Myndigheten för samhällsskydd och beredskap

Datum	Diarienr	Utgåva
2019-01-21		0.94

Avdelningen för cybersäkerhet och skydd
av samhällsviktig verksamhet

Vägledning för grundläggande kryptering

Innehåll

1 Inledning

Myndigheten för samhällsskydd och beredskap, MSB, är en statlig myndighet med uppgift att utveckla samhällets förmåga att förebygga och hantera olyckor och kriser.

Samhället måste ha en förmåga till säker hantering och överföring av information i elektroniska kommunikationsnät och it-system. Sverige måste också ha en förmåga att upprätthålla säkerhet och integritet i samhällsviktig it-infrastruktur. Denna förmåga står och faller med vår förmåga att försäkra oss om att kryptolösningar är väl valda för sina ändamål, att de är korrekt implementerade och att de används på rätt sätt.

I det förebyggande arbetet samordnar MSB hela samhällets arbete med informationssäkerhet. Detta sker bland annat genom att främja ett systematiskt och riskbaserat arbete med informationssäkerhet för organisationer, kommuner, myndigheter, företag och enskilda. Läs mer på MSB:s hemsida:
https://www.msb.se/sv/Forebyggande/Informationssakerhet/

1.1 Tillämpningsområde och avgränsning

Denna vägledning är en sammanställning av rekommendationer för att säkerställa ett tillräckligt skydd av information genom kryptering från CSEC[1], SOG-IS[2], ENISA[3] och NIST[4] i den ordningen. För fördjupning och ytterligare information och rekommendationer uppmanas läsaren att ta del av källdokumenten.

Vägledningen beskriver säkerhetsåtgärder för att införa och upprätthålla säkra kryptolösningar[5]. Rekommendationerna i vägledningen är inte tvingande.

Säkerhetsåtgärderna i denna vägledning är avsedda för information som behöver skyddas med kryptolösning till exempel för information som omfattas av sekretess[6], men som *inte* bedöms vara säkerhetsskyddsklassificerade uppgifter[7]. Krav på säkerhetsåtgärder för säkerhetsskyddsklassificerade

[1] CSEC - Sveriges Certifieringsorgan för IT-Säkerhet, https://fmv.se/csec
[2] SOG-IS - Senior Officials Group – Information Systems Security, https://www.sogis.org/
[3] ENISA - European Union Agency for Network and Information Security, https://www.enisa.europa.eu/
[4] NIST - National Institute of Standards and Technology, https://csrc.nist.gov/
[5] Med kryptolösningar avses sådana metoder och principer för skydd av information mot insyn vid överföring och lagring med hjälp av kryptering, identifiering och autentisering samt signering och verifiering av information.
[6] Enligt OSL 2009:400
[7] Även kallade hemliga uppgifter, dvs. uppgifter som omfattas av sekretess och som rör rikets säkerhet.

uppgifter återfinns hos Säkerhetspolisen respektive Försvarsmakten.

Ytterligare information om kringliggande säkerhetsåtgärder för kryptolösningar, såsom skyddet mot fysisk tillgång till utrustningen, skyddet av distributionskedjan, skydd mot bristande kontroll av åtkomsträttigheter eller skydd mot brister i processer för kodgranskning eller i hårdvara återfinns i t.ex.

- Vägledning för fysisk informationssäkerhet i it-utrymmen (MSB629 - december 2013)
- Upphandla informationssäkert - en vägledning (MSB1177 - november 2018)
- Metodstöd för systematiskt informationssäkerhetsarbete (www.informationssakerhet.se)

Uppdatering av de rekommendationer som hänvisas till i detta dokument sker kontinuerligt utifrån MSB:s rutiner för omvärldsbevakning. Eventuella synpunkter på innehållet i vägledningen kan skickas till metodstodet@informationssakerhet.se.

För att snabbt få tillgång till information om allvarliga säkerhetsbrister eller sårbarheter erbjuder MSB/CERT-SE olika tjänster för utskick. För att ta del av sådana utskick kan organisationer anmäla sig med e-postadress på https://www.cert.se/

1.2 Syfte och målgrupp

Syftet med denna vägledning är att ge organisationer stöd vid framtagning av riktlinjer och instruktioner för kryptolösningar. Vägledningen riktar sig till de som ansvarar för informations- och it-säkerhet inom olika typer av organisationer.

Beskrivna säkerhetsåtgärder i detta dokument syftar till att reducera risker i hur kryptolösningar konfigureras och implementeras. Utifrån det systematiska och riskbaserade informations- och it-säkerhetsarbetet ska riskägaren alltid väga säkerhetsåtgärdernas skydd mot identifierat behov av skydd.

1.3 Disposition

Kapitel 1 presenterar vägledningens tillämpningsområde, syfte och målgrupp.

Kapitel 2 introducerar ämnesområdet informations- och it-säkerhet.

Kapitel 3 är en kort introduktion till kryptering och begreppen som används.

Kapitel 4 – 12 beskriver rekommendationer för säker användning av kryptolösningar. Kapitlen är disponerande enligt:

- Mål – beskriver det resultat organisationen uppnår genom att genomföra kapitlets säkerhetsåtgärder.
- Bakgrund – Beskrivning av säkerhetsåtgärder, deras omfattning, tillämpningsområden, syfte och eventuella undantag.

- Rekommendationer med olika säkerhetsåtgärder där varje delåtgärd innehåller:
    - Resonemang – Förklaring till varför (del)åtgärden och rekommendationen föreslås.
    - Ett eller flera rekommendationer – Rekommendationerna beskriver vad organisationen ska göra för att uppnå en delåtgärd.

Kapitel 14 beskriver rekommendationer på DNSSEC.

Bilaga A innehåller en referenslista på standarder och andra tekniska dokument som åtgärderna är baserade på.

2 Kort om informations- och it-säkerhet

I dagens digitaliserade samhälle ställs allt högre krav på att hantera information säkert. Informationssäkerhet innebär att hantera information så att:

- endast behöriga personer får ta del av den (konfidentialitet)
- den alltid går att lita på, att den är korrekt och inte är manipulerad eller förstörd (riktighet)
- den alltid finns åtkomlig och användbar när den behövs (tillgänglighet)

För att uppnå informationssäkerhet - det vill säga bevara informationens konfidentialitet, riktighet och tillgänglighet - behöver man införa olika säkerhetsåtgärder. Säkerhetsåtgärder kan vara av administrativ, teknisk eller fysisk karaktär; normalt är det en kombination av dessa karaktärer.

