Kommunförbundet Skåne

Version 0.4
Bilaga 7, RAPS

Rutiner för SITHS kort

Support eHälsa Cesam Skåne: ehalsosupport@kfsk.se
0723-71 53 00

Innehåll

Versionshistorik

Version	Datum	Status
0.1	131018	Bilaga 7 inskickad till Inera för granskning
0.2	131122	Revidering enligt granskningsrapport 2013-11-04
0.3	140115	Revidering enligt granskningsrapport 2014-01-09
0.4	140817	Revidering av olika textstycken

Inloggning i systemen

Du loggar in i SITHS Admin med din e-tjänstelegitimation:

- SITHS Admin via Internet: https://cve.trust.telia.com/ccat/

Du loggar in i självadministrationen med din personliga e-legitimation:

- Självadministrationen via Internet: https://cve.trust.telia.com/ccu

Du loggar in i SIS Capture station med din personliga e-legitimation.

Dokumentets syfte

Detta dokument beskriver basrutinerna för administration av eTjänstekort och reservkort.

Dokumentets målgrupp

ORA som utbildats av RA
CRA/LRA som utbildats av RA/ORA i gällande regelverk och SITHS admin.

1 eTjänstekort

eTjänstekortet som inte är SIS-godkänt, är ett s.k. ”företagskort utan foto”.

På eTjänstekortet finns ett chip för lagring av ett personligt Telia e-leg och ett tjänstecertifikat d.v.s. en elektronisk tjänstelegitimation, HCC. På kortet finns även magnetremsa och mifareslinga som kan användas om lokala behörigheter ska kopplas till kortet, t.ex. för inpassering.

Med den personliga e-legitimationen kan användaren skriva under t.ex. deklarationen, Försäkringskassans e-dokument, anmäla till donationsregistret, logga in på kommunens egen sida för e-tjänster etc.
Den elektroniska tjänstelegitimationen används vid inloggning/åtkomst av Pascal, NPÖ, Nationella säkerhetstjänster etc.

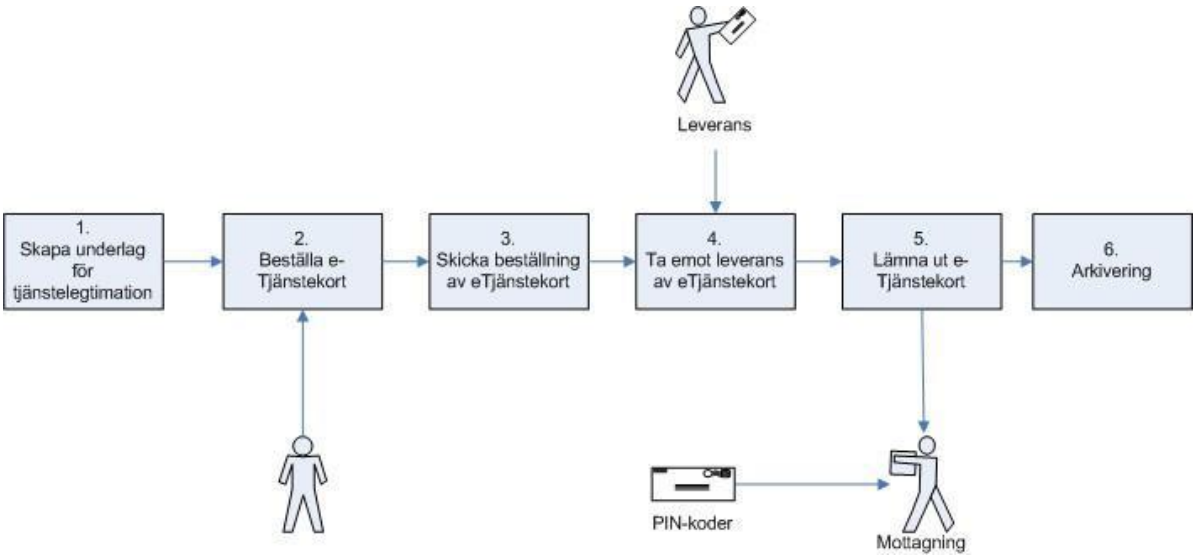
Reservkort

Reservkorten används framför allt då det är viktigt att användaren får ett kort omedelbart. För mer information om reservkort läs kapitel 2 i detta dokument.

1.1 Utgivning av eTjänstekort

På eTjänstekort och reservkort finns en e-tjänstelegitimation utgiven av SITHS CA. Denna kallas för HCC Person och består av ett identifieringscertifikat och ett signeringscertifikat. Identifieringscertifikatet används för säker elektronisk identifiering och signeringscertifikatet används för signering av elektronisk information. Det är olika pinkoder till identifieringscertifikat och signeringscertifikatet.

E-tjänstelegitimationen innehåller information för att unikt kunna identifiera personen inom kommunen/Kommunförbundet, bland annat för- och efternamn, HSA-id som är unikt för individen och som ersätter personnummer så att detta inte behöver användas i tjänsten, giltighetstid för certifikatet, yrkestitel, utgivare av certifikatet, e-postadress m.m.



1. Skapa underlag för e-tjänstelegitimation

Allmänt: Beställning av behörighet ska komma från verksamhetschef/motsvarande på avsedd blankett. Personen som ska få ett eTjänstekort behöver inte vara närvarande när underlaget för e-tjänstelegitimationen skapas.

- Klicka på snabblänken (aktuell kommun) som visas i mitten eller på fliken ”HCC Administration” för att komma till sidan för administration av e-tjänstelegitimationer.
- Ange sökkriterier för personen och klicka på ”Sök”.
- Om din sökning ger mer än en träff, välj rätt person i resultatlistan som presenteras. Kontrollera att uppgifterna är korrekta innan du beställer en ny e-tjänstelegitimation.
- Välj "Begär HCC till nytt kort".
- Kontrollera att det är markering ”Företagskort utan foto” vid ”Korttyp”.
- Välj giltighetstid på e-tjänstelegitimationen som motsvarar personens anställnings- eller uppdragstid. Maximal giltighetstid för en e-tjänstelegitimation är fem år.
- Underteckna beställningen genom att klicka på knappen "Signera och skicka". Ange din pinkod för signering.
- Klicka på "stäng".

