Nasjonal sikkerhetsmyndighet

Vår saksbehandler	Vår dato	Vår referanse
v/ Britt Jøsok	2012-10-02	A03 - S:12/01827-2
	Deres dato	Deres referanse
	2012-06-26	12/2016
	Antall vedlegg	Side
		1 av 2

Til
Fornyings-, administrasjons- og kirkedepartementet

Postboks 8004 Dep
0030 Oslo

Kopi til
FD

Høring - Forslag til endring i personopplysningsforskriften

Nasjonal sikkerhetsmyndighet (NSM) viser til brev av 26.06.12 der det bes om høringsuttalelse til forslag om endringer i personopplysningsforskriften, innen 01.10.12. NSM beklager at svaret sendes etter høringsfristens utløp.

NSMs kommentarer nedenfor er relatert til høringsnotatets del A.

NSM har i ulike sammenhenger tidligere avgitt høringsuttalelser i forbindelse med datalagringsdirektivet. Vi finner at våre synspunkter i disse sammenhengene også er relevant her, og legger derfor ved to tidligere brev med vedlegg.[1]

NSM mener at informasjonen i databasen bør krypteres for å beskytte både konfidensialitet, integritet og autentisitet.

Bruk av lukket lagring vil ikke fjerne behovet for kryptering. Om man velger å benytte fysisk beskyttelse for å sikre dataenes konfidensialitet, må man likevel bruke kryptering for å sikre dataenes integritet/autentisitet, i tillegg til systemets integritet, autentisitet og tilgjengelig. På denne måten kan man stole på dataene man henter ut. Etter NSMs oppfatning vil det ikke være tilstrekkelig med fysisk sikring i den forbindelse. Det må benyttes elektroniske mekanismer i tillegg.

For å sikre at det stilles krav til slike elektroniske beskyttelsesmekanismer foreslår NSM at forskriftsutkastet §7-1, 3.ledd litra d) endres til følgende ordlyd:

d) *Elektronisk sikring av lagringssystemet og lagret informasjon, for å sikre integritet, autentisitet og tilgjengelighet*

[1] Brev til Forsvarsdepartementet datert 10.04.12 med vedlegg av 07.09.11 og 17.01.12 (samt vedlegg 06.06.11)

Postadresse
Postboks 14
1306 BÆRUM
POSTTERMINAL

Sivil telefon/telefaks
+47 67 86 40 00/+47 67 86 40 09
E-postadresse
post@nsm.stat.no

Militær telefon/telefaks
515 40 00/515 40 09
Internetadresse (URL)
www.nsm.stat.no

Når det gjelder kravene i samme bestemmelse litra f) ønsker NSM å presisere at det vil være uheldig dersom det stilles ulike krav til krypteringsmekanismer, eller til implementeringen av disse, ved elektronisk forsendelse nasjonalt og ved forsendelse over landegrensene. NSM ser at litra f) gir NSM en rolle ifbm forsendelse av data over landegrensene, og ber om at det vurderes om dette kravet bør gjøres generisk ifht all bruk av kryptomekanismer.

NSM står til disposisjon for ytterligere informasjon og begrunnelse dersom det er behov for dette.

Med hilsen

for Kjetil Nilsen

Direktør NSM

Nasjonal sikkerhetsmyndighet

Vår saksbehandler
v/ v/ Britt Jøsok

Vår dato
2012-04-10

Vår referanse
A03 - S:12/00274-2

Deres dato
2012-02-14

Deres referanse
2009/02874-35/FD

Antall vedlegg

Side
1 av 2

Til
Forsvarsdepartementet

Postboks 8126 Dep
0032 Oslo

Kopi til

Høringsnotat og forskriftsutkast - Datalagringsforskriften

Nasjonal sikkerhetsmyndighet (NSM) viser til brev fra Forsvarsdepartementet til NSM av 14.02.12, samt til purring pr epost datert 30.03.12. NSM ble gitt ny frist for innspill til den 10.04.12. NSM beklager at det ikke har vært mulig å gi tilbakemelding innen den opprinnelige fristen.