Hur informationssäkerhetsarbetet kan bedrivas på ett systematiskt och riskbaserat sätt beskrivs t.ex. i SS-EN ISO/IEC-27001. Standarden presenterar de krav som ställs på organisationer så att de enligt praxis kan styra och leda sitt informationssäkerhetsarbete. MSB har tagit fram ett stöd för organisationer att bedriva ett systematiska och riskbaserade informationssäkerhetsarbetet utifrån ovan nämnda standard. Detta återfinns på https://www.informationssakerhet.se/metodstod-for-lis.

2.1 It-säkerhet

It-relaterade tekniska säkerhetsåtgärder för att upprätthålla informations-säkerhet kallas it-säkerhetsåtgärder. It-säkerhetsåtgärder är beroende av informationssäkerhetsåtgärder av t.ex. administrativ karaktär.

En viktig säkerhetsåtgärd för att skydda information vid överföring och lagring är kryptering. Den skyddsnivå som kryptering som teknik ger är dock beroende av de krav som finns, inte enbart teknisk synvinkel. Krav på hur kryptonycklar hanteras, åtkomst till kryptolösningar och val av kryptolösningar är mycket viktiga i sammanhanget.

Kryptering är således inte enbart en it-säkerhetsåtgärd, utan mycket beroende av andra säkerhetsåtgärder som vidtas i samband med hanteringen av kryptolösningen.

2.2 Efterlevnad av rekommendationerna

Under vissa omständigheter är full efterlevnad av denna vägledning inte möjlig. Exempelvis kan äldre system (eng. *legacy*) sakna möjlighet att uppfylla rekommendationerna. Vid sådana situationer ska en riskanalys visa vad som behöver åtgärdas och en åtgärdsplan för att hantera identifierade risker upprättas.

3 Grundläggande om kryptering

Kryptering är en viktig säkerhetsåtgärd för att skydda information när den lagras eller överförs[8]. Information, data, som krypteras är oläslig för alla som inte har tillgång till korrekt nyckel för att dekryptera informationen eller datat. Korrekt hantering av krypteringslösningar är viktigt för såväl den enskilda organisationen som för hela samhället.

3.1 Kryptolösningar

En kryptolösning ger en skyddsnivå som beror på hur den installeras och konfigureras. Följande faktorer behöver beaktas:

- den kryptografiska algoritmen är tillräckligt stark
- det kryptografiska protokoll som tillämpar algoritmen är tillräckligt säkert
- kryptonyckeln är tillräckligt lång och skapas på ett säkert sätt
- kryptonyckeln hanteras säkert över sin livscykel

Krypteringsalgoritmen omvandlar klartexten till oläslig kryptotext med hjälp av en kryptonyckel. Det ska inte vara möjligt att återskapa klartexten utan tillgång till nyckeln, även med kännedom om hur algoritmen fungerar[9]. De flesta algoritmer är idag publikt tillgängliga, vilket bidrar till att de löpande utsätts för granskningar. Brister som upptäckas i granskningar kan då publiceras med förslag på hur användningen av algoritmen kan ändras.

Kapitel 5 innehåller beskrivningar och åtgärder för kryptografiska algoritmer.

Kryptografiska protokoll använder kryptoalgoritmer och kryptonycklar samt utför själva krypteringen. Protokollen skiljer sig från varandra beroende på hur de använder kryptoalgoritmer och nycklar. Medan kryptoalgoritmer ofta är konstanta så kan kryptografiska protokoll förändras över tiden. Sårbarheter i protokollen hanteras genom att en ny version av protokollet släpps där protokollet förbättrats, eller att buggar i implementationen rättas.

Kapitel 6 - 11 innehåller säkerhetsåtgärder för att implementera och konfigurera kryptografiska protokoll på ett säkert sätt.

---

[8] I strikt mening är det skillnad mellan data och information. Data blir information när innebörden i den blivit tolkad. Många gånger behöver man inte hålla isär begreppen data och information. Men vid exempelvis överföring mellan datorer eller lagring i datorminnen är det data, inte information, som hanteras. (Källa: Svenska datatermgruppen)

[9] Kerckhoffs's princip från 1883 (något omskriven): Ett kryptosystem ska vara säkert även om allt i systemet är allmän kunskap, förutom nyckeln. (*Journal des sciences militaires*, vol. IX, pp. 5–38, Jan. 1883, pp. 161–191, Feb. 1883.)

Kryptonyckeln är den del i kryptolösningen som behöver hållas hemlig och som tillsammans med krypteringsalgoritmer avgör hur klartext omvandlas till kryptotext, eller vice versa. Det finns olika typer av kryptonycklar beroende på vilken typ av kryptering som används. Vid symmetrisk kryptering används en hemlig nyckel som görs i kopior och delas ut så bara de behöriga parterna har tillgång till den. Vid asymmetrisk kryptering använd ett nyckelpar, bestående av en privat och en publik nyckel. Den publika nyckeln är tillgänglig för alla, medan den privata endast ska vara känd av nyckelns ägare.

Kapitel 5 innehåller beskrivningar och säkerhetsåtgärder för kryptonycklarnas längd. Kapitel 12 och 13 innehåller beskrivningar och säkerhetsåtgärder för hur kryptonycklarna ska hanteras på ett säkert sätt.

3.2 Kommersiella kryptolösningar

Vanligtvis använder sig organisationer av kryptolösningar som är implementerade i it-system från vanliga kommersiella leverantörer. Detta gör att sammanlagda skyddsnivån i en kryptolösning är ytterst svår att verifiera som slutanvändare. Vissa kommersiella krypteringslösningar kan dock vara helt, eller delvis, kontrollerade av certifieringsorgan eller annan pålitlig tredjepartsaktör.

3.3 Om kryptering och signalskyddssystem

I säkerhetsskyddsförordningen (1996:633)[10] anges att ”Hemliga uppgifter får krypteras endast med kryptosystem som har godkänts av Försvarsmakten.”

Dessa av Försvarsmakten godkända kryptosystem kallas *signalskyddssystem*. Ett signalskyddssystem består av signalskyddsmateriel, signalskyddsnycklar och/eller aktiva kort samt en instruktion för hur systemet ska hanteras. Statliga myndigheter, landsting, länsstyrelser, kommuner, företag och organisationer som har behov av att på ett säkert och tillförlitligt sätt kunna samverka genom att kommunicera information som behöver skyddas utifrån säkerhetsskydds-lagstiftningen kan efter ansökan bli tilldelade signalskyddssystem.

