom 5 arbetsdagar skall korten avregistreras genom Avsändarens försorg.

19. Arkivering av kvittenser

Regler kring arkivering, se Tillitsramverket

Elektroniska kvittenser av ordinarie kort lagras i SITHS Admin.

Arkivering av eventuella papperskvittenser skall ske under betryggande former så att kvittenserna kan tas fram i läsbart skick vid revision. Bevaras i tio år.

Skåp ska endast vara tillgängliga för register- och säkerhetsansvarig personal samt ID-administratörer.

Elektronisk arkivering är tillåtet om läsbarheten kan garanteras under hela perioden.

Kvittensen skapas och skrivs under på papper för att sedan skannas in. För att det ska vara tillåtet att förstöra originalet, det vill säga i detta fall pappret, måste det finnas ett fastställt gallringsbeslut.



Funktionscertifikat

Ett funktionscertifikat är en elektronisk identitetshandling, som identifierar en maskin/server eller en IT-funktion. Ett funktionscertifikat kan också användas för att signera e-post från funktionsbrevlådor.

Certifikatet skall hanteras som en värdehandling. Behörig personal (beställare, mottagare och Ansvarig utgivare/Biträdande utgivare) går i god för certifikatets riktighet och att det inte hamnar i obehörigas händer.

Förutsättningar:

- Funktionscertifikat kan beställas för domännamn och/eller e-postadresser under noden dc=Services i SITHS Admin
- Krävs att Ansvarig utgivare eller Biträdande utgivare har behörighet i tjänsteträdet.
- Organisationen ska ha en gren för utfärdande av funktionscertifikat i HSA tjänsteträd
- Konfiguration av organisationsparametrar, e-post- samt kvittensmallar ska göras i SITHS Admins tjänsteträd.
- Ansökan för organisation om att få gren upplagd i HSA görs via ansökningsformulär på inera.se.
- Domän- och e-postvalidering för organisationen ska skickas in och vara godkänd av SITHS Policy Authority
- Om utfärdande utgivningsområde inte äger domännamnet eller e-postadressen ska domänvalideringen kompletteras med en fullmakt
- Vid behov ska Ansvarig utgivare ha tilldelat roll till Biträdande utgivare i tjänsteträdet
- Dokumenterad rutin ska finnas hos organisationen
- Om organisationen ska använda elektroniska blanketter och/eller elektronisk signering ska detta beskrivas i rutinen, inklusive hur spårbarhet uppnås

För att Ansvarig utgivare/Biträdande utgivare ska kunna utfärda SITHS funktionscertifikat krävs att:

- Blanketten ”Beställning av SITHS funktionscertifikat” är korrekt ifylld, undertecknad och lämnad till Ansvarig utgivare/Biträdande utgivare. En blankett krävs alltid oberoende om det är nyutfärdade eller förnyelse av ett certifikat.
- Certifikatsigneringsbegäran (CSR) på fil är tillgänglig för Ansvarig utgivare/Biträdande utgivare
- Funktionscertifikatsbeställare har mandat att beställa certifikat för sin organisation
- Mottagaren ska identifieras vid ett personligt möte med Ansvarig utgivare/Biträdande utgivare. Om Ansvarig utgivare/Biträdande utgivare tidigare har identifierat mottagaren kan funktionscertifikatet överlämnas utan ett personligt möte. Vid elektronisk kvittens så kontrolleras att den ansvarige mottagaren har signerat med sitt SITHS certifikat, vilket medför att det inte behövs något personligt möte.



