Kortliste krav til krypto

Forkortet kravliste til krypto for beskyttelse av lavgradert og sensitiv informasjon.

Bakgrunn

Kryptografiske mekanismer er implementert i mange komponenter og moduler av IT-systemer og er en forutsetning for elektronisk informasjonssikkerhet. For å være sikker på at en mekanisme kan benyttes i graderte informasjonssystem og brukes til å beskytte gradert og sensitiv informasjon, må mekanismene oppfylle noen grunnleggende krav.

NSMs krav til krypto er spesifisert i *NSM Cryptographic Requirements* (NCR), tilgjengelig for nedlastning fra NSMs hjemmeside. NCR presenterer tre nivåer til styrke for kryptografiske mekanismer. De ulike nivåene gjelder i følgende tilfeller:

> *ENHANCED* – Kryptografiske mekanismer for beskyttelse av gradert informasjon opp til og med STRENGT HEMMELIG mot enhver trussel.
>
> *STANDARD* – Kryptografiske mekanismer for beskyttelse av BEGRENSET informasjon mot enhver trussel og kryptografisk separasjon av ulike informasjonssystem som kjører i partisjonert operasjonsmåte. *NSM anbefaler i tillegg disse mekanismene for beskyttelse av svært sensitiv, men ugradert informasjon.*
>
> *MODERATE* – Kryptografiske mekanismer for beskyttelse av gradert informasjon innad i informasjonssystem som kjører i fellesnivå operasjonsmåte. *NSM anbefaler i tillegg disse mekanismene for beskyttelse av sensitiv, men ugradert informasjon.*

Introduksjon

Kortlistene presenterer de viktigste kravene til STANDARD og MODERATE. Det kan forekomme ytterligere muligheter i NCR enn det som presenteres her, men da er mekanismene som presenteres her de foretrukne.

Kravene er bygd opp rundt tre søyler som alle må være på plass for helhetlig kryptosikkerhet; robuste kryptomekanismer, evaluerte implementasjoner og sikker nøkkelforvaltning.

Under hver søyle er det et spørsmål om eget system som skal besvares. Når alle tre spørsmålene er besvart har man et godt utgangspunkt for videre dialog med NSM, enten det gjelder godkjenning av kryptoløsninger i graderte systemer eller råd- og veiledning innen kryptoløsninger generelt.

Ved etablering av nye systemer, anbefales det å sende dette dokumentet til utviklere, leverandører og systemintegratorer og be dem besvare spørsmålene. På den måten kan man enkelt få oversikt over sikkerhetstilstanden og modenheten til ulike leverandører og produkter. Dersom man benytter utviklere i utlandet anbefales det å oversende *NSM Cryptographic Requirements* som er på engelsk.

Innholdsfortegnelse

Kortliste krav til krypto på nivå STANDARD

Sikkerhetsfunksjon - Kryptografiske mekanismer (NCR kapittel 6 og 7)

Det er viktig å benytte en korrekt kryptografisk mekanisme for den sikkerhetsfunksjonen man ønsker. Som oftest vil det være sikkerhetsfunksjoner som krever at flere av disse mekanismene benyttes sammensatt.

Funksjon	*Mekanisme*	*Nøkkellengde*
Avtrykk	SHA-2	256, 384, 512
Konfidensialitetsbeskyttelse	AES	128, 256
Nøkkeletablering	EC-DH	256, 384
Integritetsbeskyttelse	EC-DSA	256, 384

✓ *Hvilke mekanismer benyttes hvor og til hva?*

Tillit – Evaluering og sertifisering (NCR kapittel 8.1)

For å være sikker på at mekanismene er implementert og utføres på en sikker måte, skal alle moduler som håndterer nøkler være evaluert og sertifisert.