[10] Motsvarande skrivning finns även i nya säkerhetsskyddsförordningen (2018:658).

4 Användning av kryptolösningar

4.1 Mål

Det önskade resultatet vid användning av kryptolösningar är att skydda data vid överföring eller vid lagring.

4.2 Bakgrund

4.2.1 Omfattning

Detta kapitel beskriver på vilket sätt kryptolösningar ska användas för att skydda data vid lagring och vid överföring.

4.2.2 Syfte

Kryptering kan exempelvis användas som en it-säkerhetsåtgärd för att skydda information utifrån:

- **Konfidentialitet:** kryptolösning för att skydda data mot obehörig åtkomst vid lagring eller överföring.
- **Riktighet:** kryptolösning genom att använda digitala signaturer eller autentiseringskoder för att verifiera att data inte obehörigt har förändrats. Detta kan i sin tur användas för att påvisa
    - *Oavvislighet*: kryptolösning för att bevisa att en handling eller händelse har ägt rum eller visa på att den inte har ägt rum.
    - *Autentisering:* kryptolösning för att verifiera användare eller it-system som begär tillgång till resurser, information eller it-system är rätt användare eller för att verifiera att mottagare och avsändare av information är den avsändare eller det it-system som det utger sig för att vara.

Ofta används en kryptolösning för att uppnå mer än ett av dessa mål.

Inom en organisation är det mycket vanligt att flera olika kryptolösningar används för att kunna skydda data vid överföring och lagring.

4.3 Generella säkerhetsåtgärder

4.3.1	Kryptering vid överföring av data
Resonemang	Vid överföring av data utsätts denna för risk att avlyssnas av obehöriga (konfidentialitet) eller för att manipuleras (riktighet). Detta kan motverkas genom att använda kryptering som en säkerhetsåtgärd. Det är sällan en organisation har sådan kontroll över

	sin nätverksinfrastruktur att den kan kallas ”säker”, således ska nätverksförbindelser vanligtvis anses vara ”osäkra”. För att avgöra behovet av kryptering av data behöves en informationsflödesmodell. Denna kan visa vilken datakommunikation som pågår mellan systemkomponenter, mellan system, mellan verksamhetsområden och mellan organisationer.
Rekommendation id	**Rekommendation**
4.3.1.1	Den kryptolösning som används för att skydda data som överförs via nätverk ska använda en rekommenderad kryptografisk algoritm (se kapitel 5) och ett rekommenderat kryptografiskt protokoll (se kapitel 6-11).
4.3.1.2	Behovet av krypterad kommunikation ska beakta alla typer av datakommunikation.
4.3.2	**Kryptering av data som lagras**
Resonemang	Genom kryptering av lagringsmedium kan lägre krav ställas på fysiska säkerhetsåtgärder för att skydda informationen t vid transport, lagring och hantering av den krypterade informationen,
Rekommendation id	**Rekommendation**

4.3.2.1	Den kryptering som används för att skydda data som lagras ska tillämpa en kryptografisk algoritm som är uppräknad i kapitel 5.
4.3.2.2	När kryptering används för att skydda data som lagras så det ske genom: • fullständig kryptering av lagringsmediet (eng. *full disk encryption*) eller • delvis kryptering av lagringsmediet där skyddet kompletteras med säker behörighets- och åtkomstkontroll. Det ska även finnas funktioner som säkerställer att data som kräver kryptering endast skrivs till den skyddade partitionen
4.3.3	**Val av kryptolösningar**
Resonemang	Det är omöjligt för en leverantör att garantera att en produkt är helt säker, vilket också gäller kryptolösningar. Detta kan bero på fel design, buggar eller hårdvarufel. En oberoende granskning kan till viss del fastställa att produkten eller it-systemet uppnår de ställda säkerhetskraven och att kända sårbarheter upptäcks. Med vilken säkerhet en produkt eller it-system är säker fastställs av den nivå av tillit som ges för att ett systems eller en produkts säkerhetsfunktioner uppfyller de specificerade kraven (assuransnivå). Efter riskanalys och att ha analyserat informationens behov av skydd bestämmer organisationen hur säker en kryptolösning behöver vara.
Rekommendation id	**Rekommendation**

4.3.3.1	Regler för användning av kryptografiska säkerhetsåtgärder för skydd av information ska utvecklas och införas i organisationen.
4.3.3.2	Produkter som tillhandahåller kryptografisk funktionalitet bör ha genomgått en oberoende granskning/evaluering mot en fastställd assuransnivå. Produktens assuransnivå ska minst motsvara organisationens identifierade behov.
4.3.4	**Inventering**
Resonemang	Kryptolösningar är en viktig del i arbetet med att säkra information. För att ha en överblick av den utrustning som ingår i dessa lösningar behöver dessa föras upp och dokumenteras i inventarie-förteckningar. På så sätt kan organisationen få vetskap om vilka versioner som användas av en viss utrustning och på enklare sätt avgöra behovet av uppgradering och/eller utbyte. Vid händelse att det framkommer och publiceras sårbarheter i vissa versioner av mjukvara eller utrustning är det viktigt att snabbt kunna identifiera om, och i så fall var, sådan används i organisationen.
Rekommendation id	**Rekommendation**
4.3.4.1	Det ska vara möjligt att redogöra för alla komponenter i en kryptolösning. Detta innebär både hårdvara och mjukvara.
4.3.5	**Revision**
Resonemang	Revision av kryptolösningar utgör ett tillfälle för att kontrollera om lösningarna uppnår förväntade krav i författningar samt externa och interna krav. Det ger också underlag till punkter där förbättringar kan ske och uppslag till om regelverk ska ses över, uppdateras och beslutas.
Rekommendation id	**Rekommendation**

4.3.5.1	Revision av kryptolösningen ska ske vid: • överlämning/förändring av administrativa ansvarsområden för kryptolösningen • utbyte av personal med tillgång till kryptolösningen • minst en gång per år
4.3.5.2	En revision ska utföras med ändamålet att: • inventera all kryptografisk utrustning och alla nycklar • bekräfta att de säkerhetsåtgärder som beskrivs i regelverket för användning av kryptografiska säkerhetsåtgärder och nyckelhanteringsplanen efterlevs
4.3.6	**Dokumentation**
Resonemang	För att underlätta administration av kryptolösningen ska själva lösningen samt de kringliggande processerna dokumenteras. Detta bidrar också till att det blir enklare att kontrollera kryptolösningen.
Rekommendation id	**Rekommendation**

4.3.6.1	För varje kryptolösning ska följande dokumenteras:
	• vem som har administrationsrättigheter
	• vem vars administrationsrättigheter har återkallats
	• beskrivning av kryptolösningen
	  • vilken information kryptolösningen ska skydda.
	  • vilka tekniska komponenter som ingår i kryptolösningen
	  • vilka val gällande algoritmer och protokoll som gjorts samt övriga konfigurationer inklusive vilka val som är aktiverade respektive inaktiverade.
	• dokument relaterade till kryptolösningen, exempelvis riktlinjer för användare och/eller produktmanualer.
	• identifierade sårbarheter, riskbedömningar och åtgärdsplan.
	• alla genomförda granskningar, inventeringar och revisioner relaterade till kryptolösningen.

