# Hantering av borttagna personobjekt med giltiga certifikat

Beskrivning av totallösningen

## Innehåll



# Revisionshistorik

| Version | Datum | Författare | Kommentar |
|---|---|---|---|
| 1.0 | 2016-03-14 | Henrika Littorin, Kerstin Arvedson | Avstämt med förvaltning och förvaltningsgrupp. Godkänt av tjänsteansvariga för HSA och SITHS. |
| 1.1 | 2016-10-20 | Henrika Littorin | Ändrad period för totalkörningar till två gånger per år. |
| 1.2 | 2020-05-25 | Katrine Streng | Justerat efter ändrad benämning av HCC till certifikat. |

# 1. Övergripande beskrivning

## 1.1 Bakgrund

Anslutna organisationer har önskat bättre stöd för certifikat-hanteringen när en person slutar. En persons objekt ska tas bort från HSA direkt när personen slutar, men då kan man i SITHS inte längre se personobjektet och därmed inte heller spärra certifikat eller avregistrera SITHS-kort.

## 1.2 Syfte

Skapa en smidig och korrekt hantering både i HSA och SITHS, genom att:

- direkt när personen slutar kunna ta bort personen från HSA
- att ändå kunna spärra certifikat och avregistrera personens SITHS-kort, trots att personen är borttagen i HSA
- att kunna söka fram eller ta ut rapport över vilka personer som har slutat men ännu inte fått sina certifikat spärrade, så att dessa uppmärksammas och att organisationen därmed inte missar att spärra certifikat eller återkräva SITHS-kort.

## 1.3 Översiktlig beskrivning av lösningen

Lösningen har följande olika delar:

- Skript för tillägg av giltiga men ej publicerade certifikat och SITHS-attribut resp. borttagning av ogiltiga eller inaktuella SITHS-attribut från personobjekt.
- Lösning i HSA Admin som vid borttagning av personobjekt med giltigt certifikat, inte flyttar personobjektet till organisationens Limbo-gren, utan låter objektet ligga kvar och istället tilldelar det objektklassen *hsaDeletedPersonWithValidCertificates*. I HSA Admin visas dessutom ett sådant borttaget personobjekt med en röd överstruken ikon.
- Skript som regelbundet kontrollerar personobjekt med *hsaDeletedPersonWithValidCertificates* och flyttar det till organisationens Limbo-gren när alla dess giltiga certifikat spärrats.
- En ny funktion i HSA-portalen som listar personer med giltiga certifikat som har tagits bort ur HSA och därmed fått den nya objektklassen.
- En ny rapport i SITHS Admin som listar personer med giltiga certifikat som har tagits bort ur HSA och därmed fått den nya objektklassen.
- En ny webservice i HSA som understödjer ovan rapport i SITHS Admin i att hitta personer med den nya objektklassen

I och med att lösningen inte flyttar personobjektet vid borttagning kan befintliga behörighetsstrukturer i både SITHS och HSA fungera som de är utan förändring.

# 2. Rutin för kontroll av personposters certifikat och SITHS-uppgifter

## 2.1 Syfte

Att få en korrekt bild i HSA över vilka personobjekt som har giltiga certifikat vilket är en förutsättning för att denna nya hantering ska fungera fullt ut.

Detta är en certifikat-kontrollprocedur som redan idag tillämpas av enskilda organisationer via beställning direkt mot SITHS:s och HSA:s leverantörer.

## 2.2 Kontroll av att ingen SITHS-information saknas i HSA

Två gånger per år (i april och oktober) tar SITHS' applikationsleverantör fram en totalfil över alla giltiga certifikat. Denna jämförs sedan med alla personobjekt i HSA för att verifiera att alla giltiga certifikat samt övriga SITHS-attribut inkl. hsaMifareSerialNumber finns publicerade till alla matchande personobjekt. Vid behov kompletteras personobjekt med den saknade informationen.

Denna funktionalitet är ett komplement till möjligheten att via SITHS Admin publicera certifikat till HSA i efterhand för en enskild person där publiceringen misslyckats.

## 2.3 Kontroll av att ingen SITHS-information i HSA är inaktuell

Kontroll av SITHS-information införs enligt:

- Att inga utgångna eller spärrade certifikat eller andra inaktuella SITHS-attribut finns publicerade till något personobjekt. I så fall rensas dessa bort
    - certifikat-uppgifterna kontrolleras mot spärrlista och slutdatum.

Skriptet körs en gång per dygn nattetid. Konfigurerbart för vilka organisationsgrenar som kontrollen ska köras.

# 3. Utökad hantering i HSA Admin vid borttagning och skapande av personobjekt

## 3.1 Borttagning av personobjekt

När en person slutar ska dess personobjekt tas bort från HSA.

Idag kontrollerar HSA Admin vid borttagning om personen har någon kopia under organisationen. Om personen har kopia tas personposten bort. Om personen inte har någon

kopia, dvs. är sista instansen av personposten så genomförs en flytt till organisationens limbo-gren.

