Beslutad av: Chef Säkerhet och beredskap

Diarienummer: RS 255-2016

Giltighet: från 2016-03-31 [rev 18-11-01]

Rutin

vid kryptering av e-post i Outlook

Rutinen gäller för alla förvaltningar och bolag

Innehållsansvar: Koncernstab Utförarstyrning och samordning/Enhet Säkerhet och beredskap

Dokumentet ersätter:

VÄSTRA GÖTALANDSREGIONEN

Versionshistorik

Datum	Version	Förändringsorsak
16-03-31	1.0	Dokumentet upprättas.
18-11-01	1.1	Uppdaterat enligt gällande mall. Smärre textjusteringar och förtydliganden så att det framgår att det är tillåtet att använda krypteringen med extern part som använder samma krypteringsprotokoll.

Giltighet

Denna rutin är utformad med stöd av Västra Götalandsregionens (VGR) Säkerhetspolicy och Riktlinjer för informationssäkerhet och gäller därmed för alla VGR:s förvaltningar och ägda bolag.

Syfte

Syftet med krypterad e-post är att sekretessbelagd och annan känslig information kan överföras snabbt, effektivt och med hög säkerhet så att informationen är skyddad från obehörig åtkomst eller förändring.

För att uppnå en god informationssäkerhet krävs välfungerande tekniska lösningar såväl som tydliga hanteringsrutiner för användarna så att det tillsammans ger ett bra skydd. Rutinen är framtagen som ett stöd, för att använda tekniken på ett sätt som uppfyller VGR:s krav på informationssäkerhet vid användning av krypterad e-post i Outlook.

Allmänt

En förutsättning för att utbyta krypterad information är att båda parter använder sig av betrodda certifikat. VGR:s tjänstekort TjänsteID+ innehåller ett personligt certifikat som är den nyckel som används för att kryptera/dekryptera. Med detta certifikat kan krypterad e-post utväxlas med alla som använder samma typ av certifikat, exempelvis kommuner, landsting och privata vårdgivare som har SITHS/Efos samt många myndigheter.

Kryptering ger tekniskt sett ett bra skydd så att informationen inte kan bli åtkomlig för obehöriga. Det finns samtidigt risker för att bli ”utelåst” om användaren byter eller förlorar sitt TjänsteID+ (certifikatet). Därför är det viktigt att användare tar del av och följer denna rutin så att kryptering bara används för överföring av information och ingen information lagras krypterat i e-posten.

Se även instruktion för kryptering i Outlook

http://intra.vgregion.se/sv/Insidan/IT/Jag-vill-veta-mer-om-ISIT-i-VGR/Objekt--objektsidor/IT-arbetsplats/Kontorsprogramtjanster/E-post/Kryptering-av-e-post/

Ansvar

Det är verksamhetschefs ansvar att rutinen och lokala förutsättningar för att skicka krypterad e-post är väl kända bland medarbetarna. Finns osäkerhet om vad som är sekretessbelagd information eller annan känslig information måste detta tydliggöras inom respektive verksamhet.

Användaren ansvarar för att vid kryptering av e-post följa denna rutin och vara noga med att säkerställa att e-post skickas till rätt person.

VGR som juridisk person har yttersta ansvaret för att våra system och teknik används på ett korrekt sätt. Det innebär att arbetsgivaren kan komma att kontrollera att krypterad e-post inte missbrukas för oegentligheter eller annat som bryter mot VGR:s värdegrund. Användaren är därför skyldig att på begäran dekryptera information ifrån regionens e-postsystem för arbetsgivarens kontroll.

Kryptering av e-post

Sekretessbelagd information eller annan känslig information ska krypteras om den skickas via e-post. För att kryptera/dekryptera e-posten i Outlook används TjänsteID+. Annan information ska inte krypteras, eftersom det vid kryptering skapas ett beroende till användarens/mottagarens personliga certifikat, TjänsteID+.

Om TjänsteID+ förloras/går sönder/giltighetstiden går ut är det inte möjligt att dekryptera informationen. Enda möjligheten att få åtkomst till informationen i sådant fall är om avsändaren/mottagaren har kvar informationen och kan sända om den.

Kryptering för skyddad överföring – inte lagring

Kryptering ska enbart användas för att skydda överföring av information och inte lagring av den av ovan angivna skäl. Det betyder att informationen måste överföras från e-posten till annan lämplig lagringsplats, i första hand server i nätverket.

Kryptering/dekryptering

I VGR används TjänsteID+ och pinkod (SITHS/Efos) för att kryptera/dekryptera meddelanden i e-posten sändare/mottagare med.