	Dokumentationen ska hållas uppdaterad och tillgänglig.
4.3.7	**Administratörsrättigheter**
Resonemang	En administratörsroll i en kryptolösning medför ofta åtkomst till informationen som lösningen skyddar i okrypterat format genom att administratören har åtkomt till krypteringsnycklarna. All åtkomst till kryptolösningar ska analyseras och dokumenteras.
Rekommendation id	**Rekommendation**

4.3.7.1	Innan personal får administratörsrättigheter till kryptolösningar ska det säkerställas att personalen har: • ett faktiskt behov av åtkomst • tagit del av och förstått de relevanta reglerna för kryptolösningen
4.3.8	**Fysisk säkerhet och åtkomst**
Resonemang	Kryptolösningar där kryptonyckel är aktiverad kan medföra att någon som bereder sig åtkomst till it-utrustningen kan få tillgång till okrypterad information. Kryptolösningar med aktiverad kryptonyckel ska skyddas från • obehörig användning på samma sätt som okrypterade data • att den aktiverade nyckeln kan extraheras, kopieras eller på annat sätt spridas till obehöriga Kryptolösningar används ofta för att skydda värdefull information och kryptolösningen i sig kan vara dyr samt det arbete som misstanke om obehörig åtkomst kräver av organisationen är kostsam. .
Rekommendation id	**Rekommendation**

4.3.8.1	Den kryptografiska utrustningen med aktiverad nyckel ska förvaras i ett utrymme vars säkerhet uppnår det skydd som nyckeln kräver. Nyckeln kräver alltid ett skydd som är minst motsvarar det skydd som den okrypterade informationen behöver eller värdet av att kunna säkerställa ursprung genom signering. Gäller nycklar för krypterar/dekrypterar ochsignering.
4.3.8.2	Utrustning som installerats och konfigurerats med en kryptonyckel (eng. *in a keyed state*) måste vid distribution, hantering och transport ges ett skydd som är minst motsvarar det skydd som den okrypterade informationen behöver eller värdet av att kunna säkerställa ursprung genom signering.
4.3.8.3	Utrustning utan inlästa (aktiverade) kryptonycklar ska hanteras och transporteras på ett sådant sätt att stöld, manipulation eller skada på utrustningen kan undvikas.
4.3.9	**Signalskydd (eng. high grade cryptographic products)**
Resonemang	Om hemliga uppgifter (säkerhetsskydds-klassificerade uppgifter) ska kommuniceras till ett informationssystem utanför verksamhetsutövarens kontroll ska uppgifterna skyddas med hjälp av kryptografiska funktioner som har godkänts av Försvarsmakten (signalskydd).
Rekommendation id	**Rekommendation**
4.3.9.1	Information som bedöms som hemlig uppgift (säkerhetsskyddsklassificerad uppgift) får endast kommuniceras om de skyddas med hjälp av kryptografiska funktioner som har godkänts av Försvarsmakten (signalskydd).

5 Rekommenderade kryptografiska algoritmer

5.1 Mål

Vid kryptering av data ska rekommenderad kryptografisk algoritm med rätt nyckellängd användas.

5.2 Bakgrund

5.2.1 Omfattning

Detta kapitel beskriver kryptografiska algoritmer som rekommenderas vid oberoende granskningar enligt Common Criteria (CC) av produkter som implementerar kryptografisk funktionalitet. CSEC:s regelverk finns beskrivet i form av ”Scheme Publications”, vara kryptografiska algoritmer behandlas i ”*CSEC:s kryptopolicy”* (SP-188).

CSEC:s lista av godkända kryptografiska algoritmer (SP-188) bygger i grunden på SOG-IS dokumentet ”*Agreed Cryptographic Mechanisms”*. Då SP-188 inte redogör för godkända elliptiska kurvor, modulusvärden eller Galois/Counter Mode har dessa hämtats ur SOG-IS dokument.

5.2.2 Syfte

En rekommenderad algoritm omvandlar data på ett sätt som gör det omöjligt att inom en rimlig tid och kostnad med hjälp av modern datorkraft fastställa ursprunglig klartext utan tillgång till nyckeln.

För att minimera risken att krypterad data kan dekrypteras bör vikt läggas vid valet av algoritm. Utvecklingen av modern datorkraft tillsammans med forskning inom kryptoanalys bidrar till att algoritmer ibland inte längre kan garantera tillräckligt skydd. Valet av algoritm ska göras med säkerhetsmarginaler för framtida attacker i åtanke, beroende på hur länge den krypterade informationen måste skyddas.

Det finns ingen garanti för att algoritmer är säkra mot okända attacker. Algoritmerna som rekommenderas i detta kapitel har varit föremål för omfattande granskningar av industrin, myndigheter och inom den akademiska världen. Både teoretiskt och i praktiken har dessa algoritmer visat sig starka.

Val av längd (storlek) på nyckel är också av stor vikt och ska anpassas till val av algoritm och den tid som informationen förväntas vara i behov av skydd.

Just nu pågår utvecklingen av kvantdatorer som, till skillnad från konventionella datorer, sägs kunna lösa matematiska problem som dagens algoritmer bygger på snabbare. När kvantdatorer har tillräcklig förmåga kommer en del algoritmer inte längre att kunna erbjuda tillräckligt skydd. Det pågår arbeten med att ta fram, testa och standardisera algoritmer som kvantdatorer inte ska kunna forcera. Bland annat arbetar NIST med projektet

”*Post-Quantum Cryptography Standardization”.*

De rekommenderade kryptografiska algoritmerna kan delas in i fyra kategorier: asymmetriska algoritmer, symmetriska algoritmer, digitala signaturer och hashfunktioner. Algoritmer och nyckellängder anges i tabellen nedan. Tabellen presenterar även rekommenderade elliptiska kurvor.