NSM har i tidligere uttalelser ment noe om behovet for, og kravene som bør stilles til, bruk av krypto i forbindelse med lagring av data i denne sammenheng. NSM har avgitt både en generell uttalelse til Justisdepartementet datert 07.09.11 og en konkret uttalelse datert 17.01.12 til Datatilsynets forslag til konsesjon som har vært på høringsrunde. NSM finner at begge disse uttalelsene er relevante også i denne sammenheng, og vedlegger derfor kopi av begge brevene.[1][2]

Når det gjelder Post- og teletilsynets forslag til forskrift §§ 3-1, 3-2 og 3-3, mener NSM at grenseflatene mot Datatilsynets konsesjon er uklare. Datatilsynets konsesjon skal håndtere eventuelle krav til krypto. De nevnte bestemmelsene handler imidlertid om å sikre henholdsvis dataenes integritet og/eller konfidensialitet. Det er ikke sagt noe om hvordan man skal kunne sikre dette, eller hvordan dette er forventet implementert hos lagringspliktige. NSM kan imidlertid ikke se at dette kan gjøres på en tilfredsstillende måte uten å stille krav om bruk av kryptografiske mekanismer.

NSM mener derfor at kravene i §§ 3-1, 3-2 og 3-3 må spesifiseres nærmere og eventuelt harmoniseres med kravene som Datatilsynet stiller i konsesjonen til de lagringspliktige.

Med hilsen

for Kjetil Nilsen
Sjef NSM

---

[1] Kopi av brev fra NSM til JD datert 07.09.11
[2] Kopi av brev til Datatilsynet 17.01.12

Postadresse
Postboks 14
1306 BÆRUM
POSTTERMINAL

Sivil telefon/telefaks
+47 67 86 40 00/+47 67 86 40 09
E-postadresse
post@nsm.stat.no

Militær telefon/telefaks
515 40 00/515 40 09
Internetadresse (URL)
www.nsm.stat.no

Nasjonal sikkerhetsmyndighet

Vår saksbehandler
Lars Olaussen
+47 67864323, 0515 4323
lars.olaussen@nsm.stat.no

Vår dato
2011-09-07

Tidligere dato

Vår referanse
2011/00950-002/NSM/430

Tidligere referanse

Til
Justis- og politidepartementet

Kopi til
Forsvarsdepartementet

Internt

Intern kopi

Oppfølging av Stortingets vedtak om gjennomføring av EUs datalagringsdirektiv i norsk rett - retningslinjer om kryptering

1 Bakgrunn

I forbindelse med Stortingets vedtak om gjennomføring av EUs datalagringsdirektiv har Transport- og kommunikasjonskomiteen i Stortinget bestemt at «Nasjonal sikkerhetsmyndighet (NSM) gir retningslinjer for hvilken krypteringsgrad som er nødvendig for å ivareta sikkerheten».

NSM anser at informasjon underlagt datalagringsdirektivet er sensitiv, men ugradert, og har behov for beskyttelse.

2 Drøfting

NSM har publisert et kravdokument til kryptomekanismer for beskyttelse av både gradert og ugradert informasjon. Dette dokumentet, *NSM Cryptographic Requirements*, inneholder et kravnivå, *Moderate*, som NSM anser tilfredsstillende for å beskytte sensitiv, men ugradert informasjon. NSM anbefaler å legge dette nivået til grunn for beskytelse av informasjon fra datalagringsdirektivet.

Dette er det samme nivået som Difis *Forprosjektrapport om standardisering av krypto i offentlig sektor* anbefaler. Dette arbeidet er for tiden under høring, men dersom forprosjektrapporten og NSMs anbefaling tas til følge, vil dette nivået bli brukt på tvers av offentlig sektor for å beskytte sensitiv, men ugradert informasjon.

Moderate stiller krav til bruk av åpne standard kryptoalgoritmer, evalueringsnivået av disse algoritmene og sertifisering systemene. For konfidensialitetsbeskyttelse av informasjon, er *Advanced Encryption Standard* (AES) med 128 bits nøkkel minstekrav. Evaluering av kryptomekanismene baserer seg på den amerikanske *FIPS 140-2* standarden på nivå 2, og for sertifisering benyttes *Common Criteria* på nivå 3.

