Instruktion, nyckelhantering för lagrade krypterade data

Instruktion för nyckelhantering till lagrad och krypterade data för tjänster som Inera tillhandahåller

V1.0

Reviderat och godkänt av Fredrik Rosenberg och Bengt-Göran Andersson

Datum
2019-09-03

Innehåll

1. Dokumentinformation

1.1 Revisionshistorik

Version	Revision Datum	Beskrivning av ändringar	Ändringarna gjorda av
0.8	2019-06-10	Första utkast, baserat på MSB:s Vägledning för grundläggande kryptering	Bengt-Göran Andersson, Inera
0.81	2019-08-21	Referenser uppdaterat	Bengt-Göran Andersson, Inera
1.0	2019-09-03	Version 1.0 tillsammans med Anvisning för kryptering v3.1	Bengt-Göran Andersson, Inera

1.2 Revidering

Instruktion, nyckelhantering till lagrade krypterade data ska revideras årligen eller när skäl finns att uppdatera hela eller delar av dokumentet. Revisionsinformation dvs. nuvarande status på anvisningen finns på första sidan.

Ineras Informations- och IT-säkerhetsfunktion är ägare av denna instruktion och ska ses som en bilaga till Anvisning för kryptering_v3.1 [R1].

Det åligger varje e-tjänsteförvaltning att följa denna anvisning.

2. Inledning

Baserat på MSB:s kommande ”Vägledning för grundläggande kryptering” 2019-01-21, kapitel 12 [R2].

3. Mål

Målet är att vidta åtgärderna för att hantera av nycklar sker på ett säkert och korrekt sätt.

3.1 Bakgrund

3.1.1 Omfattning

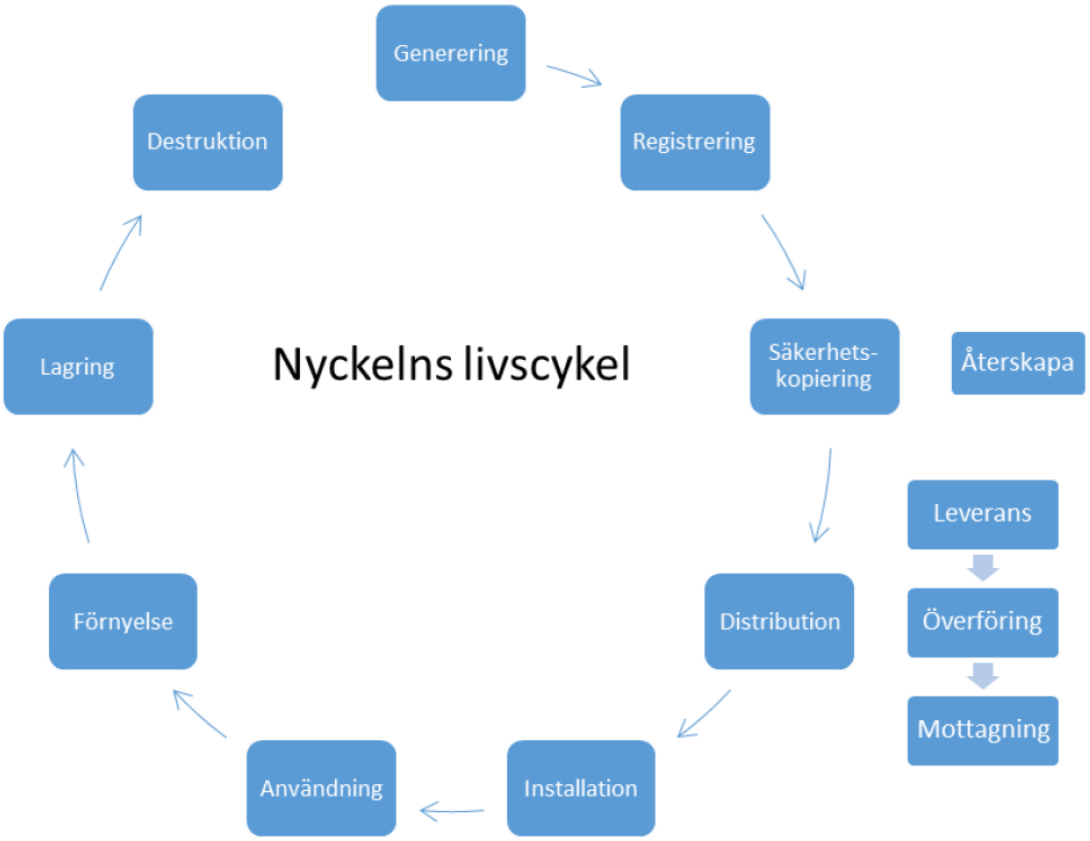
Denna instruktion beskriver regler och rutiner vilka är nödvändiga för en säker hantering av kryptografiska nycklar för krypterad och lagrade data.