5.3 Rekommenderade algoritmer och nyckellängder

Kommentar: Med engelskans “legacy” menas inställningar för äldre (föråldrade) it-system och programvaror. När en organisation ska anskaffa nya produkter med kryptolösningar ska man säkerställa att algoritmerna i tabellen som insorteras under benämningen legacy inte ska användas. Dessa får endast användas för befintliga system som inte stödjer rekommenderade algoritmer eller nyckellängder och ska fasas ut så fort som möjligt och hitta sätt att förhålla sig till bristerna tillsvidare.

Beskrivning	Kryptografisk algoritm och nyckellängd	Referens
Asymmetrisk kryptering Kryptering där olika nycklar används för kryptering och dekryptering. Därmed ska en nyckel vara hemlig och den publika nyckeln kan publiceras.	• RSA #1 v2.2 Nyckellängd 3072 (eller fler) bitar • **Legacy:** RSA #1 v1.5 Nyckellängd 2048 (eller fler) bitar	SP-188 A.5
	• RSA-OAEP #1 v2.2 Mask generation function MGF1, baserad på SHA-224, SHA-256, SHA-384 eller SHA-512 • **Legacy:** RSA #1 v1.5 Mask generation function MGF1, baserad på SHA-224, SHA-256, SHA-384 eller SHA-512	SP-188 A.6
Symmetrisk kryptering Kryptering där samma nyckel används för kryptering och dekryptering. Därmed får nyckeln enbart vara känd av behöriga parter.	• AES Nyckellängd 128, 192 eller 256 bitar • **Legacy:** 3 DES Nyckellängd 168 bitar (1x2x3)	SP-188 A.1
	Mode • CTR Counter mode • OFB Output feedback mode	SP-188 A.4

	• CBC Cipherblock chaining mode • CBC-CS Cipherblock chaining mode, chiphertext stealing • CFB Cipher feedback mode	
	Message authentication • CMAC • CBC-MAC • HMAC, nyckellängd minst 125 bitar • **Legacy:** HMAC och HMAC-SHA1 Nyckellängd minst 100 bitar	SP-188 A.7
Elliptiska kurvor De kurvor som ska användas vid Elliptic Curve Cryptography.	• BrainpoolP256r1 • BrainpoolP384r1 • BrainpoolP512r1 • NIST P-256 • NIST P-384 • NIST P-521 • FRP256v1	SOG-IS 4.3
Digitala signaturer Ett bevis på ett meddelandes riktighet och att avsändaren är verifierad.	• RSA-PSS • KCDSA • Schnorr • EC-KCDSA • EC-DSA • EC-GDSA • EC-Schnorr • **Legacy:** RSA hash PKCS#1 v1.5	SP-188 A.6
Hashfunktion En envägsfunktion som skapar ett avbildningar med fast längd av en datamängd, även kallat hashvärde. Dess funktion är att det inte ska gå att konstruera två olika indata som sedan resulterar i samma hashvärde.	• SHA-2 Hash-längd: SHA-256, SHA-384 • SHA-3 Hash-längd: 384 eller 256 bitar • **Legacy:** SHA-2 Hash-längd: SHA-224 bitar	SP-188 A.3
Nyckelutbyte	• ECDH, nyckellängd minst 385 bitar • **Legacy:** DH, modulusvärde på minst 4096 bitar	SOG-IS 5.4

5.4 Åtgärder

5.4.1	**Användning av rekommenderade algoritmer**
Resonemang	När en kryptolösning konfigureras ska samtliga icke-godkända algoritmer inaktiveras. Detta ska motverka att felaktig konfiguration av it-system som kan resultera i att en svag algoritm används. Om så skulle vara fallet skulle användaren vara omedveten om den lägre säkerhetsnivån.
Rekommendation id	**Rekommendation**
5.4.1.1	It-system som används i kryptolösningar ska stödja de rekommenderade kryptografiska algoritmerna (se kapitel 5).
5.4.1.2	It-system som används i kryptolösningar ska vara konfigurerade så att kryptografiska algoritmer som inte är rekommenderade ska vara inaktiverade.
5.4.2	**Vid bristande stöd för algoritmer och nyckellängder**
Resonemang	It-system som inte stödjer användning av rekommenderade kryptografiska protokoll, algoritmer eller nyckellängder innebär ett otillräckligt skydd En organisation ska så långt det är möjligt utgå från att använda så stark kryptering som möjligt avseende nyckellängder, algoritmer och andra typer av konfigurationer.
Rekommendation id	**Rekommendation**

5.4.2.1	Befintlig utrustning som saknar stöd för rekommenderade kryptografiska nyckellängder ska konfigureras med längsta möjliga nyckellängd.
5.4.2.2	Befintlig utrustning som saknar stöd för rekommenderade kryptografiska algoritmer och protokoll ska konfigureras med bästa konfigurerbart möjliga algoritm och protokoll.
5.4.2.3	Befintliga it-system (legacy) som saknar stöd för rekommenderade kryptografiska algoritmer och/eller nyckellängder bör bytas ut/uppgraderas snarast möjligt.
5.4.3	**Användning av RSA**
Resonemang	Genom sättet RSA är konstruerat som algoritm måste olika nycklar användas för signering och autentisering.
Rekommendation id	**Rekommendation**
5.4.3.1	Vid användning av RSA ska separata nycklar användas för digitala signaturer och kryptering.
5.4.4	**Generellt gällande godkända hashfunktioner**
Resonemang	Framsteg inom forskning i kryptografi tyder på att SHA-1 kan vara sårbar mot kollisionsattacker, det vill säga att det går att konstruera två olika indata som sedan resulterar i samma hashvärde.
Rekommendation id	**Rekommendation**

5.4.4.1	De godkända hash-funktionerna är SHA-2 och SHA-3.
5.4.5	**Metoder för symmetrisk kryptering genom blockchiffer**
Resonemang	Metoden (eng. *Mode of operation*) "Electronic Code Book" (ECB) kan resultera i att mönster i klartexten (såsom upprepningar) återfinns i det krypterade meddelandet. Detta skapar ett mönster som gör det enklare att forcera kryptot och eventuellt kunna återskapa nyckeln.
Rekommendation id	**Rekommendation**
5.4.5.1	AES ska användas med någon av metoderna CBC, CFB, OFB eller CTR.
5.4.6	**Användning av 3DES (endast befintliga system, "legacy")**
Resonemang	3DES bygger på användandet av DES i tre iterationer och kan användas med antingen två (i ordningen 1, 2, 1), eller tre olika nycklar (i ordningen 1, 2, 3). Av dessa två metoder ger alternativet med tre olika nycklar högre säkerhet. 3DES får inte användas med endast en nyckel, vilket är synonymt med DES.
Rekommendation id	**Rekommendation**
5.4.6.1	3DES (legacy) ska användas med tre (3) 1(1*2*3, 1,2,3).
5.4.7	**Användning av AES-GCM**
Resonemang	AES kan implementeras på flera sätt. "Galois/Counter Mode" (GCM) är den föredragna AES sätten tack vare dess effektivitet och prestanda. AES-GCM består av två funktioner: autentiserad kryptering och autentiserad dekryptering. Referens: SOG-IS 3.5
Rekommendation	**Rekommendation**

id	
5.4.7.1	AES implementationer ska använda metoden GCM.

