Gäller för: Västra Götalandsregionen
Innehållsansvar: Fredrika Holm Fredriksson, (freho10), Strateg
Granskad av: Anders Andersson, (andan18), Enhetschef
Godkänd av: Johan Flarup, (johfl), Direktör

Giltig från: 2025-01-24
Giltig till: 2029-12-31

Användning av kryptering

Regional rutin 2025 - 2029

Ledningssystem för informationssäkerhet och dataskydd

VÄSTRA GÖTALANDSREGIONEN

Innehållsförteckning

1 Inledning

Syftet med denna rutin är att säkerställa en lämplig och effektiv användning av kryptering i Västra Götalandsregionen (VGR) för att skydda informationens konfidentialitet, äkthet och riktighet vid teknisk lagring, överföring och teknisk bearbetning.

Rutinen är en del av VGR:s ledningssystem för informationssäkerhet och dataskydd (LISD) och gäller därmed för alla VGR:s förvaltningar och ägda bolag.

Till rutinen rekommenderas Ineras anvisning för kryptering[1] som är ett stödjande dokument. Angående hashfunktioner rekommenderas NIST hash functions[2] som stödjande dokument.

2 Omfattning

Rutinen omfattar kryptering av VGR:s digitala informationstillgångar vid teknisk lagring, överföring och teknisk bearbetning oavsett informationsbehandlingsresurs och lagringsmedia.

Angående molntjänster finns rutin Informationssäkerhet för extern molntjänst som innehåller kompletterande information. Regional rutin Användning av kryptering är fortfarande gällande.

Rutinen omfattar inte val av algoritm eller nyckellängd eftersom det beror på design, användningsområde och specifika krav på informationstillgångar.

3 Termer och begrepp

Huvuddelen av termer och begrepp är hämtade från MSB termbank för informationssäkerhet, ISO Online Browsing Platform och andra rutiner under *Informationssäkerhet och dataskydd – Regional riktlinje 2023-2027* (RS 2023-02811).

Kryptering	Omvandling av vanlig text till kryptotext med hjälp av ett kryptosystem och en krypteringsnyckel eller en publik krypteringsnyckel i syfte att förhindra obehörig åtkomst till information. Förenklat är kryptering en process där matematiska algoritmer används för att omvandla

[1] Anvisning Kryptering (rivta.se)
[2] Hash Functions | CSRC (nist.gov)

	information till en form som är oläslig för obehöriga personer.
Kryptografiskt system	Utrustning och/eller program som används för att utföra kryptografiska algoritmer samt nyckelhantering för dessa.
Krypteringsnyckel	Används för kryptering och dekryptering av information.
Nyckelhantering	administration och tekniska metoder för skapande, förvaring, distribution, användning och förstöring samt eventuell certifiering av krypteringsnycklar.
Hashfunktion	Funktion som avbildar en godtyckligt lång datasträng till en datasträng med fast längd, s.k. hashvärde. Hashfunktioner används ofta för att säkerställa integritet hos information och som unika identifierare.
IS/IT-tjänst	Är en avgränsning av en eller flera digitala informationsbehandlingsresurser. Exempelvis IT-system, applikation, mjukvara, nätverk, lagringssystem eller infrastruktur.
Informationstillgång	Information och informationsbehandlande resurser som är av värde för en organisation. Informationstillgångar kan vara av fysisk eller logisk karaktär, eller bådadera. Exempel på informationstillgångar är: information, program, tjänster, datorer, nätverk, människor eller immateriella tillgångar.

4 Ansvar och roller

Ansvar och roller inom informationssäkerhet och dataskydd styrs av regional riktlinje för informationssäkerhet och dataskydd (LISD).

4.1 Digitaliseringsdirektör

Ansvarar för nyckelhantering (generering, registrering, säkerhetskopiering, distribution, installation, användning, förnyelse, lagring, destruktion) och att information skyddas med lämplig kryptering.

4.2 Projektägare

Ansvarar för att informationssäkerhets- och dataskyddsarbete genomförs vid verksamhetsutveckling för att utifrån informationens värde för verksamheten identifiera om det finns informationssäkerhetskrav på kryptering.

