



SVENLJUNGA  
KOMMUN

# riktlinje

---

## Riktlinje för kryptering

---

Beslutat av	Kommunstyrelsen
Beslutandedatum	2023-05-08, § 64
Ansvarig	IT-chef
Revideras	Vid behov
Följas upp	Årligen

---



# Innehållsförteckning

Inledning .....	3
Nyckelhantering .....	3
Riktlinjer för kryptering.....	4

## Inledning

Kryptering kan användas för flera ändamål, att förhindra obehörig åtkomst till information, eller genom kryptografiska signaturer garantera informationens riktighet eller äkthet.

IT-enheten ska vid behov tillhandahålla godkända krypteringslösningar och rutiner för hur dessa ska användas.

Implementerandet eller behov av kryptering ska baseras utifrån informationsklassning eller tekniska möjligheter, om behov finnes ska kryptering ske oberoende med undantag för tekniska förhinder. Undantag ska godkännas av informationssäkerhetsgruppen.

Vanligen finns behov av kryptering då det föreligger höga skydds krav på konfidentialitet och/eller riktighet.

Krypteringslösningar ska bygga på etablerade standarder och ska tas fram av IT-enheten i samråd med systemförvaltare och informationssäkerhetsgruppen.

Införande av krypteringslösningar ska prövas och godkännas av informationssäkerhetsgruppen

## Nyckelhantering

Ibland kan krypteringslösningar medföra nya risker relaterade till nyckelhantering. Dessa risker behöver hanteras bl.a. genom revokering, validering och återställning av nycklar:

- Genom revokering av nycklar görs det möjligt att spärra åtkomst till IT-resurser.
- Validering av nycklars giltighet och autenticitet möjliggör att användare av en IT-resurs kan avgöra om en nyckel är giltig och att innehavaren kan kontrolleras.
- Återställning av nycklar är en funktion för att göra det möjligt att återställa information även om nyckel förloras. Detta kan t.ex. åstadkommas genom användandet av en särskild återställningsnyckel eller genom att nycklar säkerhetskopieras.

Dock kan sådana lösningar innebära andra säkerhetsrisker eftersom

nycklarna finns på fler ställen, och det ställer stora krav på åtkomstkontroll, administrativa rutiner och loggning så att åtkomst till nycklar kan spåras.

## Riktlinjer för kryptering

- Krypteringslösningar ska baseras på etablerade standarder och införande ska godkännas av informationssäkerhetsgruppen.
- Nyckelhantering ska säkerställas för att tillgodose de krav som finns för IT-resurs avseende
  - Revokering av nycklar
  - Validering av nycklars giltighet och autenticitet
  - Återställning av nycklar
- Krypteringsnycklar är konfidentiell information och ska skyddas därefter.
- Rutiner för hantering av kryptografiska nycklar ska vara dokumenterade och belysa aspekter som hur nycklarna tas fram, hur de lagras och hur åtkomst ska ske.