19.1 Gör så här för att skapa och leverera funktionscertifikat

Beställning av HCC funktion (PKCS#10)

- Kontrollera om möjligt i en CSR-decoder¹ att namnet (commonName) i CSR stämmer med funktionsobjektet
- Sök i SITHS Admin efter funktionen som ska finnas i HSA:s tjänsteträd (dc=Services)
- Klicka på funktionen och välj ”Beställ HCC Funktion (PKCS#10)”

Funktion: RBMuse002.reg.skane.se

HSA-id: SE162321000255-F12060

E-postadress:

BESTÄLL HCC FUNKTION (PKCS#10)

- Leta efter ansvarig mottagare i organisationsträdet och klicka på namnet.
- Välj något av nedanstående alternativ
 - Legitimering
 - Underskrift
- Ange giltighetstiden max 2 år
- Ladda upp den levererade CSR-filen

Funktion: RBMuse002.reg.skane.se

HSA-id: SE162321000255-F12060

E-postadress:

Beställ HCC Funktion (PKCS#10)

Ansvarig:
Kerstin Hörstedt

HCC-användning:
 Legitimering
 Underskrift

Giltig t.o.m.:
2019 11 28

PKCS 10 Data:
[L:\Koncernkontoret\Av] [E:\G002]

SIGNERA OCH SKICKA **STÄNG**

- Klicka på ”Signera och Skicka”
- SITHS Admin kontrollerar att nyckellängden är minst 2048 bitars RSA
- Välj ”Ladda ned PKCS#10”. Spara filen med funktionens namn eller HSA-id på lämplig plats.
- Skriv ut kvittensen, fysiskt eller elektroniskt. I undantagsfall så kan alternativet ”Känd” användas om personen tidigare har identifierats personligen med en giltig identitetshandling. När mottagare elektroniskt signerar dokumentet ska Ansvarig utgivare/Biträdande utgivare markera alternativet ”Identifierad genom rekommenderad post”.

¹ Till exempel <https://certlogik.com/decoder/>



- Om utlämningen genomförs på distans ska mottagaren av certifikatet ha återsänt den underskrivna kvittensen innan certifikatfilen levereras till den ansvarige mottagaren.
- lämna ut certifikatet till ansvarig mottagare.

19.2 Arkivera kvittens

Arkiveringen skall ske i låsbart skåp eller, när det gäller elektroniska beställningar och kvittenser, på en nätverksenhet som kontinuerligt säkerhetskopieras.

De ska endast vara tillgängliga för register- och säkerhetsansvarig personal samt ID-administratörer.

Kvittensen ska sparas tillsammans med beställning och ev. fullmakt i minst 10 år.

20. Domänvalidering

Förutsättningar:

- Direktansluten organisation äger delegerad rätt av SITHS CA att utfärda certifikat till domäner och/eller e-postadresser inom utgivningsområdet.
- Direktansluten organisation får utfärda certifikat till en domän och/eller e-postadress som ägs av en annan organisation om nyttjanderätten till i certifikatnamnet ingående domännamn och e-postadresser skriftligt styrkts som ska kunna visas upp vid en revision
- SITHS PA ansvarar för att ägarskapet för domänen kontrolleras innan registrering samt därefter regelbundet.
- Om SITHS PA vid domänkontrollen upptäcker frågor kring ägarskap, kontaktas Ansvarig utgivare för aktuellt utgivningsområde.
- Om det inte går att bevisa att organisationen äger domänen kommer eventuellt utfärdade certifikat att revokeras, samt rättigheten att utfärda nya tas bort.

SITHS PA säkerställer att:

- Relevanta ansökningsblanketter har skickats till kundservice@inera.se. Det ska finnas en ansökningsblankett för varje ”o”.
- Validering sker av varje anmälan och endast godkända hanteras vidare
- Person som har skickat in domänvalideringen är Ansvarig utgivare
- Utgivningsområdet är upplagd i HSA:s tjänsteträd
- Godkänd domän läggs upp i SITHS Admin
- Återkoppling till kund sker
- Kontroller av fortsatt ägarskap av domänen görs regelbundet



Gör så här för att anmäla domäner

Domäner och e-postadresser som er organisation äger

- Fyll i ”Blankett anmälan domän och e-postvalidering SITHS” vilka domäner och/eller e-postdomäner som er organisation vill utfärda funktionscertifikat till.
- För .sjunet.org domän krävs att organisationen har ett giltigt Sjunet avtal
- Skicka anmälan till kundservice@inera.se

För domäner och e-postadresser som er organisation inte äger tillkommer

- Om de domäner och/eller e-postadresser som er organisation vill utfärda certifikat till ägs av en annan organisation ska Ansvarig utgivare säkerställa att det finns en fullmakt från den ägande organisationen

Kontroller som utförs i samband med validering

På uppdrag av SITHS PA kontrollerar Inera att den organisation som är registrerad som ägare till domänen eller e-postdomän ger sitt medgivande till att utgivningsområdet får utfärda funktionscertifikat för aktuell domän. Valideringens utfall är beroende av det svar som fås vid kontrollen.