När certifikatbegäran är slutförd kan du gå vidare med kortbeställningen i SIS Capture Station (SCS).

2. Beställ eTjänstekort

För att du ska kunna göra en kortbeställning måste den dator där du arbetar vara utrustad med:

- Programvaran SCS
- ActiveX-komponenten CaptureX

- Klicka på fliken "SCS Beställningar" i SITHS Admin. Beställningar som påbörjats visas för fortsatt handläggning.
- Välj att "Starta SCS i icke SIS-läge".
- Markera det underlag som ska kopplas till det nya eTjänstekortet och klicka ”öppna”. Personuppgifter visas.
- Fyll i kommunens kontorsnummer.
- Fyll i kommunnamn vid ”Övrig information”. Tryck ”Nästa”.
- Fyll i personens namn i fältet ”intyg/nr”.
- Tryck ”Nästa” 3 ggr.
- Nu visas allt som kommer med på kortet. Kontrollera att alla uppgifter i beställningen är korrekta. Skriv ut beställningsunderlaget och förvara det på säkert ställe, t.ex. i ett kassaskåp, tills dess att eTjänstekortet ska lämnas ut.
- Underteckna beställningen genom att klicka på knappen "Signera" och ange din pinkod för signering. Nu är beställningen färdig att skicka iväg till eTjänstekortsleverantören.

3. Skicka beställning av eTjänstekort

Allmänt: Vänta om det är möjligt med att skicka iväg beställningen av eTjänstekortet tills dess att det finns flera beställningar att skicka samtidigt. Fraktkostnaden från korttillverkaren är densamma oberoende av om ett eller flera kort beställs vid samma tillfälle. Observera även att du måste stänga ner ”SCS beställningar” i SITHS Admin efter det att du gjort en eTjänstekortsbeställning och sedan

öppna programmet SIS Capture Station ifrån programmenyn för att kunna skicka iväg beställningarna.

- Logga in i "SIS Capture Station" med din personliga e-legitimation d.v.s. markera Telia certifikatet.
- Välj ”Övriga kort” och klicka "Skicka beställningar till Gemalto AB".
- Din lista med färdiga beställningar visas. Här ges en möjlighet att göra en sista kontroll genom att markera en eller flera beställningar och därefter klicka ”Granska beställning”. Är något oklart kan du klicka ”Lås upp” och ”Radera order” d.v.s. beställningen.
- Markera de beställningar som ska skickas iväg och klicka "Skicka beställning(ar)".
- Underteckna beställningen genom att ange din pinkod för signering. Beställningsunderlaget översänds nu elektroniskt till kortleverantören.

4. Ta emot leverans av eTjänstekort

Allmänt: Nya eTjänstekort levereras alltid med e-tjänstelegitimation. eTjänstekorten levereras med rekommenderad post till den leveransadress enskild kommun/Kommunförbundet uppgett. Beställningen levereras ungefär fem arbetsdagar efter det att beställningen skickades.

- Var och en kommun ska ha en dokumenterad rutin för vem som tar emot rekommenderad försändelse med SITHS kort. I rutinen ska framgå att mottagaren har fullmakt att ta emot rekommenderad post och därmed är bemyndigad mottagare.
- Om mottagaren också är korthandläggare låser denna person in försändelsen i värdeskåp i väntan på utlämning/mottagande.
- Om mottagaren av försändelsen inte är korthandläggare låser mottagaren in försändelsen i värdeskåp i avvaktan på överlämnande till korthandläggaren.
- Vid överenskommen dag/tid överlämnar mottagaren personligen försändelsen till aktuell korthandläggare. OBS! Försändelsen får inte skickas med internpost.

5. Lämna ut eTjänstekort

Allmänt: Pinkoder till eTjänstekortet levereras till personens folkbokföringsadress ungefär två dagar efter det att korten levererats till kommunen/Kommunförbundet. eTjänstekortet får endast lämnas ut till den person som kortet är utställt till. Personen måste vara närvarande med giltig id-handling och pinkoder.

- **Identifieringskontroll**

Nytt kort eller Reservkort

- Personlig närvaro med giltig legitimation.
- Att annan känd person inom organisationen skriftligen går i god för medarbetarens identitet (se rutin för Intyg).

Giltiga id-handlingar är körkort, SIS-kort, nationella id-kortet, Skatteverkets id-kort och pass i vinröd bok. Identifieringsrutinen kan lämpligen följa rekommendationen från ”De sju stegen”:

1. Handling från medarbetaren - plockas ut ur fodral, eller dylikt av medarbetaren.
2. Personbedömning - finns det en anledning till att vara misstänksam?
3. Titta först på individen - därefter på ID-handlingen.
4. Kontrollera ID-handling - ej ändrad eller skadad, kontrollera giltighetstid och notera NID, SIS, KK

eller EU-Passnummer.

5. (Kontroll av kort för betalning - utgår då vi ej hanterar VISA-kort eller liknande)
6. Kontroll av namnteckning - en namnteckning skall
överensstämma med ID-handlingens namnteckning.
7. Återlämna handling

- Överlämna ett pappersexemplar av Telias villkor för e-legitimation. Observera att villkoren måste överlämnas i pappersform. Policyn tillåter inte att uppgiften endast bifogas som fil i mejl eller publiceras tillgänglig i nätverket.
- Sök upp personen i SITHS Admin under HCC Administration och välj ”Lämna ut kort”.
- Legitimera personen med giltig id-handling och kontrollera att personnummer och namn på det nya eTjänstekortet stämmer med uppgifterna på id-handlingen som används för legitimering. Registrera i systemet vilken id-handling som använts vid legitimering, kontrollera att kortnumret är rätt och signera utlämningen med din pinkod för signering. Kortet har fått status ”Utlämnat”.
- Sätt i mottagarens eTjänstekort i kortläsare 2 och välj ”Kvittens”. Visa vilken text mottagaren skriver under. Klicka därefter på knappen ”Signera” och låt mottagaren ange sin pinkod för signering. Den elektroniska kvittensen är nu undertecknad och kortet har fått status ”Mottaget”.
- Skriv ut ett exemplar av den signerade kvittensen ” Mottagande av SITHS kort” och överlämna utskriften till användaren.
- Lämna ut informationen ” SITHS-kortet – så funkar det” till användaren och informera om hur självadministration av e-tjänstelegitimationen fungerar via Net-iD ikonen i aktivitetsfältet, t.ex. byte av pinkoder, samt vad som gäller vid spärrning och återlämning av kort.