3.1.2 Syfte

I teorin kan de flesta kryptografiska algoritmer forceras genom kryptoanalys. Detta kräver i realiteten en ytterst svåråtkomlig mängd datorkraft och resurser. Därför blir en forcering av algoritmen i praktiken en omöjlighet – såvida rätt algoritm, protokoll och nyckellängd väljs och är korrekt implementerade. Om kryptonyckeln röjs finns däremot inget behov av att angripa algoritmen.
Angrepp mot kryptolösningar kommer alltid att riktas mot den svagaste länken, vilket ofta är hanteringen av nyckeln. Därmed är säker nyckelhantering en kritisk komponent vid användning av kryptografi. Otillräckligt skydd av nyckelhantering innebär att hela kryptolösningens säkerhet äventyras.
För att krypteringen ska vara effektiv måste kryptonycklarna skyddas på den nivå som motsvarar det identifierade skyddsbehovet för informationstillgången som ska skyddas i okrypterad form. Det vidtagna skyddet av nyckeln ska gälla under hela nyckelns livslängd, givet att skyddsbehovet hos informationstillgången den skyddar består.

3.1.3 Om nyckelhantering

Instruktionen för nyckelhantering omfattar alla nödvändiga åtgärder för att skapa, skydda, kontrollera användandet och utplånandet av kryptonyckeln. Hela processen från att en kryptonyckel skapas tills det att den ska förstöras kallas för nyckelns livscykel (eng. *key management life cycle*) och) med referens till [R2] :



3.1.4 Risker

Det finns två stora risker relaterat till nyckelhantering:

- Att nycklar exponeras mot obehöriga individer eller applikationer (dvs. att konfidentialiteten för nyckeln som informationstillgång går förlorad), vilket eventuellt kan leda till förlust av skyddet som kryptolösningen erbjuder och informationen som denna skyddar.
- Förstörda nycklar som inte kan återskapas, vilket medför att de data som krypteras med nyckeln går förlorat.

Kryptonycklar kan lagras i kryptografiska hårdvarumoduler (HSM), på smarta kort och som filer. Vid mjukvarubaserad nyckelhantering innebär att skyddet av nycklar är begränsat till mjukvarans förutsättningar.
Bristfällig förståelse och dokumentation av processer och aktiviteter kopplade till nyckelhantering försvårar arbetet och riskerar säkerheten för kryptolösningen.
Hur nyckeln ska hanteras beror bl.a. på

- skyddsbehovet av den krypterade informationen
- mängden data och nycklar
- format på nycklar
- hastigheten och frekvensen av transaktioner

3.1.5 Återskapa nycklar

En förlorad krypteringsnyckel medför att de data som krypteras med nyckeln går förlorat. Det bör finnas möjlighet att säkerhetskopiera nyckeln. Observera att säkerhetskopian av nyckeln måste skyddas på samma sätt som originalet. En riskanalys bör ligga till grund för huruvida en nyckel ska gå att återskapas vid en situation där den går förlorad. Här ställs behoven av att skydda tillgängligheten till en informationstillgång mot att skydda konfidentialiteten av den samma.

3.1.6 Dubbelkommando vid aktivering av nycklar

För att undvika att kryptonycklar aktiveras, eller återskapas, av endast en person finns det en möjlighet att använda sig av s.k. dubbelkommando. Rekommendationen att mer än en person är närvarande vid aktiveringen/återskapandet av nyckeln bör implementeras som säkerhetsåtgärd.
Ett exempel på dubbelkommando kan vara av formen ”***M***-of-***N***”, vilket innebär följande:
För att en nyckel ska kunna aktiveras utdelas aktiveringsinformation till ***N***-stycken individer, system eller enheter. Uppdelningen ska medföra att en aktivering endast kan ske om en tillräckligt stor andel av ***N*** hjälps åt. Detta antal benämns som ***M***. Ifall färre än ***M***-stycken sammanträder kan inte nyckeln aktiveras.
Minsta värde på ***N*** är tre och ***M*** är två. För att aktivera nyckeln krävs då att två av de tre individerna samverka.