6 Rekommenderade kryptografiska protokoll

6.1 Mål

Vid nätverksöverföring ska rekommenderat kryptografiskt protokoll användas, som i sin tur implementerar rekommenderade kryptografiska algoritmer.

6.2 Bakgrund

6.2.1 Omfattning

Detta kapitel är en inledning till kapitel 7 - 11 där varje kapitel presenterar ett rekommenderat kryptografiskt protokoll. Då protokollen skiljer sig från varandra har de delats upp i separata kapitel. De rekommenderade protokollen är:

Transport Layer Security (TLS) – kapitel 7
för att kryptera nätverkstrafik mellan applikationer.

Secure Shell (SSH) – kapitel 8
för att kryptera nätverkstrafik vid t.ex. fjärrstyrning och administration av it-utrustning.

Secure Multipurpose Internet Mail Extension (S/MIME) – kapitel 0
för att kryptera e-post.

OpenPGP Message Format – kapitel 10
för att kryptera e-mail och filer.

Internet Protocol Security (IPsec) – kapitel 11
för krypterade tunnlar, (eng. Virtual Private Networks)

6.2.2 Syfte

Vid krypterad kommunikation över nätverk används kryptografiska protokoll för att hantera uppkoppling, nyckelutbyte, i förekommande fall autentisering, dataöverföring och nedkoppling. Ett kryptografiskt protokoll är en implementation och tillämpning av en eller flera kryptografiska algoritmer.

Ett kryptografiskt protokoll hanterar ofta flera kryptografiska algoritmer, olika nyckellängder och en kombination av dessa. Det är viktigt att kryptografiska protokoll konfigureras att använda rekommenderade algoritmer och nyckellängder.

6.3 Åtgärder

6.3.1	**Användning av rekommenderade protokoll**
Resonemang	Otillräcklig konfiguration av, eller otillräckligt systemstöd för, kryptolösningar som använder ett rekommenderat protokoll kan leda till en mindre säker kryptering jämfört med vad som förväntas. När en kryptolösning konfigureras ska samtliga icke-godkända protokoll och algoritmer inaktiveras.
Rekommendation id	**Rekommendation**
6.3.1.1	Produkter som används i kryptolösningar ska stödja de rekommenderade kryptografiska protokoll som krävs.
6.3.1.2	Produkter som används i kryptolösningar ska vara konfigurerade att endast använda rekommenderade kryptografiska protokoll.
6.3.2	**Uppdaterad programvara**
Resonemang	Äldre versioner av programvaror som implementerar kryptolösningar kan innehålla sårbarheter. Tillverkaren ger ut nya versioner av programvaran för att åtgärda detta. Äldre system kan sakna möjligheten att kunna uppgraderas. Vid sådana situationer ska riskanalys visa vad som behöver åtgärdas och en åtgärdsplan för att hantera identifierade risker upprättas.
Rekommendation id	**Rekommendation**
6.3.2.1	Endast uppdaterade implementationer av den senaste versionen av programvaror ska användas.
6.3.2.2	Kryptolösningar som inte kan uppgraderas ska skyddas med kompenserande åtgärder. En dokumenterad åtgärdsplan ska påvisa hur identifierade risker-hanteras.

7 Protokoll: Transport Layer Security (TLS)

För att kryptera nätverkstrafik mellan applikationer

7.1 Mål

Målet med att vidta åtgärderna i detta kapitel är att användandet av TLS sker på ett säkert och korrekt sätt.

7.2 Bakgrund

7.2.1 Omfattning

Detta kapitel beskriver under vilka förutsättningar som TLS kan användas som ett kryptografiskt protokoll. Transportkryptering med TLS kan användas tillsammans med flera olika protokoll, såsom HTTP, FTP, IMAP, POP3, LDAP och SMTP. Ofta sätts ett "S" som postfix på protokollnamnet för att indikera att protokollet tunnlas genom TLS, t.ex. HTTPS.

TLS bygger på det tidigare protokollet SSL (Secure Sockel Layer), som inte längre anses säkert, det är inte heller kompatibelt med TLS. Begreppen SSL och TLS används dock ofta synonymt vilket kan orsaka förvirring.

7.2.2 Syfte

TLS är designat för att tillhandahålla säker kommunikation över internet och har många olika användningsområden på internet. Några exempel är att skydda hemsidor, e-post, instant messaging, och röst/videosamtal. TLS använder sig både av asymmetrisk och symmetrisk kryptering.

TLS är ett protokoll framtaget av Internet Engineering Taskforce (IETF). Protokollets första version publicerades i januari 1999 och har sedan dess uppdaterats av RFC 5246 (augusti 2008) och RFC 6176 (mars 2011).

TLS 1.3 är ett nyligen publicerat protokoll. (i RFC 8446, augusti 2018). TLS 1.3 har infört stora förändringar i hur de kryptografiska algoritmerna implementeras jämfört med TLS 1.2. TLS version 1.3 är inte testad tillräckligt för att rekommenderas i denna vägledning i dagsläget. MSB kommer följa hur testerna av TLS 1.3 går.

TLS möjliggör tre funktioner:

- Kryptering av informationen
- Autentisering av server
- Autentisering av klient

Klientautentisering tas inte upp i denna vägledning.

Vid konfiguration av TLS används ibland begreppet ”Cipher Suite”. Denna består av ett antal delkomponenter: *Key Exchange Algorithm*, *Encryption Algorithm* och *Message Authentication Code*. Vid handskakningen mellan klient och server väljs vilken Cipher Suite som ska användas:

1. klienten skickar en lista över vilka algoritmer och protokoll den har stöd för i prioriteringsordning
2. servern väljer en av dessa enligt den högsta i sin prioritetsordning, alternativt nekar anslutningen om ingen matchning hittas.