För domäner utförs kontrollen antingen genom:

- E-post
Inera skickar e-post till någon av följande e-postadresser som efterföljs av @<domänen som ska valideras>
 - admin, administrator, webmaster, hostmaster eller postmaster
- DNS-post
 - Skapa en txt-post vid namn ”_sithsvalidation” i domänens DNS-zonfil med ett värde som Inera tillhandahåller
- Webbsida
Ladda upp en txt fil vid namn ”sithsvalidation.txt”, med innehåll som Inera tillhandahåller, på servern:
<http://www.exempel.se/.well-known/pki-validation/>

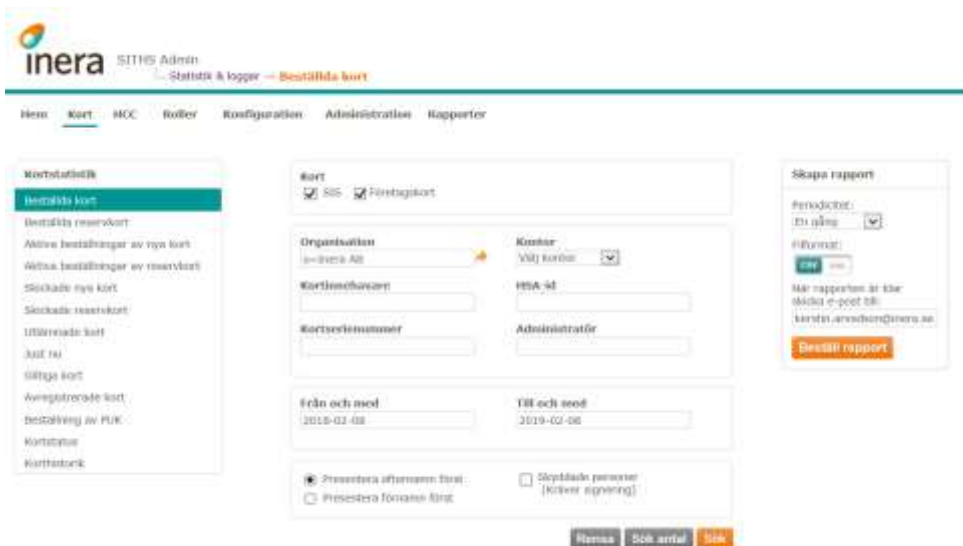
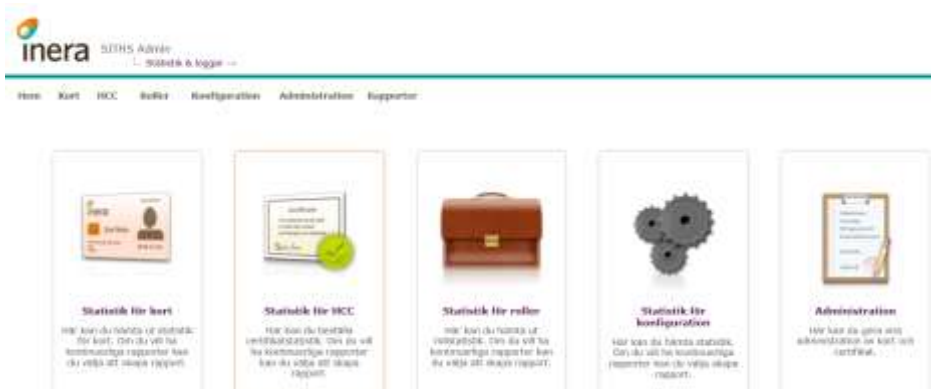
21. Statistik och loggar

Rapporter kan beställas online och offline under menyval ”Statistik & Loggar”.

Offlinerapporterna är tillgängliga dagen efter beställning.

