VGR obevakad mjukvaruprocess

Datum

Unattended RPA med SITHS Funktionscertifikat

September | 2024 | rev.1

VÄSTRA GÖTALANDSREGIONEN

Sammanfattning

Västra Götalandsregionen (VGR) har skapat ett sätt att köra obevakad automatiserad mjukvaruprocess på ett säkert sätt mot de applikationer som tillåter ömsesidig autentisering (mTLS) med SITHS funktionscertifikat.

Förutom tekniska förutsättningar måste det även finnas informationsägare som tar ansvar för den informationsbehandling som sker.

Dokumentet innehåller en lista med aktiviteter för genomförande.

Andreas Östberg
Lösningsarkitekt innovation och IT-säkerhetssamordnare, koncernstab digitalisering
E-post: andreas.ostberg@vgregion.se

Bakgrund

Under flera år har frågan om att möjliggöra obevakad mjukvaruprocess att arbeta med patientdata utretts av regioner och Inera utan att komma till en lösning som täcker önskvärda fall.

Även denna lösning är begränsad i när den kan tillämpas, men i de fall den fungerar innebär den tydliga vinster i att frigöra personal i hälso- och sjukvården till att koncentrera sig på ordinarie arbetsuppgifter i stället för att fastna vid dator med eTjänstekort (SITHS) i kortläsaren medan processen jobbar.

Förutsättningar

Unattended RPA med SITHS Funktionscertifikat kräver tre saker:

1. Informationsägare som tar ansvar för informationsbehandlingen. Tänk på mjukvaruprocessen som en medarbetare som behandlar verksamhetens information
2. Applikationer/tjänster/API:er som tillåter mTLS och där åtkomst/behörigheter sätts upp i applikationen (det funkar inte när åtkomst enbart är en konsekvens av medarbetaruppdrag i HSA-katalog. Där har Sverige och Inera fortfarande kört fast)
3. Ett SITHS Funktionscertifikat för ändamålet som sätts upp på den dator/server som kör mjukvaruprocessen, lämpligen en permanent/full clone VDI där mjukvaruprocessen kan schemaläggas.

Genomförande

Ordningen på genomförande kan variera, men innehåller alla eller de flesta av dessa steg:

- Utveckla en kvalitetssäkrad och dokumenterad mjukvaruprocess. Processägare eller informationsägare hos verksamheten ska godkänna processdokumentationen
- Testa och verifiera löpande
- Säkra att informationsägare förstått och tagit ansvar för informationsbehandlingen
- Beställ ett SITHS funktionscertifikat för ändamålet. Ett för utveckling/test och ett för produktion kan behövas.
- Beställ ett fiktivt konto via KiV som skall kopplas till en virtuell maskin och funktionscert. Kontot resulterar i ett AD-konto som kan köra mjukvaruprocessen.
- Koppla funktionscertifikat till informationsägare genom beställningen och/eller dokumentation av lösningen
- Sätt upp funktionscertifikat + kedja på den dator eller VDI som ska köra mjukvaruprocessen
- Se till att det konto som ska köra mjukvaruprocessen har behörighet att använda funktionscertifikatets privata nycklar
- Konfigurera mjukvaruprocessen att använda funktionscertifikatet
- Sätt upp att applikationer/tjänster som mjukvaruprocessen använder tillåter anslutning med SITHS Funktionscertifikat
- I de fall endast specifika certifikat tillåts upprätta mTSL mot applikationen/tjänsten, konfigurera det beställda funktionscertifikatet i listan av godkända certifikat.
- Om det behövs, sätt upp en användare av applikationen/tjänsten som kan kopplas till certifikatet. Oftast sker kopplingen på HSA-Id.
- Sätt upp behörigheter i applikationen/tjänsten för användaren eller certifikatet.
- Schemalägg mjukvaruprocessen
- Logga/övervaka mjukvaruprocessen och sätt upp notifieringar
- Klar? Kör!

Mer information

Beställning av SITHS Funktionscertifikat

Görs i VGR serviceportal
https://plexus-prod.vgregion.se/sp?id=sc_cat_item&sys_id=27994fb747cda5109e2a21ebd36d43d3

Hantering av SITHS Funktionscertifikat

Hantering av certifikat ser litet olika ut i olika operativsystem och teknikstackar. Ta hjälp av någon som kan.

https://inera.atlassian.net/wiki/spaces/IAM/pages/448103163/SITHS+Funktionscertifikat+-+Anv+ndarguide.

Mjukvaruprocess/RPA

RPA FB rpa@vgregion.se