- Om personen sedan tidigare haft ett kort med e-tjänstelegitimation ska detta återlämnas och avregistreras, se punkt 1.2 Återlämning av eTjänstekort respektive 2.2 Återlämning av reservkort.

6. Arkivera information

Allmänt: Beställningsunderlag arkiveras elektroniskt hos kortleverantören.

Ordinarie kort

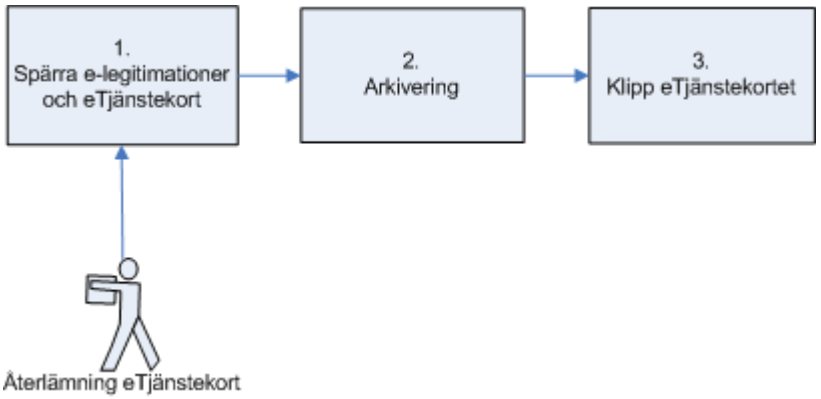
De vid beställningstillfället utskrivna underlagen för ordinarie kort ska därför förstöras i en dokumentförstörare när kortet är utlämnat. Användaren har signerat mottagandet digitalt i SITHS admin och detta finns arkiverat i systemet.

Reservkort

- Arkivera papperskvittensen på din arbetsplats i en pärm över utlämnade reservkort i bokstavsordning.
- Registret skall vara i sådan ordning att telefonförfrågningar om uppgifternas riktighet omgående kan besvaras.
- Kortkvittenser arkiveras under kortets giltighetstid och tio år därefter.
- Registret skall förvaras med betryggande säkerhet, exempelvis valv, värdeskåp eller annat väl skyddat utrymme.
- Registret får endast vara tillgängligt för register- och säkerhetsansvarig personal samt handläggare och vid kontrollbesök även för Driftleverantörens kontrollant.

1.2 Återlämning av eTjänstekort

Allmänt: Det är chefen eller uppdragsgivaren för den anställde som ansvarar för att eTjänstekortet återlämnas till SITHS administratören när personen slutar sin anställning. Den anställde har även fått såväl skriftlig som muntlig information i samband med mottagandet om att kortet är arbetsgivarens och ska återlämnas.
Återlämning sker också då identitetsuppgifterna på SITHS kortet och/eller i den personliga e-legitimationen på kortet har blivit ogiltiga, t ex då giltighetstiden på kortet och e-legitimationen gått ut, den anställde bytt för/efternamn eller om det är något tekniskt fel på kortet.
Obs! Om kortet av någon anledning inte återlämnas vid anställningens avslut ska punkt 1.3 nedan följas för att säkerställa att det inte finns aktiva kort i omlopp.



1. Spärra eTjänstekort

- Logga in i SITHS Admin och sök upp personen i systemet.
- Välj ”Avregistrera kort”.
- På vissa personer kan det finnas två eller fler SITHS kort aktiva. Dessa visas i så fall med kortnummer och information om ansvarig vårdgivare. Markera det kort som ska avregistreras.
- Ange orsak. E-tjänstelegitimationen spärras automatiskt i samband med detta.
- Signera avregistreringen genom att trycka på "Signera och Skicka" och sedan ange din pinkod för signering.

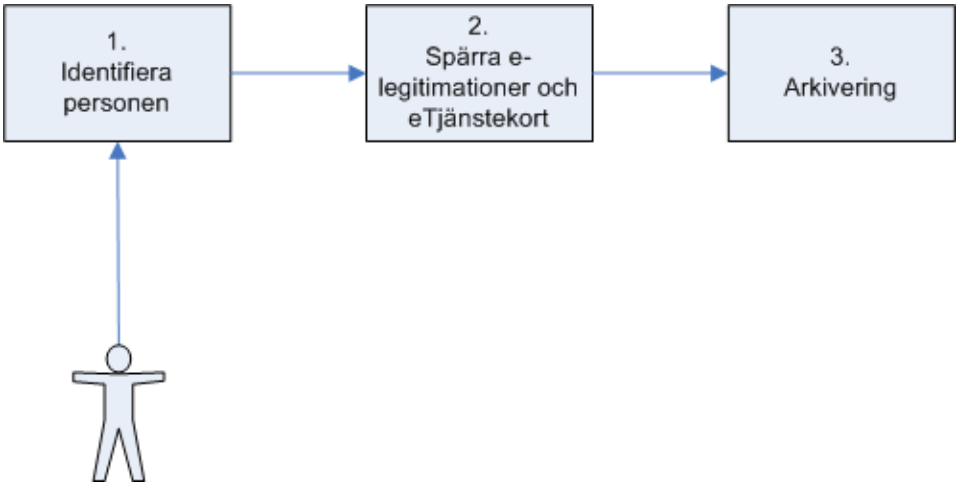
2. Arkivera information

- Information om återlämningen sparas i SITHS Admin med automatik.

3. Klipp eTjänstekortet

- Klipp eTjänstekortet genom kortnumret och chipet och släng kortdelarna.

1.3 Spärr av eTjänstekort



1. Identifiera personen

Allmänt: Kontakta alltid eTjänstekortsansvarig om någon annan än kortinnehavaren vill spärra ett eTjänstekort.