Rapporter finns för

- Kort (uppföljning av kort)
- HCC (uppföljning av certifikat)
- Roller (uppföljning av tilldelade roller inom organisationen)
- Konfigurering (uppföljning av konfigurationsändringar)
- Administration (uppföljning av borttagna personer)



Tips: De färdiga offlinerapporterna finns att hämta under menyn Rapporten dagen efter beställningen

21.1 Användningsområden för olika rapporter

21.1.1 Hitta ordinarie SITHS-kort med status = Skickat

Logga in i Statistik & loggar

<https://cve.trust.telia.com/SOL/>

- Välj:
 - Statistik för kort





- Välj rapport
 - **Just nu**
- Gör följande urval:
 - Kort = Företagskort och eller SIS-kort beroende på vilka kort ni har
 - Organisation = Din organisation
- Giltiga HCC = Ja
- Kort status = Skickat
- Tryck på Sök

- Sortera rapporten på tidpunkt, genom att klicka på rubriken Tidpunkt

Tips! Högerklicka i resultatet för genvägar och funktioner.

Just nu, 12

Tidpunkt	Korttyp	Kontorskod
2018-01-12 00:00:00	Företagskort utan foto	01
2019-08-22 00:00:00	Företagskort utan foto	01
2019-08-22 00:00:00	Företagskort utan foto	01
2019-09-02 00:00:00	Företagskort utan foto	01

- Spara din sökning till fil för att på ett lätt sätt kunna arbeta med rapporten
 - Tryck på Spara till fil

Rader per sida: 20 **Uppdatera** Visa alla kolumner **Spara till fil**

- Spar filen i Excell format.



- Filtrerar fram de kort som innehåller din organisationens utfärdarnummer.
 - Utfärdarnummer har position 5–8 i kortserienumret
Ex. 9752 **2698** 85708335630
- Säkerställ att de kort som du har i din rapport med status skickat finns på kortkontoret.
- Samtliga kort som har status skickat som **inte** finns på kortkontoret, **ska spärras** omgående och nytt kort ska beställas till användaren och lämnas ut enligt gällande rutin av en ID-administratör

Om rapporten är för stor så kan du beställa en offlinerapport som finns att hämta nästkommande dag under rubriken Rapporter

The screenshot shows the Inera SITHS Admin web interface. The navigation menu includes 'Hem', 'Kort', 'HCC', 'Ruller', 'Konfiguration', 'Administration', and 'Rapporter'. The 'Rapporter' section is active. On the left, there is a sidebar with 'Kortstatistik' and various options like 'Beställ kort', 'Aktiva beställningar av nya kort', etc. The main content area has a 'Kort' section with filters for 'SIS', 'Företagskort', and 'Reservkort'. Below this are fields for 'Organisation', 'Kontor', 'Förnamn', 'Efternamn', 'HSA-id', 'Kortserienummer', and 'Giltiga HCC'. There is also a 'Yrkestitel' dropdown. The 'Kortstatus' section has checkboxes for 'Beställt', 'Skickat', 'Utlämnat', 'Mottaget', 'Avregistrerat', and 'Makulerat'. At the bottom, there are radio buttons for 'Presentera efternamn först' and 'Presentera förnamn först'. A 'Rensa' button and a 'Sök' button are at the bottom right. A red box highlights the 'Skapa rapport' form on the right, which includes a 'Periodiskt' dropdown set to 'En gång', a 'Påformat' dropdown, and a text field for 'När rapporten är klar skicka e-post till:' with the email 'cathrine.anderson@inera.se'. A red arrow points to the 'Beställ rapport' button.

22. Regler vid verksamhetsövergång och ägarbyte

Förutsättningar

Ett ombud definieras som direktansluten organisation som på uppdrag av en tredjepartsansluten organisation administreras och ansvarar för den tredjepartsanslutna organisationens kort och certifikat i Identifieringstjänst SITHS.

För direktanslutna ska Anslutningsavtal finnas skrivet med Inera AB. För tredjepartsanslutna, som är separata juridiska personer med egna organisationsnummer, ska ett Tredjepartsavtal finnas med det direktanslutna ombudet.