4.3 Ägare IS/IT-tjänst

Ansvarar för att säkerställa lämplig och effektiv användning av kryptering i enlighet med verksamhets- och informationssäkerhetskrav. I de fall där ägare av IS/IT-tjänst ej tilldelats har projektledare ansvar att säkerställa lämplig och effektiv kryptering tills projektet överlämnar lösningen till förvaltning. Då tar ägare IS/IT-tjänst över ansvaret.

Det är även ägare av en IS/IT-tjänst som ansvarar för att förse kunder (med kund menas exempelvis privat vårdgivare, kommuner eller VGR-ägda bolag) med information om vilken kryptering som används och detaljerad information om den specifika krypteringen som används för att skydda personuppgifter. Denna information är viktig eftersom den beskriver säkerhetsåtgärder som vidtas för att skydda behandlingen av personliga data.

4.4 Informationsägare

Ansvarar för att kravställa och godkänna ändamålsenlig kryptering. Informationsägare kan företrädas av en regional processägare.

5 Kryptering

Med kryptering avses krypteringsalgoritm och tillhörande nyckel/nycklar. Kryptering används för att skydda informationens konfidentialitet, äkthet och riktighet vid teknisk lagring, överföring och teknisk bearbetning. Kryptering av den information som ska skyddas får inte vara möjlig att knäcka eller förbigå inom rimlig tid med rimliga resurser. Vad som anses vara rimligt beror på känsligheten av den

skyddade informationen[3]. För att tillgodose detta krävs det att ägare IS/IT-tjänst regelbundet granskar den tillämpade krypteringsalgoritmen för att säkerställa att inga nya brister identifierats och att vald kryptering är fortsatt lämplig för att skydda informationen. Detta resulterar i krav på design, implementation, drift och underhåll av det kryptografiska systemet.

Kryptering används för olika syften och mål:

- *konfidentialitet:* kryptering av information för att skydda känslig eller kritisk information, som antingen lagras, överförs eller bearbetas
- *riktighet och äkthet*: användning av digitala signaturer, hashfunktioner eller meddelandeautentiseringskoder för att verifiera äktheten och/eller riktigheten hos information som lagras eller överförs. Algoritmer kan användas för att kontrollera filers integritet.
- *oavvislighet:* användning av krypteringsmetoder för att belägga förekomst, eller avsaknad av förekomst, av en händelse eller aktivitet inklusive säkerställa vilken part som är ansvarig för händelsen eller aktiviteten.
- *autentisering:* användning av krypteringsmetoder för att autentisera användare och andra systemenheter som begär åtkomst till eller genomför transaktioner med systemanvändare, entiteter och resurser.

De vanligaste krypteringsteknikerna är symmetrisk och asymmetrisk kryptering.

För symmetrisk kryptering används samma nyckel vid kryptering och dekryptering. Det innebär att både sändaren och mottagaren måste ha åtkomst till den nyckeln.

För asymmetrisk kryptering används i stället två olika nycklar, en publik och en privat. Vanligtvis används den publika nyckeln för att kryptera informationen medan den privata nyckeln används för dekryptering.

5.1 När ska kryptering användas

Kryptering ska användas vid:

- Identifierade lagkrav eller när risk för informationstillgångens konfidentialitet, äkthet eller riktighet identifierats.
- Överföring i offentligt eller öppet datanätverk, när information är klassad minst nivå 1 för konfidentialitet eller riktighet[4]

[3] För vägledning i att avgöra hur känslig information är finns regional rutin Informationsklassning
[4] Regional vägledning säkerhetsåtgärder

- Teknisk lagring av som är klassad nivå 2 eller högre för konfidentialitet eller riktighet[5]. För nivå 2 krävs minst kryptering på disknivå. Beroende på de identifierade riskerna kan kryptering behövas i andra lager, exempelvis fil, databas eller applikationsnivåer (se figur 1).
- Teknisk bearbetning av information när risk för informationstillgångens konfidentialitet, äkthet eller riktighet identifierats.
- Överföring av e-post när innehållet i meddelandet är sekretessbelagt eller känsligt. Information om kryptering av e-post i Outlook finns att läsa på VGR Serviceportal ”M365 Outlook – kryptering av e-post”[6].