- Identifiera personen. Endast kortinnehavaren själv kan begära spärrning av sitt eTjänstekort och den personliga e-legitimationen. I undantagsfall kan även verksamhetsansvarig för personen göra det. Identifiering av personen kan ske genom ett enkelt förfarande, t.ex. genom att ställa motfrågor över telefon till personen.

2. Spärra e-legitimationer och eTjänstekort

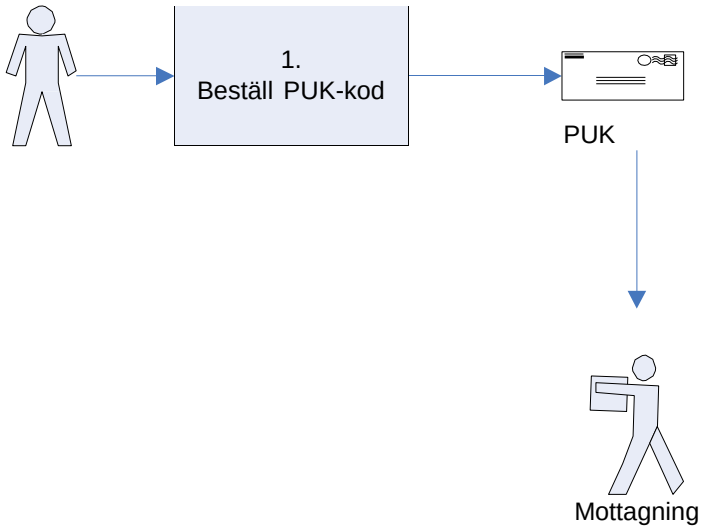
- Logga in i SITHS Admin och sök upp personen i systemet.
- Välj ”Avregistrera kort”.
- På vissa personer kan det finnas två eller fler SITHS kort aktiva. Dessa visas i så fall med kortnummer och information om ansvarig vårdgivare. Markera det kort som ska avregistreras.
- Ange orsak till att kort och tillhörande e-legitimationer ska spärras.
- Klicka på "Signera och Skicka" och ange din pinkod för signering.

Obs! Det går även att spärra kortet genom att ringa Telias spärrtjänst: Tel 0771-100 400. Kontrollera påföljande dag att e-tjänstelegitimationen är spärrad. Om e-tjänstelegitimationen inte är spärrad, spärra den manuellt i SITHS Admin, se punkt 4 Spärrning av e- tjänstelegitimation.

3. Arkivering

- Uppgifter om spärrningen sparas med automatik i systemet.

1.4 Beställning av pukkod



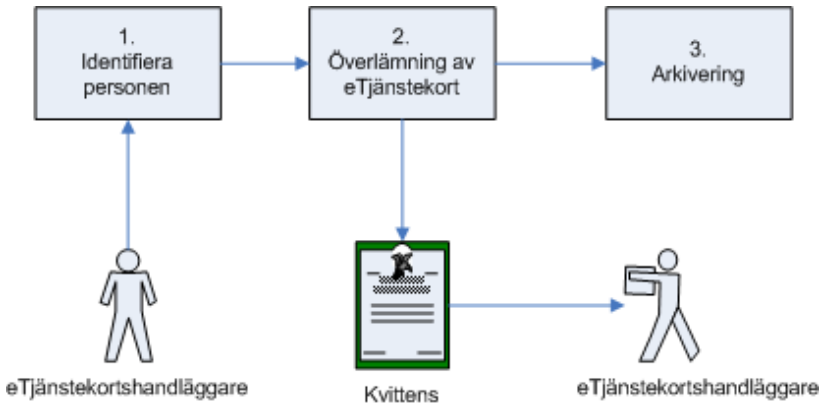
1. Beställ PUK till befintligt kort

Allmänt: Personal Unblocking Key (PUK) är en kod som man använder för att låsa upp ett elektroniskt id-kort som blockerats exempelvis efter flera misslyckade försök att ange PIN kod.

- Endast personen som eTjänstekortet är utställt till kan begära ny PUK till kortet. Personen måste närvara vid beställningen av PUK samt visa upp sitt giltiga eTjänstekort.
- Förvissa dig om att det är ägaren av eTjänstekortet som ber dig beställa ny PUK. Om du inte känner igen personen måste giltig ID-handling uppvisas.
- Sök upp personen som ska få en ny PUK under fliken ”HCC Administration”.
- Om din sökning ger mer än en träff, välj rätt person i resultatlistan som presenteras. Kontrollera att uppgifterna är korrekta innan du beställer en ny PUK.
- Välj "Begär PUK till befintligt kort".
- Kontrollera vilket kortnummer som PUK ska beställas till och markera det i systemet.
- Signera beställningen genom att trycka på "Signera och Skicka" och sedan ange din pinkod för signering.
- PUK skickas till personens folkbokföringsadress efter ca 2 dagar.

1.5 Överlämning av eTjänstekort till annan eTjänstekortshandläggare

Allmänt: Överlämning av eTjänstekort mellan handläggare som tillhör olika kontor i en kommun får endast ske i undantagsfall. Överlämningen skall alltid ske genom personligt möte.



1. Identifiera mottagande eTjänstekortshandläggare

- Identifiera mottagande eTjänstekortshandläggare och kontrollera med RA att personen är eTjänstekortshandläggare. För information om vilka id-handlingar som är giltiga se ”Identifieringskontroll”.

2. Överlämning av eTjänstekort

- I samband med att eTjänstekorten överlämnas till mottagande eTjänstekortshandläggare skrivs en kvittens där det tydligt ska framgå datum, exakt vilka eTjänstekort som överlämnas (kortnummer) samt namn på handläggarna . Kvittensen skrivs under av båda eTjänstekortshandläggarna.

3. Arkivering

- Kvittensen arkiveras hos den SITHS handläggare som beställt kortet/-en.

2 Reservkort

Reservkortet är ett på ytan blankt kort utan foto och personuppgifter. Reservkortet har ett serienummer tryckt på kortets utsida som fungerar som kortets kortnummer. I chipet på reservkortet finns ett transportcertifikat, istället för en personlig e-legitimation som på de ordinarie eTjänstekorten, och en e-tjänstelegitimation. På reservkortet finns även magnetremsa och mifareslinga som kan användas om lokala behörigheter ska kopplas till kortet, t.ex. för inpassering.

