Vedlegg 11- Krav til kryptering av nettverkskommunikasjon

(transportkryptering)

Formålet med å kryptere nettverkskommunikasjon er å hindre andre enn de kommuniserende partene i å kunne få innsyn i eller uoppdaget manipulere informasjonen som kommuniseres.

Ved bruk av TLS skal det benyttes en versjon og cipher-suite som ikke innehar kjente svakheter

Rasjonale: Historisk har det vært mange utfordringer med TLS, og flere versjoner med kjente svakheter er fortsatt i bruk.

For kommunikasjon som beskyttes med TLS mellom tjenester/servere skal det benyttes gjensidig autentisering («toveis TLS»).

Rasjonale: Uten gjensidig autentisering er det kun tilkoplende part som vet hvem motparten er, dvs. at hvem som helst kan kople seg til det aktuelle grensesnittet. Ved gjensidig autentisering må også den som kopler seg til godkjennes av tjenesten.

Tabell 1 angir kombinasjoner av TLS-versjoner og ciphere, og status for bruk i Helse Nords systemer, angitt med farge på rad. Grønne funksjoner kan fritt benyttes. Gule kombinasjoner kan beholdes inntil videre der disse allerede er i bruk, men skal ikke brukes ved utvikling eller i anskaffelser. Røde kombinasjoner er å anse som usikre og bør byttes ut/skal ikke brukes.

Tabell 1:Cipher suites - status for bruk

Ver	Cipher suite	Beskrivelse
1.2	TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384 TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 TLS_RSA_WITH_AES_256_GCM_SHA384 TLS_RSA_WITH_AES_128_GCM_SHA256 TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256 TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 TLS_RSA_WITH_AES_128_CBC_SHA	
1.1	TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA TLS_RSA_WITH_AES_256_CBC_SHA TLS_RSA_WITH_3DES_EDE_CBC_SHA	
<1.1	Alle	TLS 1.0 og eldre utgaver (SSL 2.0/3.0) er å anse som usikre pga omfattende svakheter.

TLS-oppsett skal konfigureres slik at sikreste alternativ (cipher suite) foretrekkes. Perfect forward secrecy bør støttes.

Rasjonale: Det kan være nødvendig å støtte flere alternativer pga. begrensninger i motpartens utvalg av støttede ciphers, også svakere ciphers enn strengt tatt ønskelig. For å sørge for at størst mulig andel av sesjonene benytter sikrest mulig cipher blir det da viktig at server/tjeneste har satt prioritert rekkefølge. Perfect forward secrecy sørger for at tidligere sesjonsnøkler ikke kan gjenskapes, noe som gjør det svært vanskelig å dekryptere lagret trafikk selv om man skulle få tak i en av partenes private nøkkel.

Ved bruk av IPSec skal det så langt som mulig benyttes PKI-utstedte sertifikater og IKEv2 for nøkkelutveksling

Rasjonale: Bruk av sertifikater sikrer at man vet hvem man kommuniserer med, samt at det gir mulighet for revokering. Internet Key Exchange v2 er den foretrukne måten for å gjøre nøkkelutveksling når man benytter X509-sertifikater.

IPSec punkt til punkt skal brukes i ESP tunnel mode.

Rasjonale: IPSec brukes i hovedsak for VPN-formål, da er det ønskelig å også skjule de interne IP-adressene. Tunnel mode tillater også bruk av NAT.

IKE/IPsec skal konfigureres slik at sikreste alternativ (cipher suite) foretrekkes

Rasjonale: Kommuniserende parter forhandler fram en Security Assosciation (SA) vha IKE. Det kan være nødvendig å støtte flere alternative cipher suiter pga. begrensninger i motpartens utvalg av støttede ciphers, også svakere ciphers enn strengt tatt ønskelig. For å sørge for at størst mulig andel av forbindelsene benytter sikrest mulig cipher blir det da viktig at server/tjeneste har satt prioritert rekkefølge.

Gyldighetstiden for symmetriske nøkler skal ikke overstige 24t. For svake ciphers skal nøklene byttes minimum hver time.

Rasjonale: For VPN-tuneller og tilsvarende der det flyter mye informasjon, og der kryptering ikke styres av applikasjonslaget, er det viktig å begrense skaden om den symmetriske nøkkelen kompromitteres. Ved å bytte nøkkel ofte vil datamengden som er kryptert med samme nøkkel begrenses. Den enkleste måten å gjøre dette på er å benytte Perfect Forward Secrecy-kompatible cipher suites.