För att utbyta krypterade meddelande med externa användare är det en förutsättning att de använder samma typ av certifikat (X-509) och krypteringsprotokollet S/Mime. Det ställer också krav på ett manuellt utbyte av publik krypteringsnyckel med den man vill utbyta krypterade meddelanden.

Det Tjänste-ID som var aktivt när e-posten skickades krävs för att öppna den. TjänsteID+ certifikat är giltigt i 5 år. Det innebär att när kortet byts kommer användaren inte att kunna öppna tidigare e-post. Samma sak gäller om kortet går sönder eller förkommer. Det är därför det är så viktigt att informationen inte lagras i e-postsystemet.

Se instruktion för att kryptera e-post:

http://intra.vgregion.se/sv/Insidan/IT/Jag-vill-veta-mer-om-ISIT-i-VGR/Objekt--objektsidor/IT-arbetsplats/Kontorsprogramtjanster/E-post/Kryptering-av-e-post/

Funktionsbrevlådor

Det går att skicka ett krypterat meddelande från en funktionsbrevlåda, förutsatt att den person som är inloggad skickar det från sitt personliga certifikat. Det är endast den personen som kan hantera meddelandet under sända meddelanden i funktionsbrevlådan. Däremot är det inte möjligt att skicka ett krypterat meddelande till en funktionsbrevlåda eftersom det endast går att skicka till personliga certifikat i dagsläget.

Kan endast läsas från en VGR-dator

Krypterad e-post kommer bara att kunna läsas från en VGR-dator på grund av att det idag saknas stöd för mobila enheter. Däremot kommer det synas i inkorgen att det finns ett krypterat meddelande och från vilken avsändare.

Ärendemening krypteras inte

När ett meddelande krypteras i Outlook så är det själva meddelandet och eventuella bilagor som krypteras. Det innebär att ärendemeningen måste formuleras så att information som ska skyddas inte finns med i denna. Ärendemeningen är även synlig i e-postloggar som kan komma att begäras ut.

Stark autentisering och rätt mottagare

I och med att kryptering (kort + PIN) används så sker en stark autentisering, jämfört med lösenord. Det ökar säkerheten för att endast behörig person kan ta del av informationen, men en förutsättning är fortfarande att avsändaren är noga med välja rätt mottagare. För att minimera risken för att skicka till fel person rekommenderas att egenskaper för kontakten öppnas, för att säkerställa att det är rätt mottagare.

Delegering och vidaresändning

Om brevlådan är delegerad till annan användare kan hen bara se att det inkommit ett krypterat meddelande och från vilken avsändare, men kan inte öppna meddelandet. Om ett krypterat meddelande vidaresänds så blir det meddelandet automatiskt krypterat.

Signering

Tjänste-ID + pinkod (särskild pinkod för signering) kan användas för att signera ett meddelande i Outlook. Det ger en signering som motsvarar en underskrift på papper. Signering innebär att avsändaren med garanterar e-postmeddelandets äkthet, integritet och ursprung.

Arkivering, diarieföring, och utlämning

Ett e-postmeddelande som inkommer eller skickas är en allmän handling och har samma krav på diarieföring och arkivering som all annan korrespondens.

E-post som ska arkiveras måste dekrypteras före arkivering. Kryptering får inte förhindra diarieföring. Därför ska dokumentet skickas antingen via internpost eller krypterat till enskild handläggare på diariet, som dekrypterar och diarieför. Kryptering får inte heller utgöra ett hinder för att e-posten ska kunna prövas för utlämnande av allmän handling. Detta är ytterligare ett starkt skäl för kravet på att enbart använda krypterad e-post som en överföringstjänst och inte lagring.

Patientuppgifter

Om e-post används för att kommunicera patientuppgifter, ska meddelandet krypteras och det är av särskild betydelse att uppgifterna inte blir liggande i e-postsystemet, utan uppgifterna ska överföras till avsett system eller lagringsplats och därefter raderas från Outlook.

För kommunikation med patienter ska **1177 Vårdguiden**:s meddelandetjänst användas, som är den nationella e-hälsotjänst som utvecklats för kommunikation mellan patient och vårdgivare.

Support

Supporten kan inte hjälpa till med att dekryptera ett meddelande. Det kan bara användaren själv göra med hjälp av sitt TjänsteID+. Supporten omfattar stöd i att förklara hur tjänsten fungerar eller ta emot ärenden om avvikelser inträffar.

Referenser

http://www.datainspektionen.se/lagar--regler/dataskyddsforordningen/informationssakerhet/sakerhet-for-personuppgifter-i-e-post/