En e-tjänstelegitimation kopplat till ett reservkort är likadant och fungerar på samma sätt som en e-tjänstelegitimation kopplat till ett ordinarie eTjänstekort.

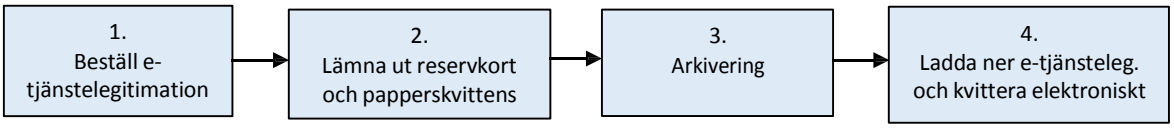
Reservkort kan användas om:

- en person inte har möjlighet att få ett eTjänstekort. Till exempel om personens uppdrag inom organisationen är kort eller personen befinner sig på en arbetsplats där man av olika anledningar inte vill/bör skylta med t.ex. sitt personnummer.
- en person har glömt eller tappat bort sitt ordinarie eTjänstekort.
- det plötsligt är något tekniskt fel på det ordinarie eTjänstekortet

2.1Beställa e-tjänstelegitimation

Allmänt: Beställning av behörighet ska komma från verksamhetschef/motsvarande på avsedd blankett.

- Om personen har andra e-tjänstelegitimationer som inte ska finnas, spärra dessa, se punkt 4. Spärrning av e-tjänstelegitimation. Detsamma gäller om personen har andra giltiga kort som inte ska finnas.



1. Beställ e-tjänstelegitimation till reservkortet

- Plocka fram ett reservkort med tillhörande pinkodsbrev och kontrollera att brevet fortfarande är oöppnat.
- Klicka på snabblänken (aktuell kommun) som visas i mitten eller på fliken ”HCC Administration” för att komma till sidan för administration av e-tjänstelegitimationer.
- Ange sökkriterier för personen och klicka på ”Sök”.
- Om din sökning ger mer än en träff, välj rätt person i resultatlistan som presenteras. Kontrollera att uppgifterna är korrekta innan du beställer en ny e-tjänstelegitimation.
- Välj ”Begär HCC till reservkort”.
- Ange reservkortets kortnummer som står skrivet på kortet.
- Kontrollera giltighetstid för den e-tjänstelegitimation som begäran avser. HCC till reservkort får ha en giltighetstid om högst 6 månader. Om personen har en visstidsanställning som är kortare än 6 månader anges det exakta t.o.m. datum som verksamhetschef/motsvarande fyllt i på underlaget.
- Signera beställningen genom att klicka på ”Signera och skicka” och ange din pinkod för signering. Klicka därefter på ”stäng”.

2. Lämna ut reservkort och pinkoder samt underteckna papperskvittens

- Utlämning av reservkort sker alltid av CRA eller LRA
- Välj ”Lämna ut kort”.
- Legitimera personen med giltig id-handling och markera vilken id-handling som använts.
- Välj kvittens och ”skriv ut”. Låt personen underteckna kortkvittensen och underteckna den därefter själv. Överlämna en kopia av den underskrivna kvittensen till personen och arkivera originalet, sparas i 10 år.
- Överlämna reservkortet och tillhörande pinkoder till personen och informera personen om hur e-tjänstelegitimationen hämtas till kortet (HCC-guiden), se steg 4 i denna rutin. Är det första gången personen ska ladda ned HCC till ett Reservkort bör administratören var med och handleda. Det är inte sällsynt att problem uppstår i processen då HCC- guiden följs och administratören måste då finnas till hands för att hjälpa personen.
- Lämna ut informationen ” SITHS-kortet – så funkar det” till användaren och informera om hur självadministration av e-tjänstelegitimationen fungerar via Net-iD ikonen i aktivitetsfältet, t.ex. byte av pinkoder, samt vad som gäller vid spärrning och återlämning av kort.

3. Arkivera information

- Arkivera papperskvittensen på din arbetsplats i en pärm över utlämnade reservkort i bokstavsordning. Spara originalet i 10 år. Pärmen ska förvaras inlåst och oåtkomlig för obehöriga.

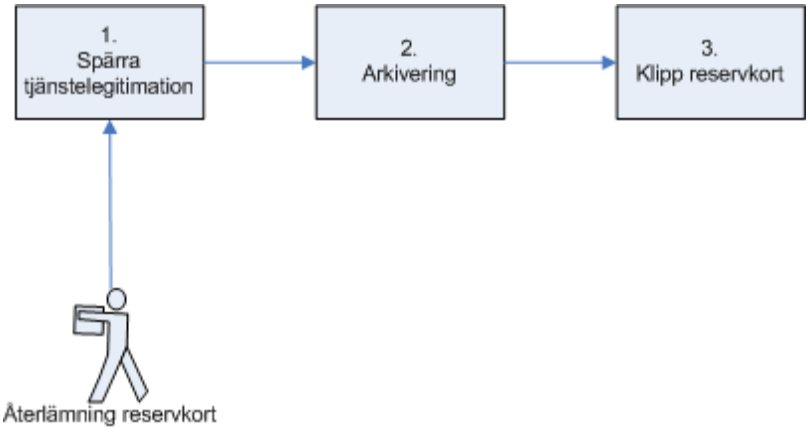
4. Nedladdning av e-tjänstelegitimation och elektronisk kvittering

Allmänt: Detta görs av personen som fått reservkortet. eTjänstekortsadministratör bör dock finnas till hands då problem ibland uppstår då HCC-guiden körs.

- Personen som fått ett reservkort placerar kortet i kortläsaren och loggar in i Självadministrationen. Telia e-legitimation markeras och legitimeringskoden fylls i. HCC- guiden öppnas.
- Kontrollera att radioknappen ”Hämta nytt HCC” är markerad och följ sedan guiden genom att klicka ”Nästa”.
- Personen undertecknar mottagandet av e-tjänstelegitimationen (HCC-certifikaten) elektroniskt genom att ange sin pinkod för signering.

