Försäkringskas

Certifikathantering Försäkringskassan

Innehållsförteckning

Inledning

Detta dokument vänder sig till kunder och partners som är i behov att kommunicera med Försäkringskassans publicerade tjänster över internet.

Försäkringskassan använder i dagsläget primärt SHS, SSEK, REST och Webservicetrafik och baserar sin säkerhet på kryptering via certifikat.

Försäkringskassan följer branschstandard för kryptering och säker kommunikation som rekommenderas av våra säkerhetsexperter. I de fall säkerhetshål upptäcks för de certifikat Försäkringskassan använder förbehåller sig Försäkringskassan rätten att på kort varsel byta certifikat.

1 Förutsättningar

1.1 Godkända CA

Godkända utgivare idag Expisoft (tidigare Steria) och certifikat från Siths.

https://eid.expisoft.se/
http://www.inera.se/siths

Tekniska frågor gällande certifikaten hänvisas till respektive CA utfärdare.

1.2 Godkännande av övriga CA

Om de redan av Försäkringskassan godkända CA inte kan användas av den externa partnern så har Försäkringskassan tre grundläggande krav för att godkänna andra utfärdare.
Först måste de uppfylla kravet om organisationsnummer ska finnas i certifikatets header på formatet ”serialNumber=<orgnr>”
En CA Policy skall finnas tillgänglig samt att vi ska kunna kolla certets giltighet via CRL eller OCSP.
Och slutligen måste den CA man ämnar använda vara en känd CA.

En sådan granskning har en ledtid på två månader.

1.3 SerialNumber=OrgNr

Ett krav från Försäkringskassan är att certifikatheadern måste innehålla serialNumber=orgNr där orgNr motsvarar organisationsnumret för den externa part som anropar Försäkringskassan. Detta är en del i hur säkerhets implementationen är utförd hos Försäkringskassan.

Om en extern partner skall använda en annan organisations certifikat för kommunikation mot Försäkringskassan måste den informationen ges till Försäkringskassan så att en delegeringsregel kan konfigureras.

1.4 Publika nycklar från Försäkringskassan

Försäkringskassan använder certifikat utfärdade av Expisoft (Steria) 2048 bitars med sha256.

Om den externa partnern har behov av Försäkringskassans publika nycklar för våra inlämningsadresser så finns dom aktuella nycklarna publicerade här:

http://pki.forsakringskassan.se/SHS/latest/prod/
http://pki.forsakringskassan.se/SHS/latest/test/

1.5 Övrig information och support

För frågor av teknisk karaktär gällande tjänster som publiceras vänligen kontakta shssupport@forsakringskassan.se