Ombudet har en godkänd tillitsdeklaration och äger därmed rätt att, efter godkännande av SITHS PA, ansluta annan organisation inom offentlig förvaltning samt leverantörer av tjänster till dessa ("Tredje Part") till SITHS.



22.1 Regler gällande utfärdarnummer

Regler för SIS-kort, se punkt 28.4.

22.1.1 Organisationen äger sitt eget utfärdarnummer:

Den organisation vars utfärdarnummer finns på kortet ansvarar för korten under dess livstid. Kort med utfärdarnummer kan via avtal överlåtas vid en verksamhetsövergång.

22.1.2 När ett ombuds utfärdarnummer har använts vid utfärdande av SITHS-kort:

- Den organisation vars utfärdarnummer finns på kortet ansvarar för korten under dess livstid
- Vid byte av ombud eller övergång till direktanslutning är det den organisation som äger utfärdarnumret som bestämmer om administrationen av befintliga kort kan föras över till annan organisation eller om korten ska spärras. Detta regleras med fullmakt eller genom en skrivning i tredjepartsavtalet.
- I de fall där kortadministrationen har överförts, ska ägaren av utfärdarnumret kunna utföra revision på sina kort hos det nya ombudet.
- Det nya ombudet ska tillse att ombudets, eller tredjepartsorganisationens egna, utfärdarnummer används vid utfärdande av nya kort.

23. Namnbyte av organisation

En organisation byter namn, men har kvar samma organisationsnummer och eventuellt HSA-id.

- Ev. byte av logga
- Uppdatering av SITHS kontaktuppgifter i Easy

24. Lägga ner utgivningsområde

- Säga upp avtal hos Inera
 - Ta bort behörigheter i SITHS Admin
- Säkra att utgivningsområdets kort samt SITHS funktionscertifikat är spärrade

Övrigt att tänka på:

- Se över eventuellt eget supportavtal för Net iD
- Vid behov säg upp alla tredjepartsavtal
- Säg upp avtalet med Cygate
- Vid utfärdande av SIS-kort anmäl hos DNV att SITHS-kortutfärdande ska upphöra



25. Från tredjepartsanslutning till direktanslutning

- Teckna eget avtal med Inera AB
- Besvara tillitsdeklarationen, skriv rutiner och utför personkontroll
- Säga upp avtalet med befintligt ombud
- Reglera ansvarsfrågan gällande SITHS certifikat gentemot det gamla ombudet genom ett avtal
- Reglera ansvarsfrågan gällande korten gentemot ombudet genom ett avtal, vars utförning beror på:
 - Om organisationen har eget utfärdarnummer
 - Om organisationen har använt ombudets utfärdarnummer

26. Byte av ombud/Övergång till ombud

26.1 Tredjepartsansluten organisation som vill byta ombud

26.1.1 Tredjepartsansluten organisation

Aktiviteter att genomföra:

- Säga upp befintligt avtal med nuvarande ombud
- Teckna nytt avtal med det nya ombudet
- Teckna avtal om ansvarsfördelning för kort, SITHS personcertifikat samt i förekommande fall SITHS funktionscertifikat, mellan det gamla ombudet och det nya. Avtalet ska tecknas mellan alla tre parter. Om avtal ej tecknas ska kort och certifikat spärras.

Övrigt att tänka på:

- Vid utfärdande av SIS-godkända kort – se punkt 28.4.

26.1.2 Avgående ombud

Aktiviteter att genomföra:

- Teckna avtal om ansvarsfördelning för kort, SITHS personcertifikat samt i förekommande fall SITHS funktionscertifikat, mellan det gamla ombudet och det nya. Avtalet ska tecknas mellan alla tre parter. Om avtal ej tecknas ska kort och certifikat spärras
- Kvittenser för redan utgivna kort ska sparas hos det avgående ombudet
- Ta bort behörigheter i SITHS Admin
- Anmäl till SITHS PA att organisationen inte längre ska agera ombud genom att uppdatera kontaktuppgifterna
- Se till att nya ombudet anger korrekt utfärdarnummer