För att öka säkerheten begränsar man servern till att bara tillåta ett visst urval av Cipher Suites för att undvika klienter som inte har stöd för de rekommenderade algoritmerna och protokollen.

X.509-certifikat (Public Key Infrastructure, PKI) och asymmetrisk kryptering används för autentisering och utbyte av en sessionsnyckel (eng. *session key*) inom ramen för Key Exchange Algorithm. Sessionsnycklen tas fram slumpmässigt av klienten och är en symmetrisk nyckel med begränsad livslängd och används för att kryptera data mellan parterna för en specifik session. Hanteringen av PKI-nycklar (t.ex. X.509-certifikat med tillhörande privat nyckel) hanteras i kapitel 12.

Rekommenderade algoritmer och nyckellängder återfinns i kapitel 5.

Sammantaget är det sålunda dessa Cipher Suites som är de rekommenderade inom TLS 1.2:

1. TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
2. TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
3. TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384
4. TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256
5. TLS_DHE_RSA_WITH_AES_256_GCM_SHA384
6. TLS_DHE_RSA_WITH_AES_128_GCM_SHA256
7. TLS_DHE_RSA_WITH_AES_256_CBC_SHA256
8. TLS_DHE_RSA_WITH_AES_128_CBC_SHA256

7.2.3 Kommentar om Secure Socket Layer (SSL)

Den senaste versionen som släpptes av SSL var version 3.0. Ingen version av SSL ska användas.

7.3 Åtgärder

7.3.1	Användning av TLS
Resonemang	SSL är ett gammalt protokoll som inte utvecklats sedan 1999 och där många sårbarheter har upptäckts. SSL har ersatts av TLS, där de tidigare versionerna har haft identifierade sårbarheter.
Rekommendation id	**Rekommendation**
7.3.1.1	Vid användning av TLS ska version 1.2 användas. Tidigare versioner ska vara avstängda.
7.3.1.2	Inga versioner av SSL ska användas, SSL ska vara inaktiverat.

7.3.2	Användning av TLS
Resonemang	TLS är ett mycket välspritt protokoll som är implementerat i bl.a. it-system som hanterar webb, e-post, chat och IP-telefoni. Såsom all annan mjukvara kan produkter innehålla svagheter i form av buggar eller designfel. Då protokollet används i så stor utsträckning och för så många olika tillämpningar så även gränssnittet mellan applikationsprotokoll (t.ex. HTTP) och TLS-protokollet viktigt att konfigurera rätt.
Rekommendation id	**Rekommendation**

7.3.2.1	Följande inställningar ska göras för webbservrar och annan webbkommunikation: • Använd alltid senaste versionen av operativsystem, servermjukvara och ett uppdaterat TLS-bibliotek. Se till att kontinuerligt uppdatera både operativsystem och de komponenter som används av webbservern. • Inaktivera alltid cachning av HTTP-respons vilket motverkar att information lagras lokalt på klienten som kan bli tillgänglig efter utloggning. • Aktivera HTTP Strict Transport Security. Detta medför att ”mixed-content” inte tillåts på en webbsida dvs. att man ska köra hela sessionen över TLS när man använder TLS och inte blanda krypterad och okrypterad data. • Aktivera forward secrecy (PFS) så att ECDHE och DHE används vid förhandling av sessionsnycklar. • Maximal TLS-sessionslängd utan omförhandling ska konfigureras till 12 timmar. Maximal inaktiv TLS-sessionslängd ska konfigureras till 35 minuter.

7.3.2.2	Följande inställningar ska göras som skydd mot identifierade attacker mot TLS-protokollet: • Inaktivera Client-Initiated Renegotiation som ett skydd mot DoS attacker. • Inaktivera TLS-kompression vilket skyddar mot CRIME- och TIME-attacker. • Inaktivera HTTP-kompression, eller vidta säkerhetsåtgärder mot Cross-Site Request Forgery (CSRF) vilket skyddar mot BREACH-attacker. • Inaktivera DHE_EXPORT - tillåt inte svaga Cipher Suites som bl.a. innehåller 512 bits Diffie-Hellman grupper som anses vara kompromitterad vilket är skydd mot mot Logjam attacker. • Inaktivera TLS_FALLBACK_SCSV för att säkerställa att ingen omförhandling av kommunikationen till lägre protokollversioner sker, vilket är ett skydd mot POODLE-attacker.

8 Protokoll: Secure Shell (SSH)

För att kryptera nätverkstrafik vid t.ex. fjärrstyrning och administration av it-utrustning.

8.1 Mål

Målet med att vidta åtgärderna i detta kapitel är att användandet av SSH sker på ett säkert och korrekt sätt.

8.2 Bakgrund

8.2.1 Omfattning

Detta kapitel beskriver under vilka förutsättningar som kommersiella – och öppna (eng. *open source*) – implementationer av SSH kan användas som ett kryptografiskt protokoll. Åtgärderna gäller implementationer av SSH som uppfyller RFC 4250 från IETF.

8.2.2 Syfte

SSH är ett protokoll som t.ex. används för säker fjärrstyrning och administration av it-system via datornätverk.

Kapitlet är även relevant för andra protokoll vars säkerhet bygger på SSH, såsom Secure Copy (SCP) och Secure File Transfer Protocol (SFTP).

8.3 Åtgärder

8.3.1	Konfigurationsinställningar för SSH, grunder
Resonemang	SSH version 2 som utvecklas från 1996 och framåt ska användas. SSH version 1 från 1995 har kända säkerhetsbrister och ska ses som *legacy*. SSH har stöd för *SSH Tunneling* och *SSH port forwardin*g vilket tillåter SSH-applikationer att skicka en anslutning vidare till en annan SSH-applikation. Det innebär det en ökad attackyta där en attack snabbt kan spridas. En angripare som lyckas få tillgång till administratörs-rättigheter för it-system kommer inte bara ha åtkomst all information, utan även fullständig kontroll över utrustningen. På grund utav de potentiella konsekvenserna vid en den typen av angrepp ska administratörskontot inte användas för inloggning direkt mot servern.
Rekommendation id	**Rekommendation**