2.2 Återlämning av reservkort

Allmänt: Observera att pinkodskuvertet inte ska återlämnas till eTjänstekortsadministratören. Endast kortet återlämnas.



1. Spärra e-tjänstelegitimationen på reservkortet

- Logga in i SITHS Admin och sök upp personen i systemet.
- Välj ”Avregistrera kort” och ange anledningen till att kortet avregistreras.
- Signera avregistreringen genom att klicka på ”Signera och skicka” och ange din pinkod för signering.

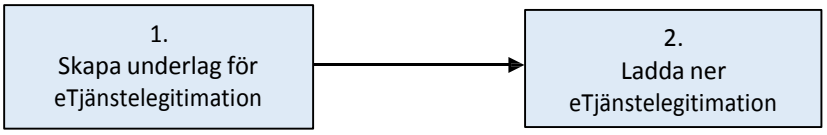
2. Arkivering

- Information om avregistreringen sparas i SITHS Admin med automatik.

3. Klipp reservkortet

- Klipp reservkortet genom kortnumret och chipet och släng kortdelarna. Använt reservkort får endast återanvändas av samma person.

3. E-tjänstelegitimation till befintligt eTjänstekort



1. Skapa underlag för e-tjänstelegitimation

Allmänt: Personen som ska få e-tjänstelegitimation till ett befintligt eTjänstekort behöver inte vara närvarande när underlaget för e-tjänstelegitimationen skapas.

- Sök upp personen som ska få en ny e-tjänstelegitimation under fliken ”HCC Administration”.
- Om din sökning ger mer än en träff, välj rätt person i resultatlistan som presenteras.

- Kontrollera om det finns en giltig e-tjänstelegitimation kopplat till kortet som ska spärras. Om så är fallet, spärra den, se punkt 4. Spärrning av e-tjänstelegitimation.
- Välj ”Begär HCC till befintligt kort”.
- Välj giltighetstid på e-tjänstelegitimationen som motsvarar personens anställnings- eller uppdragstid. Maximal giltighetstid för en e-tjänstelegitimation är fem år, men giltighetstiden för e-tjänstelegitimationen kan aldrig överstiga eTjänstekortets giltighetstid.
- Signera och skicka beställningen genom att klicka på ”Signera och skicka” och ange sedan din pinkod för signering.

2. Nedladdning av e-tjänstelegitimation

Allmänt: Detta görs av personen som ska få e-tjänstelegitimationen. eTjänstekortsadministratör bör dock finnas till hands då problem ibland uppstår då HCC-guiden körs.

- Placera kortet i kortläsaren och logga in i Självadministrationen. Telia e-legitimation markeras och legitimeringskoden fylls i. HCC- guiden öppnas.
- Kontrollera att radioknappen ”Hämta nytt HCC” är markerad och följ sedan guiden genom att klicka ”Nästa”.
- Personen undertecknar mottagandet av e-tjänstelegitimationen (HCC-certifikaten) elektroniskt genom att ange sin pinkod för signering.

3a. E-tjänstelegitimation till befintligt reservkort

1. Skapa underlag för e-tjänstelegitimation

Allmänt: Ett reservkort får av säkerhetsskäl inte återanvändas av någon annan person än den som ursprungligen fått kortet.

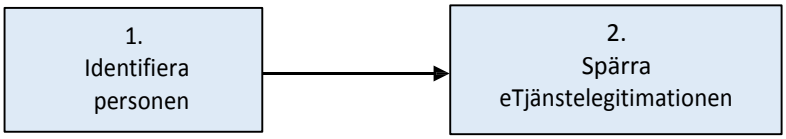
- Sök upp personen som ska få en ny e-tjänstelegitimation under fliken ”HCC Administration”.
- Om din sökning ger mer än en träff, välj rätt person i resultatlistan som presenteras.
- Kontrollera om det finns en giltig e-tjänstelegitimation kopplat till kortet som ska spärras. Om så är fallet, spärra den enl. punkt 4. Spärrning av e-tjänstelegitimation.
- Välj ”Begär HCC till reservkort”.
- Ange reservkortets kortnummer.
- Ange giltighetstid för den e-tjänstelegitimation som begäran avser. HCC till reservkort får ha en giltighetstid om högst 6 månader. Om personen har en visstidsanställning som är kortare än 6 månader anges det exakta t.o.m. datum som verksamhetschef/motsvarande fyllt i på underlaget.
- Signera och skicka beställningen genom att klicka på ”Signera och skicka” och sedan ange din pinkod för signering.

2. Nedladdning av e-tjänstelegitimation

Allmänt: Detta görs av personen som ska få e-tjänstelegitimationen. eTjänstekortsadministratör bör dock finnas till hands då problem ibland uppstår då HCC-guiden körs.

- Placera kortet i kortläsaren och logga in i Självadministrationen. Telia e-legitimation markeras och legitimeringskoden fylls i. HCC- guiden öppnas.
- Kontrollera att radioknappen ”Hämta nytt HCC” är markerad och följ sedan guiden genom att klicka ”Nästa”.
- Personen undertecknar mottagandet av e-tjänstelegitimationen (HCC-certifikaten) elektroniskt genom att ange sin pinkod för signering.

4 Spärrning av e-tjänstelegitimation



1. Identifiera personen som begär spärr

Allmänt:
Alt.1 Innehavaren av en e-tjänstelegitimation kan begära spärr av legitimationen.
Alt.2 Verksamhetsansvarig kan även begära spärr av en e-tjänstelegitimation inom det egna ansvarsområdet.
Alt.3 eTjänstekortsadministratör ska spärra gamla, aktiva HCC – certifikat vid begäran av nytt HCC-par till kort.
Observera att e-tjänstelegitimationen spärras automatiskt då kort ”Avregistreras” i SITHS Admin.

- Identifiera personen enligt ett av följande alternativ:
  - Personlig närvaro av personen med giltig id-handling.
  - Du har personlig kännedom om personen och går själv i god för personens identitet.
  - Som reservrutin, om det misstänks föreligga risk för missbruk, kan en förenklad form av identifiering göras, t.ex. genom motringning och/eller genom att ställa kontrollfrågor.

