HELSE SØR-ØST

Fellesregional Kryptopolicy

Versjonsnummer	**Dato**	**Godkjent av**
1.0	22.12.2016	
1.1	23.10.2018	

1 Hensikt og omfang

Dette dokumentet er felles regional instruks for bruk av kryptering. Instruksen er rettet til Sykehuspartner og andre leverandører av IKT-tjenester i Helse Sør-Øst.

2 Ansvar

- **Administrerende direktør:** Er databehandlingsansvarlig og har ansvaret for at lagring og forvaltning av helse- og personopplysninger gjøres med nødvendig sikkerhet og kun i samsvar med gyldig behandlingsgrunnlag.
- **Informasjonssikkerhetsleder:** Har det utøvende ansvar for virksomhetens informasjonssikkerhetsarbeid, blant annet ved å godkjenne risikovurderinger og utføre internkontroll med informasjonssikkerheten i virksomheten.
- **Personvernombudet:** Har en rolle i å sikre at den enkeltes personvernrettigheter blir ivaretatt, at all bruk av personopplysninger skjer i samsvar med gyldig behandlingsgrunnlag og følger virksomhetens retningslinjer for informasjonssikkerhet.
- **Ledere** på alle nivåer har ansvar for oppfylling av dokumentet i egen enhet.
- **Alle ansatte og innleide** ved virksomheten som skal lagre og behandle helse- og personopplysninger, skal forholde seg til denne instruksen. Dette gjelder uavhengig av organisatorisk plassering og yrkesgruppe.

3 Fremgangsmåte

3.1 Godkjente algoritmer

Generelt for kryptografi kreves at det ikke benyttes nøkler og algoritmer som har kjente svakheter. Listen i dette kapittelet skal revideres minimum årlig, eller i tilfeller der nye sårbarheter blir kjent. Bruk av ikke godkjente algoritmer skal ikke forekomme dersom det ikke er tvingende nødvendig. Slik bruk skal alltid risikovurderes, og avvikshåndteres spesielt, med sikte på å lukke avviket.

Funksjon	**Mekanisme/algoritme**	**Nøkkellengde**	**Kommentar**
Avtrykk (Hash)	SHA-2	256, 384 eller 512 bits	SHA-3 vil også aksepteres når støtte for dette er klart

Konfidensialitetsbeskyttelse (Symmetrisk kryptografi)	AES	128 eller 256 bits	
Nøkkeletablering	EC-DH	256 eller 384 bits	
Nøkkeletablering	RSA/DH	2048, 3072 eller 4096 bits	Gyldig ut 2019. Etter dette er kun EC-DH godkjent
Integritetsbeskyttelse (Asymmetrisk kryptografi, signering)	EC-DSA	256 eller 384 bits	
Integritetsbeskyttelse (Asymmetrisk kryptografi, signering)	RSA	2048, 3072 eller 4096 bits	Gyldig ut 2019. Etter dette er kun EC-DSA godkjent

3.2 Kryptering under transport av data

Data som transporteres utenfor fysisk kontroll skal alltid, uansett medium, krypteres.

Data som transporteres innenfor fysisk kontroll skal alltid krypteres så langt det ikke medfører vesentlige ulemper. Ulempene skal dokumenteres, og følges opp som avvik. En risikovurdering skal avdekke hvorvidt manglende kryptering er innenfor risikoakseptkriterier.

Ved bruk av symmetrisk kryptering skal nøkkelutveksling i hovedsak skje ved asymmetrisk kryptering (også kalt offentlig nøkkel-kryptering). Unntak fra bruk av asymmetrisk kryptering må inngå i en risikovurdering i hvert enkelt tilfelle.

3.3 Kryptering under lagring av data

Data lagret på mobile eller bærbare enheter skal krypteres, gjerne gjennom kryptering av hele enheten. Dette gjelder også bærbare lagringsenheter, slik som minnepinner og eksterne harddisker.

I databaser og på filsystem tiltenkt permanent eller midlertidig lagring av data, skal som hovedregel kryptering implementeres.

Kryptering kan benyttes som skillemekanisme i tilfeller hvor data lagres i regionale løsninger hvor det inngår flere juridiske virksomheter. Data må da krypteres av virksomhetsspesifikke nøkler.

3.4 Kryptering under behandling av data

Kryptering er ikke et krav for behandling av data, men behandling av data skal alltid risikovurderes. Kryptering er bare ett av tiltakene som kan vurderes i forbindelse med sikring av data under behandling.