System	*Standard*	*Nivå*
Kryptomodul[1]	Common Criteria (CC)	2, 3, 4
	FIPS 140-2	1, 2, 3, 4
Nøkkelmodul[2]	CC (BSI-PP-0035/BSI-CC-PP-0084-2014)	4, 5

✓ *Hvilke evalueringer og sertifiseringer har de ulike komponentene i løsningen?*

Nøkkelforvaltning (NCR kapittel 9 og 10)

Nøkkelforvaltning gjelder fra nøkler genereres til de slettes, og inkluder oversikt over og kontroll med alle kryptonøkler som er i bruk, samt tiltak for å hindre kompromittering og misbruk. NSM ønsker at nøkler sikres best mulig (langtidsnøkler forvaltes i maskinvarebasert nøkkelmodul) slik at det kan være minst mulig begrensninger på bruk av dem (tillates brukt i flest mulige applikasjoner og tjenester).

Funksjon	*Krav*
Administrasjon, kontroll og oversikt	Digitale sertifikater skal utstedes under NSM-godkjent offentlig nøkkelhierarki (PKI)
Langtidsnøkler	Genereres, brukes og slettes i nøkkelmodul
Sesjonsnøkler	Kan genereres, brukes og slettes i kryptomodul, men bør genereres i nøkkelmodul.

✓ *Hvor og hvordan genereres, brukes, beskyttes og slettes kryptonøkler og digitale sertifikater?*

[1] Dersom sertifiseringen av IT-produktet ikke inkluderer evaluering av kryptomodulen, må denne evalueres.
[2] Smartkort i ulike formfaktorer og med ulike fysiske grensesnitt

Kortliste krav til krypto på nivå MODERATE

Sikkerhetsfunksjon – Kryptografiske mekanismer (NCR kapittel 6 og 7)

NSM anbefaler at samme mekanismer som for STANDARD benyttes for MODERATE. NSM åpner allikevel for bruk av RSA- og DH-baserte kryptomekanismer ut 2019, men dette er for bruk i eksisterende løsninger. Nye løsninger bør ikke benytte disse.

Funksjon	*Mekanisme*	*Nøkkellengde*
Avtrykk	SHA-2	256, 384, 512
Konfidensialitetsbeskyttelse	AES	128, 256
Nøkkeletablering	EC-DH	256, 384
	RSA/DH	2048, 3072, 4096
Integritetsbeskyttelse	EC-DSA	256, 384
	RSA	2048, 3072, 4096

✓ *Hvilke mekanismer benyttes hvor og til hva?*

Tillit – Evaluering og sertifisering (NCR kapittel 8.2)

NSM anbefaler at samme nøkkelmoduler som for STANDARD benyttes for MODERATE, men aksepterer bruk av generelle kryptomoduler som både håndterer lang- og korttids kryptonøkler og utfører kryptomekanismer.

System	*Standard*	*Nivå*
Krypto-/nøkkelmodul	Common Criteria	2, 3, 4, 5
	FIPS 140-2	1, 2, 3, 4

✓ *Hvilke evalueringer og sertifiseringer har de ulike komponentene i løsningen?*

Nøkkelforvaltning (NCR kapittel 9 og 10)

Sikker nøkkelforvaltning inkluderer oversikt over og kontroll med alle kryptonøkler som er i bruk, samt tiltak for å hindre kompromittering og misbruk. NSM anbefaler derfor at nøkkelmodul benyttes for MODERATE som for STANDARD, men tillater at kryptomodul også benyttes for nøkkelmodul.

Funksjon	*Krav*
Administrasjon, kontroll og oversikt	Digitale sertifikater skal utstedes under offentlig nøkkelhierarki (PKI) underlagt norsk lovgivning[3]
Langtidsnøkler	Genereres, brukes og slettes i krypto-/nøkkelmodul Nøkkellevetid er avhengig av hvilken modul som benyttes
Sesjonsnøkler	Genereres, brukes og slettes i krypto-/nøkkelmodul

✓ *Hvor og hvordan genereres, brukes, beskyttes og slettes kryptonøkler og digitale sertifikater?*

[3] I graderte IT-systemer skal sertifikatpolicy være godkjent av NSM

Vedlegg 1: Anvendelser

Krypterte minnepinner – Krypterte minnepinner gir konfidensialitetsbeskyttelse av informasjon. NSM anbefaler at minnepinner kun benyttes når man skal distribuere data fra ett system til ett annet eller når man tar med seg dokumenter og presentasjoner til møter. Ved bruk av minnepinner til langtidslagring er det stor risiko til at de går i stykker. Det er dessuten spesielt vanskelig å ha en god nøkkelhåndtering for krypterte minnepinner, noe som er en forutsetning for langtidslagring.