2. Spärra e-tjänstelegitimation

- Sök upp personen vars e-tjänstelegitimation ska spärras under fliken ”HCC Administration”.
- Om din sökning ger mer än en träff, välj rätt person i resultatlistan som presenteras.
- Markera certifikatet som ska spärras i rutan ”HCC”. Observera att både identifieringscertifikatet (aut) och signeringscertifikatet (sign) måste spärras.
- Ange orsak till att e-tjänstelegitimationen spärras.
- Signera och skicka beställningen genom att klicka på ”Signera och skicka” och sedan ange din pinkod för signering.

5 Förnyelse av utgående e-tjänstelegitimation

Tre veckor innan e-tjänstelegitimationen går ut skickas ett e-postmeddelande till kortinnehavaren med information om detta. Om ny e-tjänstelegitimation ska beställas kontaktar kortinnehavaren sin eTjänstekortsadministratör.

eTjänstekortsadministratören kan även kontrollera utgående giltighetstider i SITHS Admin statistik och loggar.

6 Tjänstecertifikat till funktioner

Ett funktionscertifikat är en elektronisk identitetshandling, som beskriver en maskin/server eller en IT-funktion. Det är ett mjukt certifikat som lagras på fil istället för på kort. Det finns både identifierings- och signeringscertifikat för HCC Funktion.

I dagsläget hanteras inte detta certifikat av Kommunförbundet Skåne. Om behov av funktionscertifikat finns kontaktas Kommunförbundet Skånes RA organisation som i sin tur förmedlar kontakt med Inera.

7 Behörighetsadministration

Behörighetsadministration i SITHS Admin hanteras av RA och ORA. Endast personer som återfinns i den tilldelande administratörens behörighetsområde kan tilldelas behörigheter (roller). Behörighet som KRA/LRA till ny administratör tilldelas efter deltagande i grundläggande SITHS-utbildning (ges i regi av Kommunförbundet Skåne).

RA och ORA måste alltid kontrollera om behörigheter behöver förändras i samband med omorganisationer.

a. Tilldelning av behörighet i SITHS Admin

Allmänt: Beställning av behörighet skickas till Kommunförbundet Skåne via avsedd blankett.
Personen som ska få en behörighet (roll) i SITHS Admin behöver inte vara närvarande när behörigheten sätts.

- Logga in i SITHS Admin.
- Sök upp personen som ska få en behörighet i organisationsträdet.
- Välj ”Administrera roller”.
- I organisationsträdet: Välj och markera den eller de organisationsgrenar som behörigheten ska börja gälla från.
- Ge personen behörigheten ”KRA” och ”LRA” i rollistan. Signera och skicka beställningen genom att klicka på ”Signera och skicka” och sedan ange din pinkod för signering.
- När signeringsfönstret stängs, kontrollera att rollen tilldelats och återfinns i tabellen längst ner i fönstret.
- Kontrollera att KRA/LRA har genomgått utbildning samt är införstådd med regelverket för SITHS kort.

b. Borttagning av behörighet i SITHS Admin

Allmänt: Beställning av borttag av behörighet skickas till Kommunförbundet Skåne via avsedd blankett.

- Logga in i SITHS Admin.
- Sök upp personen vars behörighet ska tas bort i organisationsträdet.
- Välj ”Administrera roller”.
- Välj att ta bort personens behörighet genom att klicka på symbolen för att ta bort, dvs. en papperskorg, i den ruta som svarar mot behörigheten som ska tas bort.
- Signera och skicka beställningen genom att klicka på ”Signera och skicka” och sedan ange din pinkod för signering.
- När signeringsfönstret stängs, kontrollera att rollen tagits bort i tabellen över personens roller.

8 Beställning av tillbehör

8.1 Beställning av reservkort

Allmänt**:** Beställning av reservkort sker via Kommunförbundet Skåne eller i egen regi. eTjänstekortsadministratören ska hålla ett lager av reservkort som täcker behovet inom det aktuella ansvarsområdet. Reservkort som ännu inte lämnats ut och tillhörande pinkoder förvaras i låst utrymme, oåtkomligt för obehöriga. Hur många reservkort som ska finnas i lager bedömer ansvarig verksamhetschef. Återlämnade reservkort får inte återanvändas.

a. eTjänstekortsadministratör beställer reservkort av Kommunförbundet Skåne

- Reservkort med tillhörande pinkoder beställs via e- post. E-postadress: ehalsosupport@kfsk.se . Reservkorten levereras till verksamhetens leveransadress för SITHS kort.

b. eTjänstekortsadministratör beställer reservkort av Cygate

- Reservkort med tillhörande pinkoder beställs av Cygate via *Bilaga 1.1.1 Beställning* i Yammer (nätverk CeSam Skåne, grupp eHälsa HSA/SITHS, fliken filer).

8.2 Beställning av korthållare

- eTjänstekortsadministratör beställer korthållare av Cygate via *Bilaga 1.1.1 Beställning* i Yammer (nätverk CeSam Skåne, grupp eHälsa HSA/SITHS, fliken filer).

9 Verifiering av korrekthet i SITHS admin

Informationsinnehållet i SITHS admin ska vara aktuellt och korrekt. Minst en gång i kvartalet ska respektive tredjepartsansluten kommun internt verifiera att anställnings- eller uppdragsförhållande kvarstår för de personer som finns i SITHS admin.

- Enligt gällande rutin för HPTA, bilaga 1, ska lokal HSA-administratör i kommunen en gång per kvartal ta ut listor ur Kommunkatalogen över aktuella personposter som överlämnas till ansvarig verksamhetschef för aktuellt verksamhetsområde. Verksamhetschefen kontrollerar och verifierar att anställnings-/uppdragsförhållande kvarstår för aktuella personer på listan. Förekommer avvikelser markeras dessa innan listan sändes tillbaka till HSA-administratören. HSA-administratören ansvarar för att avvikelser åtgärdas i Kommunkatalogen samt att lokal korthandläggare (CRA) omgående informeras om avvikelserna*.
- Korthandläggaren kontrollerar i SITHS admin om det finns aktiva, ej avregistrerade kort för de poster/personer som har avvikelser.
- Om det förekommer aktiva, ej avregistrerade kort ska korthandläggaren omgående avregistrera dessa kort.