3.5 Tekniske krav til nøkkelforvaltning

I samsvar med NSMs anbefaling, kreves det separat, hardware-basert sikkerhetsmodul – såkalt HSM-modul – for generering og lagring av private nøkler for utstedelse. Denne kan være koblet til hver enkelt tjener, eller man kan benytte nettverksbasert HSM. Usteder-CA skal generere og lagre privatnøklene sine på HSM modulen. For andre tjenester er bruk av HSM anbefalt, men valgfritt.

En nettverksbasert HSM anbefales, da dette gir størst fleksibilitet og økt gjenbrukbarhet. HSM-modulen må følge Common Criteria nivå 2,3,4 eller 5, og/eller FIPS 140-2 nivå 1,2,3 eller 4, jamfør NSM sine anbefalinger.

3.6 Krav til sertifikater

1. Eksterne sertifikater:
    a. Sertifikatet skal være utstedt av en offisiell, og av informasjonssikkerhetsleder i virksomheten, godkjent, standard CA
    b. Oversikten over godkjente sertifikatutstedere skal finnes som en del av Sykehuspartners ISMS
    c. For kvalifiserte sertifikater gjelder NKOMs oversikt her.
    d. Manuelt utstedte sertifikater skal ha en levetid på maksimalt 1 år.
    e. Sertifikater som fornyes automatisk skal ha en levetid på maksimalt 3 måneder
    f. Personlig Kvalifiserte sertifikater skal ha en gyldighet på maksimalt 3 år

2. Interne sertifikater:
    a. Være utstedt under Sykehuspartners regionale PKI, når denne kommer på plass. Alternativt kan også disse benytte samme utsteder som eksterne sertifikater. Eventuelle risikoer ved en slik bruk må risikovurderes.
    b. Interne sertifikater skal utstedes under EN felles rot. Det er ikke anledning til å opprette nye rot-CA eller utsteder-CA uten godkjenning av informasjonssikkerhetsleder.
    c. Manuelt utstedte sertifikater skal ha en levetid på maksimalt 1 år.
    d. Sertifikater som fornyes automatisk skal ha en levetid på maksimalt 3 måneder
3. Sertifikatet skal være gyldig for alle FQDN-tjenernavn det skal brukes på.
4. «Wildcard»-sertifikater kan benyttes innenfor en og samme tjeneste, dersom dette er formålstjenlig.
5. Sertifikatets signatur og øvrige algoritmer må følge kravene i kapittel 5.1.
6. Eventuelle avvik fra disse kravene skal beskrives i en risikovurdering, og det skal utarbeides en plan for å lukke avvikene innen rimelig tid.

3.7 Krav til forvaltning av CA, sertifikater og private nøkler

Det skal finnes et forvaltningsregime for håndtering av sertifikatutstedere, rot-CA, sertifikater og private nøkler som minimum tilfredsstiller følgende krav:

1. Rot-CA skal oppbevares på kryptert, fysisk medium, og skal ALDRI tilkobles noe nett. Samme krav gjelder for backup av ROT. Dersom dette skjer, skal løsningen ansees som kompromittert, CERT varsles, og prosedyrer skal iverksettes for å rive samt gjenoppbygge infrastrukturen, slik at man igjen kommer på et tiltrodd nivå. Dette inkluderer revokering av samtlige sertifikater i løsningen. Det må finnes en rutine for å gjennomføre dette, tilknyttet krisehåndtering hos leverandøren.
    a. Patching av offline rot gjøres minimum i forbindelse med fornyelse av utsteder CA sertifikater.
2. Utsteder-CA (Issuing CA):
    a. CA skal være dokumentert
    b. CA skal minimum herdes i henhold til leverandørs anbefalinger og Sykehuspartners krav til herding. For Microsoft CA, se https://technet.microsoft.com/en-us/library/dn786426.aspx
    c. Privat nøkkel for CA skal lagres på HSM
3. Sertifikateier, med minimum epost til rolle, skal defineres i alle sertifikater som utstedes.
4. Sertifikateier har ansvaret for å sikre at sertifikatet blir fornyet i tide ved utløp.
5. Det skal til enhver tid finnes en oversikt over samtlige steder et sertifikat er benyttet. Sertifikateier har ansvaret for å vedlikeholde denne listen.
6. Sertifikatutstedelse skal revideres minimum årlig.
7. Det skal finnes en liste over godkjente bruksområder for sertifikater. Unntak fra denne skal avvikshåndteres, og godkjennes av informasjonssikkerhetsleder, eventuelt en av denne utpekt godkjenner. Godkjennelsen skal dokumenteres i systemdokumentasjon.
8. Det skal finnes en oversikt over aktive sertifikater som minimum inneholder følgende:
    a. Sertifikatets identitet
    b. Navn på vedkommende som godkjente utstedelsen av sertifikatet
    c. Sertifikateier (rolle eller person, med tilhørende epost)
    d. Formålet med sertifikatet, inkludert hvilke enheter det er brukt på.
    e. Hvor ble sertifikatet generert?
    f. Hvor er sertifikatet lagret?
    g. Sertifikatets gyldighet fra-til.
    h. Privatnøkkelens gyldighet fra-til.
    i. Informasjon om tilbaketrekning av sertifikatet, om relevant.

