Hantering av borttagna personobjekt med giltiga certifikat

Beskrivning av den samlade funktionaliteten

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.
1.3	2022-06-21	Henrika Littorin	Omformulerat texten så att den beskriver funktionaliteten som befintlig istället för som kommande.

1. Övergripande beskrivning

1.1 Bakgrund och syfte

Utifrån ett önskemål från anslutna organisationer om bättre stöd för certifikat-hanteringen när en person slutar skapades en anpassad funktionalitet enligt beskrivning nedan. Tidigare, då en person togs bort ur HSA utan att SITHS-kort och certifikat avregistrerats, kunde man i SITHS inte längre se personobjektet och därmed inte heller spärra certifikat eller avregistrera SITHS-kort.

Efter att denna samlade funktionalitet produktionssattes 2016 kan en persons objekt nu tas bort från HSA direkt när personen slutar, och såväl SITHS-handläggaren som HSA-administratören blir uppmärksammade på att det finns giltiga kort/certifikat och kan hantera detta i efterhand. Det gör också risken mindre att en person som slutar sin anställning eller sitt uppdrag har kvar ett giltigt SITHS-kort och därmed obehörigen kan få åtkomst till känslig information.

1.2 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 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 funktion i HSA-portalen (HSA Admins kontrollkörningar) som listar personer med giltiga certifikat som har tagits bort ur HSA och därmed fått den nya objektklassen.
- En rapport i SITHS Admin som listar personer med giltiga certifikat som har tagits bort ur HSA och därmed fått den nya objektklassen.
- Ett REST-anrop mot 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 fungerar befintliga behörighetsstrukturer i både SITHS och HSA som tidigare.

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

Att HSA innehåller korrekt information om vilka personobjekt som har giltiga certifikat är en förutsättning för att denna hantering ska fungera fullt ut.

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, inklusive 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.

Därefter kontrolleras även att inga utgångna eller spärrade certifikat eller andra inaktuella SITHS-attribut finns publicerade till något personobjekt. I så fall rensas dessa bort. Certifikatsuppgifterna kontrolleras mot både spärrlista och slutdatum.

Skriptet körs en gång per dygn nattetid. Det är konfigurerbart för vilka organisationsgrenar som kontrollen ska köras.

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

3.1 Borttag av person

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

Detta sker enligt följande process:

- 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.
    - 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 personobjektet.

Motsvarande hantering kan också implementeras lokalt hos synkande organisationer. Läs mer i avsnitt 5.

3.2 Skapande av person

Vid skapande av en person via HSA Admin görs först görs en sökning för att se om det redan finns ett personobjekt med aktuellt person-id under organisationen. Om så INTE är fallet skapas ett nytt personobjekt och ett nytt HSA-id genereras. Om så ÄR fallet finns tre alternativ:

1. Personobjektet är ett ”aktivt” objekt.
    a. I så fall informeras administratören om att personen redan finns på annan plats i organisationsträdet, och om administratören väljer att gå vidare skapas en kopia av personposten.
2. Personobjektet finns i Limbo.
    a. I så fall görs en flytt av objektet från Limbo och administratören ges möjlighet att fylla på med aktuella uppgifter för personen.
3. Personobjektet finns, men har objektklassen hsaDeletedPersonWithValidCertificates.
    a. I så fall görs en flytt av personposten till organisationsgrenen där personen ska skapas, om den inte ska skapas under den enhet där den redan ligger.
    - Objektklassen och endDate tas bort och personsymbolen ändras från röd med streck över till den vanliga personsymbolen.

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, att personen därför inte kan tas bort och att man ska kontakta SITHS-handläggare. Det finns ett alternativ (kryssruta) för att återaktivera personen, d.v.s. att ta bort objektklassen och endDate. Vid återaktivering ändras personsymbolen i HSA Admin från röd med streck över till vanlig personsymbol.

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.

I HSA finns ett borttagningsskript som en gång per dygn nattetid söker igenom alla personobjekt med hsaDeletedPersonWithValidCertificates och kontrollerar om SITHS-attributen finns kvar. Om SITHS-attributen inte finns kvar, flyttas personposten till Limbo enligt ordinarie logik.

Det är konfigurerbart för vilka organisationsgrenar som kontrollen ska köras, vilket gör att organisationer som synkar personer från lokal 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 lokal 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 finns i nationella HSA Admin. 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 administrationsgränssnittet eller den lokala katalogen.