Den nya hanteringen i HSA Admin innebär

- om det finns en kopia av personobjektet så tas personobjektet bort som tidigare
- om personobjektet har certifikatsinformation registrerad i HSA genomförs en OCSP-slagning för att kontrollera om certifikatet är giltigt
    - Om det inte finns giltiga certifikat kommer personobjektet att flyttas till Limbo som tidigare
    - om personen däremot har giltiga certifikat, så kommer HSA Admin:
        - sätta objektklassen hsaDeletedPersonWithValidCertificates på posten som därmed döljs för alla utom för administratörer med behörigheter att administrera personposten samt för SITHS
        - sätta attributet endDate till aktuell tidpunkt
        - visuellt markera objektet med en personsymbol som är röd med streck över (jämför hiddenObject där personen är grå med streck över)
        - inte längre att visa valet ”Ta bort” för personobjekt med denna objektklass

Motsvarande hantering är tänkt att också kunna implementeras lokalt hos synkande organisationer.

## 3.2 Vid skapande av person

Idag kontrollerar HSA Admin vid skapande av en person om personen finns på annat ställe i samma organisation. Om personen finns på annat ställe i organisationen så skapas en kopia av personposten. Om personen finns i limbo så görs en flytt från limbo. Endast om personen inte finns alls under organisationen skapas ny post och nytt HSA-id genereras.

Ändringen i HSA Admin innebär en utökad kontroll för att få med de fall då en personpost är borttagen med den nya hanteringen med objektklassmärkning. Flödet blir då enligt nedan:

Först görs en sökning för att se om det redan finns ett personobjekt med aktuellt personnummer under organisationen.

Om det redan finns ett personobjekt under organisationen, så

- kontrolleras om kopian har objektklassen hsaDeletedPersonWithValidCertificates. Om detta saknas skapa en kopia av personposten enligt befintlig logik.
- Om kopian har objektklassen hsaDeletedPersonWithValidCertificates
    - så görs en flytt av personposten till organisationsgrenen där personen skall skapas, om den inte ska skapas under den enhet där den redan ligger.
    - Objektklassen och endDate tas bort samt personsymbolen ändras från röd med streck över till den vanliga personsymbolen.

Om personobjektet finns i limbo, så

- Görs en flytt från limbo enligt tidigare logik.

Om det inte finns något personobjekt under organisationen

- Så skapas ny personpost och nytt HSA-id genereras enligt tidigare logik.

## 3.3 Redigering av person

Personer med objektklassen hsaDeletedPersonWithValidCertificates förses med en extra flik (på samma sätt som skyddad person) där det finns information om att certifikat inte är spärrat och att personen därför inte kan tas bort och att man ska kontakta SITHS-handläggare. Det ska också finnas ett alternativ (kryssruta) för att återaktivera personen, d.v.s. att ta bort objektklassen och endDate. Vid återaktivering ändras personsymbolen från röd med streck över till vanlig personsymbol i HSA Admin.

# 4. Script för kontroll av ”borttagna” personobjekt med objektklassen hsaDeletedPersonWithValidCertificates

## 4.1 Script för flytt av borttagna personobjekt till Limbo

När organisationens SITHS-handläggare avregistrerar ett kort eller spärrar en borttagen persons certifikat så tar SITHS bort SITHS-uppgifterna från aktuellt personobjekt i HSA.

Ett borttagningsscript kommer införas i HSA. Borttagningsskriptet söker en gång per dygn nattetid igenom alla personobjekt med hsaDeletedPersonWithValidCertificates och kontrollerar om SITHS-attributen finns kvar. Om SITHS-attributen inte finns kvar, flyttas personposten till Limbo och rensas på onödiga attribut enligt ordinarie logik.

Det är konfigurerbart för vilka organisationsgrenar som kontrollen ska köras, vilket gör att organisationer som synkar personer från intern katalog kan undantas.

# 5. Lösningens påverkan på synkande organisationer

De delar av lösningen som hanterar korrekt och uppdaterad kort- och certifikatinformation i HSA omfattar både synkande organisationer och de organisationer som arbetar i den nationella installationen av HSA Admin. Denna del medför inga krav på ändringar hos synkande organisationer.

Lösningen är i övrigt utformad utifrån att den inte ska påverka de organisationer som synkar information till HSA från en intern katalog, men också att den ska kunna användas i delar eller implementeras lokalt för de synkande organisationer som så önskar. Vi ser att synkande organisationer har följande alternativ:

1. Låt bli att utnyttja funktionaliteten och kör på som tidigare med den kontroll ni haft för att se till att inga personer med giltiga certifikat tas bort ur HSA. Ert delträd undantas i den nationella hanteringen (default).

2. Inför motsvarande lösning i er lokala katalog och ert lokala admingränssnitt som vi gör på nationell nivå. Synkfunktionaliteten behöver också kompletteras för att kunna hantera den nya objektklassen. Ert delträd undantas i den nationella hanteringen. OBS! Detta förutsätter dock att ni synkar ned kort- och certifikatsuppgifter till er lokala katalog. Denna lösning är kanske mest kostsam, men ger en direkt återkoppling till lokala administratörer på hanteringen.

3. Nyttja delar av den nationella funktionaliteten, d.v.s. funktionaliteten i HSA-portalen och i SITHS Admin för att hitta borttagna personer med giltiga certifikat. Detta kräver att synkfunktionaliteten ändras så att den verifierar att de saknar certifikatsuppgifter innan den tar bort personer. Om de har certifikatsuppgifter ska istället objektklassen sättas och sannolikt behöver även objektet hållas under bevakning av synken så att det tas bort först när certifikatsuppgifterna är borttagna. Väljer ni denna lösning innebär det en lite större ändring av synkfunktionaliteten men ingen ändring i det lokala admingränssnittet eller den lokala katalogen.