3.8 Spesielle krav

3.8.1 Spesielle krav for vevtjenester og HTTPS

Alle nettsteder driftes av Sykehuspartner eller andre leverandører, som har informasjon annet enn kontekst 1 – Åpen, inkludert alle sider som har noen form for pålogging, skal være utstyrt med digitalt sertifikat, og konfigurert for sikker kommunikasjon. Protokollstøtte er minimum som følger:

Protokoll	**Krav til bruk**	**Kommentar**

TLS 1.3	Når støttet av systemet	Ny versjon av protokollen, som har sterkere fokus på sikkerhet og ytelse.
TLS 1.2	Alltid	Så langt ingen påviste hull. Bør alltid foretrekkes
TLS 1.1	Hvis STRENGT nødvendig for kompatibilitet, må søkes deaktivert så snart som mulig	Så langt ingen påviste hull, men best practice sier at denne ikke aktiveres. Protokollen har vært lite i bruk,
TLS 1.0	Hvis STRENGT nødvendig for kompatibilitet, må søkes deaktivert så snart som mulig.	Det finnes sårbarheter (POODLE for TLS, mm) i denne protokollen. Bør deaktiveres dersom det ikke er strengt nødvendig for bakoverkompatibilitet.
SSL 3.0	Aldri	SSL 3.0 har flere kjente sårbarheter. Systemer der dette må være slått på må avvikshåndteres, og overvåkes spesielt.
SSL 2.0 og PCT 1.0	Aldri	

TLS-komprimering må ikke forekomme.

Se ellers punkt 4.1 for godkjente protokoller.

Utover disse kravene må nettstedet sikres mot manipulasjon og kjente svakheter. Følgende tabell brukes for å få en enkel oversikt over kravene:

Tjenerhode	**Anbefalt konfigurasjon**	**Beskrivelse**	**Krav**
Server	Anonymiseres	En angriper som vet hva slags teknologi nettstedet benytter, vil ha en lettere jobb i forbindelse med inntrenging.	Anbefalt
X-Frame-Options	«SAMEORIGIN»	Hindrer nettstedet i å bli puttet i ramme (iframe/frame) av andre nettsteder, som er en velkjent metode for informasjonsfisking.	Ja. Feltet må defineres, men eksakte valg som gjøres avhenger av nettstedet.

X-Xss-Protection	"X-XSS-Protection: 1; mode=block"	Blokkerer «cross-site scripting» angrep.	Ja. Avvik skal dokumenteres og følges opp.
X-Content-Type-Options	X-Content-Type-Options "nosniff"	Hindrer nettleseren i å «gjette» hva slags filer som lastes ned. Stopper visse former for angrep, der filer opptrer med feil utvidelse.	Anbefalt
Strict-Transport-Security	Strict-Transport-Security "max-age=31536000; includeSubDomains;	Dette tvinger samtlige nettlesere til å benytte HTTPS, og gjør at omdirigering blir unødvendig.	Ja. Avvik skal dokumenteres og følges opp.
Content-Security-Policy/ **X-Content-Security-Policy**	Avhengig av nettstedet. Anbefaler Content-Security-Policy: upgrade-insecure-requests	Sikrer at ingenting blir lastet på nettstedet som ikke kommer fra en godkjent liste nettsteder.	Anbefales, men krever testing. Høy modenhet ellers på nettstedet er en forutsetning. X-Content-Security-Policy må benyttes for å støtte IE 11 og eldre. Content-Security-Policy støtter Edge og andre nettesere.
Public-Key-Pins	Avhengig av sertifikat, men «public-key-pins-report-only»	Beskytter mot forfalskede sertifikater.	Anbefales ikke før øvrige krav er etterlevet, og da kun i report-only modus.
Referer-Policy	strict-origin-when-cross-origin	Begrenser URL informasjon i lenker ut	