26.2 Direktansluten organisation som byter till ombud

26.2.1 Direktansluten organisation

Aktiviteter att genomföra:

- Säga upp befintligt avtal med Inera AB



- Teckna avtal med ett ombud
- Ansvara för att teckna avtal med ombudet om ansvarsfördelningen för kort, SITHS personcertifikat samt i förekommande fall SITHS funktionscertifikat. Om avtal ej tecknas ska kort och certifikat spärras
- Ta bort behörigheter i SITHS Admin
- Vid fortsatt utfärdande av SIS-godkända kort, ansök om att ombudet ska få utfärda SIS-godkända kort. Tillträdande ombud måste vara godkänd som SIS-kortutfärdare hos DNV. Se även punkt 28.4.

26.2.2 Tillträdande ombud

Aktiviteter att genomföra:

- Anmäl till SITHS PA att organisationen ska agera ombud genom att uppdatera kontaktuppgifterna
- Teckna avtal med organisationen som ska vara tredjepartsansluten
- Teckna avtal om ansvarsfördelning för kort, SITHS personcertifikat samt i förekommande fall SITHS funktionscertifikat, mellan det gamla ombudet/organisationen och det nya ombudet. Avtalet ska tecknas mellan alla tre parter. Om avtal ej tecknas ska kort och certifikat spärras.

27. Verksamhetsövergång

27.1 Direktansluten organisation övertas men lever kvar med eget organisationsnummer

En icke ansluten organisation har övertagit en direktansluten organisation och den direktanslutna organisationen lever kvar och behåller sitt organisationsnummer.

- Se ”Byte av ombud/Övergång till ombud”

Den övertagande organisationen kan ansöka att bli tredjepartsansluten via den direktanslutna organisationen

27.2 Direktansluten organisation övertas och upphör

En icke ansluten organisation har övertagit en direktansluten organisation och den direktanslutna organisationen och organisationsnumret upphör. Hanteras som en nedläggning av ansvarig utgivares område

- Se ”Lägga ner utgivningsområde”.

27.3 Direktansluten övertar en tredjepartsansluten

En direktansluten organisation tar över en tredjepartsansluten organisation

- Regler Se ”Byte av ombud/Övergång till ombud”



27.4 Utfärdade SIS-kort

- Myndigheter, regioner, kommuner och privata aktörer får utfärda SIS-kort inom sin egen organisation
- Regioner, kommunförbund och kommuner kan enligt dispens agera ombud åt varandra. Om en region, ett kommunförbund eller en kommun agerar ombud, kan tredjepartsansluten region eller kommun ansöka om att uppdatera sitt DNV-tillstånd med det nya ombudet som utgivare hos DNV och därmed kunna ha SIS-kort utan att själva vara direktanslutna till SITHS. Notera att tillträdande ombud måste vara godkänd som SIS-kortutfärdare hos DNV.
- Vid övriga kombinationer av ombud och tredjepartsansluten organisation får inte ombudet utfärda SIS-kort till annan organisation än sin egen
- Vid övergång till ett ombud, kan organisationen med eget tillstånd hos DNV välja att behålla redan utfärdade kort

28. Ombud och tredjepartsanslutning

Vid förändringar ska SITHS kontaktuppgifter uppdateras via Easy.

Kunden kan efter SITHS PA:s skriftliga och uttryckliga godkännande ansluta en annan organisation (ett 'o' i HSA-katalogen) som bedriver vård- eller omsorgsverksamhet. När Kunden ansluter en sådan annan organisation till SITHS kallas Kunden "Ombud" och den organisation som ansluts "Tredje part".

Vid Ombudets anslutning av Tredje part ansvarar Ombudet för att Tredje part uppfyller SITHS tillitsramverk. Ombudets revisioner ska även omfatta Tredje part. Tredje Part äger inte rätt att ansluta annan organisation till Tjänsten.

29. Mallar för kvittenser och e-post

29.1 E-postutskick

Detta avsnitt visar några exempel på hur en e-postmall kan se ut för olika situationer som hanteras i administrationen av SITHS-kort.