Risk	Diskkrypteting	Filkryptering	Transparent datakryptering (TDE)	Applikationskryptering eller tokenisering
Data går inte att återställa när en hårddisk blir stulen eller förlorad.	✓	✓	✓	✓
Data är otillgänglig för root- och systemadministratörer.	✗	✓	✓	✓
Data är otillgänglig för databassadministratörer.	✗	✗	✓	✓
Data skyddad från hot som använder root-inloggningsuppgifter för dataexfiltrering.	✗	✓	✓	✓
Skapa detaljerade åtkomstloggar för efterlevnadsrapporter och hotanalys	✗	✓	✗	✓
Säkerställ att säkerhetskopior och snapshots är krypterade.	✗	✓	✓	✓
Ostrukturerad data, konfigurationsfiler, loggar, etc. är skyddade mot stöld och manipulation.	✓	✓	✗	✓
Undvik att bli bunden till hårdvaru- eller databasleverantörer	✗	✓	✗	✓

Figur 1 – Vad kryptering i olika lager kan åstadkomma.

För mer information om när kryptering ska användas finns vägledning i ytterligare dokument:

- Informationsklassning – Regional vägledning säkerhetsåtgärder

5.2 Verksamhetskritiska system

För system som är kritiska för verksamheter eller VGR som helhet ska även information som bearbetas i minne och processor krypteras och vald krypteringsmetod ska dokumenteras i designspecifikationen (ADD)

[5] Regional vägledning säkerhetsåtgärder
[6] M365 Outlook - kryptering av e-post

för systemet. Kryptering av information som bearbetas kan åstadkommas med exempelvis Intel Software Guard Extension (SGX) eller AMD Secure Encrypter Virtualization (SEV).

För skyddsvärden som berörs av säkerhetsskyddslagen ska av Försvarsmakten godkänd kryptering användas. Hantering av skyddsvärden sker inom ramen för VGR:s säkerhetsskyddsarbete.

5.3 Att tänka på vid val av krypteringsalgoritm

Krypteringsalgoritm ska följa branschstandard och inga kända sårbarheter får finnas. Lämplighet hos implementerade krypteringsalgoritmer ska bevakas. Om sårbarheter identifieras ska implementerade algoritmer uppdateras eller ersättas.

Till rutinen rekommenderas Ineras anvisning för kryptering[7]. För hashfunktioner rekommenderas NIST hash functions[8]. Ansvarig för att en tillräckligt säker kryptografisk lösning tillämpas och att regelbunden granskning utförs är ägare IS/IT-tjänst.

5.4 Hashfunktion

Kryptografisk hashfunktion innebär att en datamängd omvandlas till ett hashvärde bestående av en bestämd mängd siffror och bokstäver. Hashvärden är unika för datamängden och det går inte att återskapa den ursprungliga datamängden utifrån hashvärdet.

Hashing av den information som ska skyddas får inte vara möjlig att knäcka eller förbigå inom rimlig tid och inga kända sårbarheter får finnas. Vad som anses vara rimlig tid beror på känsligheten av den skyddade informationen. För att tillgodose detta krävs det regelbunden granskning av den tillämpade hashfunktionen för att säkerställa att inga nya brister identifierats.

Hashing, eller funktion med liknande säkerhet, ska användas för (men är inte begränsade till) följande funktioner:

- Teknisk lagring av inloggningsuppgifter. Inloggningsuppgifter ska aldrig sparas i klartext utan ska alltid tilldelas ett hashvärde.
- Teknisk lagring och verifiering av digitala signaturer.

[7] Anvisning Kryptering (rivta.se)
[8] Hash Functions | CSRC (nist.gov)

- Verifiera riktighet hos mottagna filer för att kontrollera att de inte ändrats under överföring. Där det är lämpligt ska säker digital kommunikation (SDK) användas.

5.5 Elektronisk underskrift

Elektronisk underskrift används för skydd mot förvanskning och säkerställande av ursprung och autenticitet av information. Implementation av elektronisk underskrift ska uppnå informationssäkerhetsmål om riktighet och oavvislighet samt enbart använda de gällande tjänster som är godkända av koncernstab digitalisering (KSD) och som har tilldelats ägandeskap. Detta gäller för elektronisk underskrift inom VGR samt med externa avtalspartner. Detta ska kravställas vid upphandling. Kvalité på underskrift och validering ska beakta informationens värde.

Information om när elektronisk underskrift bör användas finns på VGR:s intranät under “Elektronisk underskrift”.