3.8.2 Spesielle krav for ekstern e-postutveksling

Sykehuspartners og andre leverandørers e-postformidlere skal konfigureres til å foretrekke STARTTLS. De skal også konfigureres med offisielle sertifikater på samme måte som eksterne nettsteder.
Ellers anbefales bruk av Sender Policy Framework (SPF), Domain Keys Identified Mail (DKIM) og DMARC (Domain-based Message Authentication Reporting and Conformance).
SPF skal defineres med –all som sluttparameter. ~all kan benyttes i en testperiode.

DMARC skal defineres med parameter p=reject. p=quarantine er akseptabelt i en testperiode. Postboksen dmarc@[Leverandør] skal forvaltes.

I tillegg må innkommende MTA defineres til å avvise, eller karantinere innkommende epost der SPF, DKIM eller DMARC feiler sin verifikasjon.

Det anbefales også at DNSSEC vurderes implementert for domener tilgjengelig over internett. Dette muliggjør bruk av DANE (Domain based Authentication of Named Entities) for mail servere.
Se forøvrig NSM sine anbefalinger om sikker epostutveksling.

3.8.3 Spesielle krav til TLS konfigurasjon for Windows tjenere

NSM har laget en svært god veileder, med tilhørende verktøy for å tilfredsstille kravene. Heller enn å gjengi disse kravene og begrunnelsene her, lenkes det direkte til NSM sin dokumentasjon.

- NSM sine anbefalinger for sikring av Windows TLS.
- Zip-fil med skript og veiledning for å implementere anbefalingene.

Bruk av disse anbefalingene og kravene skal følge alle krav i dette dokumentet. Dette betyr:

Kapittel 3.1 Anbefalte TLS protokoller: Følges
Kapittel 3.2 Anbefalte cipher suiter: Foretrukne, Akseptable 1 og 2. Akseptable 3 og 4 kan benyttes dersom bakoverkompatibilitet med Windows XP er nødvendig.
Suitene skal angis i prioritert rekkefølge.

4 Definisjoner

- Kryptering er en matematisk metode for nedlåsing av informasjon slik at den ikke kan leses av uvedkommende.
- Kryptering er nødvendig for å oppfylle juridiske og avtalemessige krav til konfidensialitet og integritet i forbindelse med lagring, transport og behandling av informasjon.
- Herunder stilles krav til symmetrisk kryptografi (samme nøkkel benyttes både ved kryptering og dekryptering), asymmetrisk kryptografi (to nøkler benyttes, offentlig og privat), samt enveiskryptografi, såkalte hash-algoritmer. NSM omtaler dette som «avtrykk» i sin dokumentasjon. Vi stiller krav til både algoritmer og nøkkellengder.
- Sykehuspartner og andre leverandører skal følge NSM sine krav til kryptografi, og legger seg på nivå «MODERATE» i NSM Cryptographic Requirements. Dette er krav til kryptografi for ugradert informasjon.
- For samtlige krav gjelder at de skal etterleves så langt det er mulig. Der etterlevelse ikke er mulig, skal dette meldes som avvik i henhold til avviksprosessen, og det skal utarbeides en plan for å lukke avviket.
- Leverandører plikter å besvare om deres valg av krypteringsalgoritmer tilfredsstiller fellesregionale krav i Helse Sør-Øst.

- I hver enkelt risikovurdering skal det avdekkes hvorvidt krav til kryptering er ivaretatt, og hvordan avvik skal håndteres.
- Se ellers eget dokumentet Kilder og definisjoner i regionalt styringssystem for informasjonssikkerhet .

5 Avvik eller dissens

Avvik på denne instruks meldes i virksomhetens avvikssystem. Informasjonssikkerhetsleder og/eller personvernombud skal varsles.

6 Referanser

- Se dokumentet Sikkerhetsregulerende lovverk gjeldende for helseforetaksgruppen
- Prinsippene for anvendelse og forvaltning av dokumentet er beskrevet i dokumentet Overordnede prinsipper for regionalt styringssystem for informasjonssikkerhet