29.1.1 Påminnelse av utgående certifikat

När SITHS-kortets giltighetstid närmar sig utgångsdatum måste kortinnehavaren meddelas för att få ett nytt certifikat. Ett exempel på hur ett sådant e-postmeddelande kan se ut visas nedan:

Hej,

Det är dags att förnya ditt SITHS-kort. För att kunna göra det måste du kontakta ID-administratören i din organisation, senast inom 30 dagar.

Namn: {\$certSubjectDn}

Kortnummer: {\$certCardNumber}

Kortet är giltigt till {\$certNotValidAfter}

Om du har några problem eller frågor angående ditt SITHS-kort, var vänlig kontakta ID-administratören.

Vänliga hälsningar,

ID-administratören

29.1.2 Beställning av nytt certifikat

Vid beställning av ett nytt certifikat till SITHS-kort eller till ett reservkort måste kortinnehavaren meddelas detta. Ett exempel på hur ett sådant mail kan se ut visas nedan:

Hej,

*Du har nu ett certifikat att hämta till ditt SITHS-kort. Välj den länk nedan som motsvarar din anslutningsväg och logga in med din e-legitimation för att hämta ditt nya certifikat. **Tänk på att först sätta i ditt SITHS-kort i kortläsaren!***

Om du ansluter via Internet, klicka på denna länk:

<https://cve.trust.telia.com/ccu>

Om du ansluter via Sjunet, klicka på denna länk:

<https://ccu.trust.telia.com/ccu>

Om du har några problem eller frågor angående ditt SITHS-kort, var vänlig kontakta ID-administratören i din organisation

Vänliga hälsningar,

ID-administratören

29.1.3 Misslyckad publicering av certifikat

Det kan hända att publiceringen av certifikat misslyckas. I sådana fall skickas ett meddelande till den angivna funktionsbrevlådan. Ett exempel på hur ett sådant e-postmeddelande kan se ut visas nedan:

Tyvärr har publicering av ett certifikat misslyckat. Detta kan bero på att HSA inte varit tillgänglig eller att uppgifterna för certifikatet har ändrats eller tagits bort. Det kan även bero på tekniska problem som skrivrättigheter till organisationens HSA-katalog.

Certifikatet tillhör: {\$SubjectDn} med HSA-ID {\$HsaId}



Vänligen kontrollera med HSA – administratören att uppgifterna stämmer. För att eventuellt kunna publicera certifikatet manuellt bifogas här en Base64-kodad version av certifikatet nedan. För personcertifikat, använd publiceraknappen i SITHS admin.

Felmeddelande: `{ $ErrorMessage }`

Möjlig orsak till felet: `{ $PossibleReason }`

`{ $Certificate }`

29.2 Kvittenser

Detta avsnitt visar några exempel på hur en kvittensmall kan se ut i olika situationer som ID-administratören hanterar i administrationen av SITHS-kort

29.2.1 Ordinarie kort

För att kortinnehavaren ska kunna ta emot sitt SITHS-kort måste denne kvittera mottagandet. Ett exempel på hur en sådan kvittens kan se ut visas nedan:

Jag har tagit del av och är införstådd med vilka regler som gäller vid användning, hantering och förlust av min elektroniska identitetshandling och de tillhörande koderna.

Kort och elektronisk identitetshandling med tillhörande koder är personliga. De ska hanteras som värdehandlingar vilket innebär att kort och koder ska förvaras åtskilda.

Jag har mottagit mitt SITHS-kort och förbinder mig att återlämna kort och den elektroniska identitetshandlingen när jag slutar min anställning/uppdrag inom [organisationen].

För fullständiga villkor se dokumenten ”Allmänna villkor för SITHS e-id” samt ”Villkor för Telia e-legitimation” som finns tillgängliga på <https://www.inera.se/siths/repository>

`{ $B }Mottagarens namn{ $/B }:` `{ $TargetName }`

`{ $B }Mottagarens personnummer{ $/B }:` `{ $PersonalNumber }`

`{ $B }Mottagarens HSA-id{ $/B }:` `{ $TargetHSAID }`

`{ $B }Kortserienummer{ $/B }:` `{ $SerialNumber }`

`{ $B }Kortet/certifikatet är giltigt{ $/B }:` `{ $CertValidFrom }` - `{ $CertValidTo }`

Ovanstående villkor intygas.