Kravnivået tillater bruk av rene softwarebaserte kryptomekanismer, men for store datamengder og mange tilkoblinger vil sannsynligvis hardwarebaserte løsninger være å foretrekke.

Postadresse
Postboks 14
1306 BÆRUM
POSTTERMINAL

Sivil telefon/telefaks
+47 67 86 40 00/+47 67 86 40 09
E-postadresse
post@nsm.stat.no

Militær telefon/telefaks
515 40 00/515 40 09

Internetadresse (URL)
www.nsm.stat.no

Vedlegg
0

NSM Cryptographic Requirements er tilgjengelig fra NSMs hjemmesider, under Regelverk/Veiledninger. Kravnivået *Moderate* er definert i kapittel 8 med krav til algoritmer og nøkkellengder i kapittel 7.1.11.

3 Konklusjon

Med bakgrunn i diskusjonen ovenfor anbefaler NSM at kravnivået *Moderate* fra *NSM Cryptographic Requirements* benyttes for beskyttelse av informasjon fra datalagringsdirektivet over landegrensene.

Om det er ønskelig med ytterligere detaljer, stiller NSM gjerne opp for råd og veiledning.

Leiv J. H. Skaug
Kommandørkaptein
Fungerende avdelingsdirektør KSA

Nasjonal sikkerhetsmyndighet

Vår saksbehandler
Britt Jøsok
+47 67864121, 0515-4121
britt.josok@nsm.stat.no

Vår dato
2012-01-17

Tidligere dato

Vår referanse
2010/00084-006/NSM/008

Tidligere referanse

Til
Datatilsynet

Internt

Kopi til
Justisdepartementet
Forsvarsdepartementet
Intern kopi

Høring - Utkast til konsesjon til behandling av personopplysninger – (Datalagringsdirektivet)

Nasjonal sikkerhetsmyndighet (NSM) viser til høringsbrev fra Datatilsynet av 22.12.11 der det bes om kommentarer til utkast til konsesjon for behandling av personopplysninger i forbindelse med implementering av EUs datalagringsdirektiv (DLD).

I forbindelse med Stortingets vedtak om gjennomføring av EUs datalagringsdirektiv fastslås det i Transport- og kommunikasjonskomiteens innstilling (Innst. 275L (2010-2011)) på side 9, at;
Enhver forsendelse av lagringspliktige data over landegrensene skal sikres ved at krypteringsteknologi anvendes. Nasjonal Sikkerhetsmyndighet (NSM) gir retningslinjer for hvilken krypteringsgrad som er nødvendig for å ivareta sikkerheten.

Justisdepartementet ba NSM om å utarbeide forslag til slike retningslinjer i et brev datert 06.06.11. NSM besvarte henvendelsen den 07.09.11. I brevet fremkommer det hvilke krav NSM mener det er rimelig å stille til beskyttelse av ugradert men sensitiv informasjon. Kryptokravene samsvarer også med kravene som DIFI anbefaler i sitt "Forprosjekt om standardisering av krypto i offentlig forvaltning". Kopi av begge brevene følger vedlagt til orientering.[A] NSMs kommentarer til konsesjonsvilkårene knytter seg utelukkende til Datatilsynets "krav om tilfredsstillende kryptering" og må sees i lys av vårt brev av 07.09.11.

NSM kjenner ikke i detalj standarden ETSI 102 661 som Datatilsynet har valgt å basere seg på. NSM har heller ikke hatt anledning til å gjennomføre grundige analyser av ETSI 102 661 innenfor den tidsrammen høringsfristen tillot. Våre kommentarer blir derfor av overordnet karakter.

NSM anser at all bruk av krypto må basere seg på tre søyler; 1)funksjonalitet, 2) tillit og 3) nøkkelhåndtering.

1 Funksjonalitet

Med funksjonalitet mener NSM hvilken sikkerhetsfunksjonalitet som er ønsket. Dette kan være autentisering, autentisitet, integritet og konfidensialitet. Valg av sikkerhetsfunksjonalitet som ønskes er styrende i forhold til hvilken algoritme som skal benyttes. I forhold til de

algoritmer og nøkkellengder som er nevnt i ETSI 102 661 anneks C og D, mener NSM at kun følgende bør benyttes:
Konfidensialitet: AES-128
Integritet: RSA 2048, EC-DSA 224
Nøkkelutveksling: Diffie-Hellman 2048, EC-DH224
Avtrykksalgoritme: SHA-224

I forhold til anneks D betyr dette at SHA-1 som avtrykksalgoritme og 3TDEA som symmetrisk algoritme bør fjernes fra annex D.4.5.