* I de flesta kommunerna i Skåne är administratörerna både korthandläggare och HSA-administratörer.

10 Övriga rutiner

10.1 Reklamation av kort

Allmänt: Någon gång händer det att ett kort som levererats inte fungerar eller att det slutar att fungera efter ett tag. Då kan det bli aktuellt att reklamera kortet.

Innan reklamation görs kontrollera att:

- Kortet har status skickat eller utlämnat i SITHS Admin
- Inga certifikat visas i Net iD under ”Administration”

- Använd den reklamationsblankett som finns i Yammer (nätverk CeSam Skåne, grupp eHälsa HSA/SITHS, fliken filer).
  Var observant på att produkten som reklameras ska skickas till Gemalto med bifogad kopia på ifylld blankett. Originalblanketten skickas till Inera, se info. på blanketten.

10.2 Återlämning av e-tjänstekort och reservkort till annan än eTjänstekortshandläggare

Allmänt: När en anställd slutar sin anställning och kortet inte återlämnas direkt till e-tjänstekortsadministratören ska kortet tas om hand av ansvarig chef med personalansvar. Alla chefer som har personalansvar ska vara medvetna om betydelsen av denna hantering.

- Mottagaren klipper kortet genom kortnumret och chipet inför den anställde. Delarna lämnas till eTjänstekortsadmininstratören snarast möjligt och denne avregistrerar kortet i SITHS admin och kastar det.

10.3 Upplåsning av eTjänstekort

Allmänt: För att kunna låsa upp ett eTjänstekort behövs pukkod till kortet.

- Sätt i kortet i kortläsaren, vänta på att läsaren detekterat chipet och högerklicka på Net id-ikonen längst ner till höger i aktivitetsfältet på din skärm.
- Klicka på ”Låsa upp kort med pukkod” och välj om upplåsningen gäller pinkoden för legitimering eller underskrift.
- Ange pukkoden för att låsa upp kortet vid ”säkerhetskod för upplåsning” och ange den nya pinkoden vid ”Ny säkerhetskod”. Den nya pinkoden ska skrivas in ytterligare en gång under ”Byt pinkod”. Klicka sedan på ”Ok”. Obs, om fel pukkod anges mer än 10 gånger kommer kortet inte att kunna låsas upp. Då erhålls ett felmeddelande om att kortet är låst.

10.4 Byte av pinkoder

- Sätt i kortet i kortläsaren, vänta på att läsaren detekterat chipet och högerklicka på Net id-ikonen längst ner till höger i aktivitetsfältet på din skärm.
- Klicka på ”Byt pinkod” och välj om det är pinkoden för legitimering eller underskrift som ska ändras.
- Ange den gamla pinkoden vid ”gammal pinkod” och ange den nya pinkoden vid ”Ny pinkod”. Den nya pinkoden ska skrivas in ytterligare en gång under ”Bekräfta ny pinkod”. Klicka sedan på ”Ok”.

10.5 Namnändring

Allmänt: Namn på eTjänstekortet ska överensstämma med namn i Skatteverkets register. HSA- och SITHS administratörer som kopplats till funktionsbrevlådan i respektive kommun får automatiskt ett mejl en gång/månad. I detta informeras om förändringar i namn på kommunens anställda som är inlagda i HSA-katalogen. När en namnändring skett ska HSA-posten uppdateras och nytt SITHS kort beställas.

- HSA-administratören byter namn på aktuell personpost i Kommunkatalogen och informerar eTjänstekortadministratören när bytet är klart.
- eTjänstekortadministratören söker upp personen i SITHS Admin.
- Kontrollera att det nya namnet finns i systemet.
- Välj "Begär HCC till nytt kort".
- Markera vilken korttyp som ska beställas.
- Välj giltighetstid på e-tjänstelegitimationen som motsvarar personens anställnings- eller

uppdragstid. Maximal giltighetstid för en e-tjänstelegitimation är fem år.

- Underteckna beställningen genom att klicka på knappen "Signera och skicka". Ange din pinkod för signering.
- Klicka på "stäng".
- Beställ, skicka, ta emot och lämna ut nytt eTjänstekort till personen, se punkt 1.1 *Utgivning av eTjänstekort*. Avregistrera det gamla kortet, se punkt 1.2 *Återlämning av eTjänstekort* när det nya lämnats ut.

10.6 Förutsättningar för att få e-tjänstelegitimation

Personen
- har en anställning, ett uppdrag hos arbetsgivaren/kommunen.
- är upplagd i HSA-katalogen.
- ansvarig verksamhetschef har skriftligt beställt ett eTjänstekort av administratören.

10.7 Hantering vid missbruk av eTjänstekort

Om missbruk av eTjänstekort eller e-legitimationer misstänks eller kommer tillkänna ska verksamhetsansvarig, RA och säkerhetsansvarig omedelbart informeras och vidta lämpliga

åtgärder för att stoppa missbruket, till exempel genom att begära spärrning av aktuella e-legitimationer/eTjänstecertifikat, se RAPS bilaga 1.

10.8 Hantering av eTjänstekort och e-tjänstelegitimationer för personer som tillfälligt är borta från arbetet

Personer som är tillfälligt borta från sitt arbete ska behålla kortet och tillhörande PIN/PUK-koder under frånvaron förutsatt att anställningen är pågående.
- Spärra HCC så att kortet inte kan användas för att nå sekretessklassad information under ledigheten.
- Nytt HCC laddas ned till kortet då personen är åter i tjänst.

10.9 *Personer med samordningsnummer och personer utan folkbokföringsadress*

eTjänstekort och e-tjänstelegitimationer till ovan angivna undantag kan för tillfället inte hanteras av Kommunförbundet Skånes RA organisation. Detta p.g.a. att det underlag för HCC som skapas i vårt nuvarande gränssnitt för inmatning av uppgifter till HSA inte stödjer denna typ av undantag.

10.10 *Personer med skyddade personuppgifter*

Endast RA och ORA anställda på Kommunförbundet Skåne kan hantera eTjänstekort och e-tjänstelegitimationer till personer med skyddade personuppgifter. Kontakta dessa personer.