`{ $B }Ort och datum{ $/B }`

`[Ort], { $Date }`

`{ $B }Underskrift mottagare{ $/B }`

`{ $B }Namnförtydligande{ $/B }`

`{ $TargetName }`

Personen ovan har vid mottagandet av tjänstelegitimation identifierats med giltig identitetshandling.

`{ $B }Handläggarens HSA-id:{ $/B } { $XraHSAID }`

`{ $B }Ort och datum{ $/B }`

`[Ort], { $Date }`



{B}Underskrift handläggare {B}

{B}Namnförtydligande{B}
{XraName}

29.2.2 Funktionscertifikat

Mottagaren av ett funktionscertifikat måste kvittera att denne har tagit emot det. Ett exempel på hur en sådan kvittens kan se ut visas nedan:

Jag har mottagit ett funktionscertifikat för nedan angiven funktion ifrån [organisationen]. Jag har kontrollerat att de uppgifter som står i funktionscertifikatet överensstämmer med de uppgifter som står i certifikatets ansökan.

Jag är införstådd med vilka regler som gäller vid användning, hantering och eventuell förlust av funktionscertifikatet och förbinder mig att begära spärr av det när det inte längre används.

Jag förbinder mig att, i det fall ansvaret för detta funktionscertifikat lämnas över till annan person, att meddela detta till [organisationen].

Identifiering vid utlämnande:

{IDENTIFICATION}

{B}Funktions/Organisationscertifikatets namn{B}: {OrgFuncRDN}

{B}Funktions/Organisationscertifikatets HSA-id{B}: {OrgFuncHSAID}

{B}Certifikatets serienummer{B}: {SerialNumber}

{B}Certifikatet är giltigt{B}: {CertValidFrom} - {CertValidTo}

{B}Mottagarens namn{B}: {TargetName}

{B}Mottagarens HSA-id{B}: {TargetHSAID}

Ovanstående villkor intygas.

{B}Ort och datum{B}

[Ort], {Date}

{B}Underskrift mottagare{B}

{B}Namnförtydligande{B}
{TargetName}

{B}Handläggarens HSA-id{B} {XraHSAID}

{B}Ort och datum{B}

[Ort], {Date}



{B}Namnförtydligande{/B}
{XraName}

29.2.3 Reservkort

För att kortinnehavaren ska kunna ta emot sitt reservkort måste denne skriftligen kvittera mottagandet. Ett exempel på hur en sådan kvittens kan se ut visas nedan:

Jag har tagit del av och är införstådd med vilka regler som gäller vid användning, hantering och förlust av min elektroniska identitetshandling och de tillhörande koderna.

Kort och elektronisk identitetshandling med tillhörande koder är personliga. De ska hanteras som värdehandlingar vilket innebär att kort och koder ska förvaras åtskilda.

Jag har mottagit mitt reservkort och förbinder mig att återlämna kort och den elektroniska identitetshandlingen när jag slutar min anställning/uppdrag inom [organisationen].

För fullständiga villkor se dokumentet "Allmänna villkor för SITHS e-id" som finns tillgängligt på <https://www.inera.se/siths/repository>

{B}Mottagarens namn:{/B} {TargetName}
{B}Mottagarens personnummer:{/B} {PersonalNumber}
{B}Mottagarens HSA-id:{/B} {TargetHSAID}
{B}Kortnummer:{/B} {SerialNumber}

Ovanstående villkor intygas.
{B}Ort och datum{/B}
[Ort], {Date}

{B}Underskrift mottagare{/B}

{B}Namnförtydligande{/B}
{TargetName}

Personen ovan har vid mottagandet av reservkort och tjänstelegitimation identifierats med giltig identitetshandling.

{B}Handläggarens HSA-id:{/B} {XraHSAID}

{B}Ort och datum{/B}
[Ort], {Date}

{B}Underskrift handläggare{/B}

{B}Namnförtydligande{/B}
{XraName}