3.1.7 Regler för kryptografiska system och nycklar

Ett stöd i arbetet att hantera kryptografiska nycklar är att ha ett framtaget regelverk, nyckelhanteringsplan (eng. Key Management Plan, KMP). Exempel på innehållet i ett sådant regelverk beskrivs i tabellen nedan:

ÄMNE	INNEHÅLL
BESKRIVNING AV KRYPTOLÖSNINGEN	• Miljön där kryptolösningen används • Informationsklassningen för hanterad information • En beskrivning över kryptolösningen som även innehåller dataflöden • Användningen av nycklar • Nyckelalgoritmer • Nyckellängder • Livslängd för nycklar
NYCKELINCIDENTER	• En beskrivning av de fall då en nyckel inte längre kan anses säker • Hänvisningar till de procedurer som ska följas vid rapportering och hantering av säkerhetsincidenter.
NYCKELHANTERING	• Hur nycklar genereras. som genererar nycklar • Om någon nyckel ska publiceras och i så fall var och hur • Hur nycklar ska leverans till system där de ska användas. • Om och hur kvittens av mottagning av nycklar ska göras • Hur nycklarna får distribueras till nya IT system • Hur nycklarna ska installeras • Överföring av nycklar • Var nycklar får lagras, och vilket skydd som behövs där • Om och i så fall hur nycklar får återskapas • Hur nycklar ska förstöras
REFERENSER	• Kryptolösningens dokumentation • Eventuell övrig relevant dokumentation över funktion eller användning

4. Åtgärder

4.1 Nyckelhanteringsplan

Moderna kryptolösningar är designade för att kunna motstå kryptoanalys. Ett antagande är att eventuella angripare har möjlighet att läsa ut hur krypteringen sker. Krypteringens säkerhet bygger istället på fysiska, organisatoriska och förfarandemässiga säkerhetsåtgärder såsom nyckelhanteringsplaner med regler och rutiner.
En nyckelhanteringsplan är det regelverk som beskriver skyddet av kryptonycklar.

4.1.1 Rekommendation

- Regler för användning, skydd och giltighetstid för kryptografiska nycklar för deras hela livscykel ska utvecklas och införas i organisationen.

4.2 Kryptonycklars livslängd

Kryptonycklar ska skapas med en förutbestämd livslängd. Det ska finnas rutiner för att förnya eller bytas ut nyckeln i samband med att livslängden
närmar sig sitt slut. Livslängden (eng. cryptoperiods) för nyckeln varierar beroende på faktorer så som informationens behov av skydd, möjligheten för organisationen att skydda nyckeln och produkten.13 Ofta kan produktens dokumentation innehålla rekommendationer gällande nycklars livslängder.

4.2.1 Rekommendation

- Livslängden för en kryptonyckel ska baseras på en riskanalys där hänsyn tas till skyddsbehovet hos informationen, möjligheten att skydda nyckeln över tid, val av krypteringsalgoritm samt produktens dokumentation.
- Beslut om livslängden för kryptonycklar ska dokumenteras.
- Beslutade livslängder för olika typer av kryptonycklar ska finnas för alla organisationens krypteringslösningar.

4.3 Vid röjande av nycklar

Kommer obehörig åt kryptonyckeln har denne möjlighet att ta del av all den information som krypterats med den aktuella nyckeln. En kryptonyckel kan finnas i flera exemplar, dvs. den kan användas för kryptering av information som förmedlas till och från flera olika IT-system.
Det är viktigt att den som misstänker att en nyckel röjts omedelbart rapporterar detta som en nyckelincident. De åtgärder som måste vidtas ska ske skyndsamt. Detta för att skadan ska bli så begränsad som möjligt. Hur allt detta ska gå till i praktiken ska vara en del av en organisations nyckelhanteringsplan

4.3.1 Rekommendation

- Nycklar ska omedelbart bytas ut vid misstanke om att de har röjts – dvs. att en nyckelincident inträffat.
- Informationsägaren (eller den med motsvarande roll) för den information som kan vara påverkad av att nyckeln är röjd ska informeras om händelsen.

5. Referenslista

Ref	Dokumentnamn	Dokument
R1	Anvisning för kryptering v3.1	https://rivta.se/documents
R2	Vägledning för grundläggande kryptering OBS	https://kryptera.se/assets/uploads/2019/02/vacc88gledning-grundlacc88ggande-kryptering-focc88r-kommentarer.pdf