6 Nyckelhantering

När en nyckel skapas ska användningsområde, beställare och ansvarig för krypteringsnyckeln dokumenteras i beställningsformuläret ”certifikat” i ärendehanteringssystemet Plexus. När nyckeln är skapad och ska levereras måste den skyddas med lika starkt skydd som krävs för informationen som nyckeln krypterar. Detta gäller för nyckeln under hela livslängden. En nyckel måste även ha ett bestämt slutdatum när den måste uppdateras eller tas ur bruk. Livslängden på nyckeln kan grundas i mängden arbete som behövs för att förnya nyckeln, när förnyelse är hanterbart (exempelvis för att undvika situationer när en stor mängd nycklar måste uppdateras samtidigt) samt risken att nyckeln blir röjd om den används för länge.

Ska nyckeln tas ur bruk ska det säkerställas att nyckeln destrueras så att återskapande inte är möjligt, detta gäller även för eventuella säkerhetskopior av nyckeln.

6.1 Att tänka på med krypteringsnyckel

Alla krypteringsnycklar ska skyddas mot ändring och förlust. Hemliga och privata nycklar måste dessutom skyddas mot obehörig användning och röjande. Det är ägare IS/IT-tjänst som ansvarar för att krypteringsnycklar hanteras säkert, är uppdaterade och att de inte blir röjda. Utrustning som används för att skapa, lagra och arkivera nycklar

ska skyddas fysiskt och endast vara åtkomstbara genom autentisering med flerfaktorsautentisering.

Om en misstanke uppstår att en obehörig användare kommer åt en nyckel, eller om nyckeln blir allmänt känd, ska detta skyndsamt hanteras som incident enligt regional incidenthanteringsrutin.

6.2 Beställa certifikat

Ett certifikat används för att autentisera olika typer av identiteter och för att säkerställa att information som skickas är säker och krypterad. Det används för kryptering, digitala signaturer och autentisering, exempelvis för att autentisera identiteten på en webbplats och skapa en säker anslutning med hjälp av kryptering. Det kan även användas för att autentisera en server som data skickas till och från och för att säkerställa integriteten hos nycklarna som används. Certifikat erhålls genom VGR:s serviceportal[9]. Det är även i serviceportalen som certifikat kan förnyas och återkallas.

6.3 Livscykelhantering

För att målet med kryptering ska uppnås krävs en korrekt livscykelhantering som involverar att skapa, använda, förvara och slutligen radera krypteringsnycklar. Livscykelhantering finns till för att minimera risken av att nycklar exponeras mot obehöriga och för att säkerställa att nycklar hanteras på ett säkert sätt. En bristande livscykelhantering kan leda till att säkerheten som kryptering erbjuder går förlorad, eller att nycklar inte går att återskapa vilket leder till dataförlust.

När kryptering används för känslig eller kritisk information samt där det finns lagkrav att informationen måste ha hög tillgänglighet ska säkerhetskopiering av nycklar ske för att säkerställa att ingen information går förlorad. Säkerhetskopian ska behandlas med samma försiktighet som den ursprungliga nyckeln.

7 Relaterade dokument

Elektronisk underskrift: Referensarkitektur för elektronisk underskrift och stämpel - Rev A (rivta.se)

Kryptering av e-post i Outlook: M365 Outlook - kryptering av e-post

[9] Certifikat finns i serviceportalen under ”Hem→Alla kataloger→IT→Nätverk→Certifikat”

Rutin informationssäkerhet för extern molntjänst 2024-2028: Informationssäkerhet för extern molntjänst - Regional rutin 2024 - 2028

Säker digital kommunikation: Regional rutin säker digital kommunikation (vgregion.se)

Stödjande dokument för kryptering: Anvisning Kryptering (rivta.se)

Stödjande dokument för kryptering och hashing: KLASSA - Vägledning för kryptografi (skr.se)

Stödjande dokument för hashing: Hash Functions | CSRC (nist.gov)

VGRs tjänst för PKI: VGR PKI - Koncernkontoret (vgregion.se)

Information om handlingen

Handlingstyp: Rutin

Gäller för: Västra Götalandsregionen

Innehållsansvar: Fredrika Holm Fredriksson, (freho10), Strateg

Granskad av: Anders Andersson, (andan18), Enhetschef

Godkänd av: Johan Flarup, (johfl), Direktör

Dokument-ID: RS10162-1596316381-219

Version: 2.0

Giltig från: 2025-01-24

Giltig till: 2029-12-31