- Siden samme bruker både låser ned og låser opp minnepinnen, blir ikke distribusjon av nøkkel utfordrende. Det anbefales å benytte smartkort for nøkkelgenerering, -beskyttelse og sletting, slik at uvedkommende ikke kan gjette seg til passordet/nøkkelen. Slike løsninger kan håndteres ene og alene av brukeren.

Harddiskkryptering - Harddiskkryptering sikrer i hovedsak konfidensialitetsbeskyttelse av data når datamaskinen er avslått. Dermed er dataene sikret dersom datamaskinen mistes eller stjeles. Man kan også benytte harddiskkryptering for integritetsbeskyttelse av systemet, da i kombinasjon med *Trusted Platform Module* (TPM). Harddiskkryptering kan også forenkle avhending av harddisker, da disse kan anses sikkert slettet når nøkkelen er sikkert slettet.

- For å sikre at ikke tap av nøkkel gir tap av data, bør man sørge for sikkerhetskopi av nøkkel. Dersom man stadig er på nett og kan synkronisere data, kan man sørge for at data ikke går tapt selv om nøkkel går tapt. Slike løsninger bør håndteres av IT-avdelingen.

Kryptert epostoverføring – For å konfidensialitetssikre overføring av epost må man sikre både kommunikasjonen mellom epost-klient og epost-tjener, og mellom epost-tjenere. Til dette benyttes som regel Transport Layer Security (TLS) med ulike protokoller. For kommunikasjon mellom epost-tjenere kalles varianten STARTTLS.

- Siden mottaker må installere sertifikat, må dette være tiltrodd hos alle avsendere. Det er derfor viktig at sertifikatet kommer fra en offentlig tiltrodd tredjepart. For TLS for ugraderte anvendelser anbefaler NSM sertifikater fra Buypass.

Signering av epost – For endringsbeskyttelse av epost må hver epost signeres. Dette hindrer ikke innsyn, men at uvedkommende kan endre innholdet under overføring uten å bli oppdaget. Dette gjøres enklest ved hjelp av digitale sertifikater og S/MIME-signering av eposten.

- Siden mottaker må gjenkjenne sertifikatet eposten er signert med, må avsender benytte et sertifikat fra en offentlig tiltrodd tredjepart (kommersiell PKI-leverandør).

Sikkert nettsted –For å autentisere nettsted og konfidensialitetsbeskytte overføringen av informasjon til og fra nettstedet, må man benytte digitale sertifikater og TLS.

- Siden den som kobler seg til må stole på sertifikatet nettstedet er bundet til, må sertifikatet være utstedt av en offentlig tiltrodd tredjepart. For TLS for ugraderte anvendelser anbefaler NSM sertifikater fra Buypass.

Sikker fjerntilgang - Sikker fjerntilgang er en sikker forbindelse mellom mobile enheter, som bærbare PC-er og smarttelefoner, og bedriftens interne nett. Ved å etablere en kryptert «tunnel» til hjemmenettet vil klienten få tilgang til bedriftens informasjon uten at uvedkommende får avlyttet trafikken.

- Ved å utstede digitale sertifikater for IPSec eller TLS til klienter og fjerntilgangstjener, vil man enkelt kunne konfigurere sikker fjerntilgang. Etablering av offentlig nøkkelinfrastruktur for utstedelse av digitale sertifikater vil være mer utfordrende enn å kjøpe sertifikater fra tiltrodde tredjeparter, men gir muligheter for nye ytterligere sertifikater og anvendelser.