2 Tillit

Med tillit mener NSM hvilken styrke implementeringen har.
For å sikre at kryptomekanismene er korrekt, robust og sikkert implementert, mener NSM at det vil være naturlig å kreve at disse er sertifisert. Anneks D sier følgende: *The recommendations given in this annex assume that the algorithm is properly implemented, used, and managed and run in a secure environment not subject to side-channel attacks.* Etter NSMs oppfatning kan man bare forutsette dette dersom implementeringen er evaluert og sertifisert.

3 Nøkkelhåndtering

Med nøkkelhåndtering mener NSM regimet knyttet til hvordan nøkler genereres, lagres, benyttes og slettes. Den foreslåtte løsningen vil trolig ha et stort antall nøkler som må håndteres på en sikker måte for å opprettholde sikkerheten i løsningen. NSM anser at Hardware Security Module (HSM) må benyttes for sikkert å generere et stort antall nøkler, beskytte dem, bruke dem og slette dem når de ikke lenger behøves. HSM bør også benyttes for å sikre kopier av nøkler for katastrofegjenoppretting.

Vi viser for øvrig til vedlagte korrespondanse med Justisdepartementet som uttrykk for vårt syn.

Med hilsen

Kjetil Nilsen
Direktør

Britt Jøsok
Seniorrådgiver

[A] Vedlegg: Kopi av korrespondanse mellom Justisdepartementet og NSM datert 060611 og 070911

15 JUN 2011

DET KONGELIGE
JUSTIS- OG POLITIDEPARTEMENT

Nasjonal sikkerhetsmyndighe
23 JUN 2011
Saks-nr.: 20110950 -1/430

Nasjonal sikkerhetsmyndighet
Postboks 14
1316 Bærum Postterminal

Deres ref.	Vår ref.	Dato
	201103076-RBA/UPE	6.6.2011

Oppfølgning av Stortingets vedtak om gjennomføring av EUs datalagringsdirektiv i norsk rett - retningslinjer om kryptering.

Vi viser til Stortingets vedtak om gjennomføring av EUs datalagringsdirektiv i norsk rett. Som en del av dette vil være nødvendig å utarbeide retningslinjer for kryptering. Lov 15. april 2011 nr. 11 om endringer i ekomloven og straffeprosessloven mv.(gjennomføring av EUs datalagringsdirektiv i norsk rett) trer i kraft samtidig med politiregisterloven, og senest 1. april 2012.

Før loven kan tre i kraft er det visse tiltak som må på plass, jf. Prop. 49 L (2010-2011) og Transport- og kommunikasjonskomiteens innstilling (Innst. 275 L (2010-2011)).

Av komitéinnstillingen side 9 fremgår følgende:
"Enhver forsendelse av lagringspliktige data over landegrensene skal sikres ved at krypteringsteknologi anvendes. Nasjonal sikkerhetsmyndighet (NSM) gir retningslinjer for hvilken krypteringsgrad som er nødvendig for å ivareta sikkerheten."

På bakgrunn av dette ber Justisdepartementet Nasjonal sikkerhetsmyndighet (NSM) om å utarbeide forslag til retningslinjer for bruk av kryptering ved forsendelse av lagringsdata over landegrensene.

Vi ber om at forslag til retningslinjer er oss i hende innen. 15 september 2011.

Med hilsen

Mette Stangerhaugen e.f.
ekspedisjonssjef

Knut Anders Moi
avdelingsdirektør

Postadresse	Kontoradresse	Telefon - sentralbord	Rednings- og beredskapsavdelingen	Saksbehandler
Postboks 8005 Dep	Akersg. 42	22 24 90 90	Telefaks	Knut Anders Moi
0030 Oslo		Org. nr.: 972 417 831	22 24 51 64	22248466

Kopi:
Forsvarsdepartementet