8.3.1.1	Vid användning av SSH ska nedan namngivna inställningsalternativ konfigureras på detta sätt: • Protocol 2: Inaktivera SSH version 1. • ListenAddress xxx.xxx.xxx.xxx: På it-system med mer än ett nätverksgränssnitt ska SSH-tjänsten konfigureras att enbart lyssna på rätt IP-adress • AllowTCPForwarning no: Inaktivera ”connection forwarding” • Gatewayports no: Inaktivera ”gateway ports” • PermitLoginRoot no: Inaktivera möjligheten att logga in som användare “root” • HostBasedAuthentication no: Inaktivera “host-based authentication” • RhostsAuthentication no: Inaktivera “rhosts-based authentication” • IgnoreRhosts no: Inaktivera “rhosts-based authentication” • PermitEmptyPasswords no: Inaktivera möjligheten att sätta tomma lösenord • Banner/directory/file: Konfigurera ett lämpligt hälsningsmeddelande för inloggningen • LoginGraceTime xx: Konfigurera tiden för inaktivering vid inloggningsförsök till maximalt 60 sekunders inaktivitet • X11forwarding no: Inaktivera “X forwarding” • HostKeyAlgorithms xx: Konfigurera rekommenderade kryptografiska algoritmer efter denna vägleds kapitel 5 Tabellen nedan visar de inställningar som ska aktiveras vid användning av SSH. Den konfiguration som presenteras ovan är baserad på OpenSSH. Vid användning av andra SSH-implementationer kan inställningarna komma att behöva anpassas.
8.3.2	**Autentisering för SSH**
Resonemang	Autentisering med kryptografiska nycklar är ofta det säkrare alternativet jämfört med inloggning med användarnamn och lösenord.
Rekommendation	**Rekommendation**

id	
8.3.2.1	Autentisering för SSH bör ske via kryptografiska nycklar (eng. *public key-based authentication*).
8.3.2.2	I det fall autentisering sker via lösenord ska tekniska åtgärder implementeras för att försvåra för potentiella angripare att kunna gissa sig till lösenord (eng. *brute-force attacks*).
8.3.2.3	I det fall autentisering sker via lösenord ska lösenorden vara starka avsett komplexitet och längd.
8.3.3	**Automatiserad fjärrstyrning**
Resonemang	Medan autentisering utan lösenord kan förenkla och automatisera fjärrstyrning och fjärradministration, finns även en risk att någon obehörig kan få tillgång till systemet. Om *SSH port forwarding* / *SSH tunneling* inte är säkert konfigurerat finns det en risk att en angripare kan komma åt tunneln, och därmed få åtkomst till ytterligare system. Om *agent credential forwarding* är aktivt finns en risk att angriparen kan komma åt lagrad autentiseringsdata och använda denna för att ansluta till ytterligare system. X11 är en programvara och nätverksprotokoll som tillhandahåller ett grafiskt användargränssnitt (GUI) via ett nätverk. Om X11 inte stängs av finns en risk att en angripare får kontroll utöver datorns skärm tillsammans med mus och tangentbord. Att tillåta ”Console access” betyder att varje användare som loggar in via *console* kan köra program som normalt sätt endast kan köras med administratörsrättigheter.
Rekommendation id	**Rekommendation**

8.3.3.1	När fjärrstyrning tillåts utan autentisering med lösenord ska funktionen “Forced Command” (även kallad ”command restriction”) användas för att specificera vilket kommando som ska kunna exekveras.
8.3.3.2	Vid användning av funktionaliteten ”Forced Command” ska alla parametrar valideras.
8.3.3.3	När autentisering tillåts utan lösenord för automatiseringsändamål ska följande funktioner inaktiveras: • Port forwarding • Agent credential forwarding • X11 display remoting • Console access Åtkomst (access) får endast ske från i förväg godkänd IP-adress.
8.3.4	**Hjälpprogrammet ”ssh-agent”**
Resonemang	Hjälpprogrammet ”ssh-agent” kan hantera och lagra privata nycklar som lagras på en dator, och verifiera nycklarna åt övriga system. När ”ssh-agent” startas kommer det att efterfråga användarens lösenord. Lösenordet låser upp användarens privata nyckel. Sedan hanteras autentisering mot övriga system av ”ssh-agent” utan att användaren behöver mata in sitt lösenord igen. När detta sker finns en risk för obehörig åtkomst till it-systemet och otillbörligt utnyttjande med den upplåsta nyckeln.
Rekommendation id	**Rekommendation**
8.3.4.1	Hjälpprogrammet ”ssh-agent” (eller liknande program där nycklar lagras upplåsa i en cache) får endast användas på it-system där följande är konfigurerat: • Skärmlås (eller motsvarande) aktiveras efter en kort inaktivitetsperiod (högst 10 minuter). • Nyckelns cache töms inom fyra timmars inaktivitet, eller kortare tid.

9 Protokoll: Secure Multipurpose Internet Mail Extension (S/MIME)

För att kryptera e-post.

9.1 Mål

Målet med att vidta åtgärderna i detta kapitel är att användandet av S/MIME för organisationens e-post sker på ett säkert och korrekt sätt.

9.2 Bakgrund

9.2.1 Omfattning

Detta kapitel beskriver under vilka förutsättningar som S/MIME kan användas som ett kryptografiskt protokoll. Åtgärderna gäller implementationer av S/MIME som uppfyller RFC 5751 från IETF.

För konfiguration av kommunikation mellan e-postservrar, se kapitel 7 (TLS).

9.2.2 Syfte

S/MIME är ett protokoll som används för säker överföring av e-post ände-till-ände (eng. *end-to-end*), det vill säga från avsändande till mottagande e-postklient.

Notera att när e-post krypteras blir det svårare att inspektera och filtrera e-post som innehåller virus eller skadlig kod.

S/MIME används ofta för att autentisera e-postavsändaren. För att säkert hantera de kryptografiska nycklar som används för autentiseringsfunktionen bör dessa nycklar lagras på personliga nyckelenheter, såsom smarta kort med nyckeln lagrad på kortet.

9.3 Åtgärder

9.3.1	Användning av S/MIME
Resonemang	S/MIME version 3.0 och senare versioner publiceras i IETF-standarden. Den bygger på tidigare versioner av protokollet som inte längre ska användas. Klientprogramvaran för e-post kan ofta konfigureras gällande val av krypterings- och hashalgoritm.
Rekommendation id	**Rekommendation**

9.3.1.1.1	Vid användning av S/MIME ska version 3.0 eller senare användas.
9.3.1.1.2	Rekommenderade algoritmer, i enlighet med KAPXX, ska konfigureras att användas av S/MIME-programvaran.

10 Protokoll: OpenPGP Message Format

För att kryptera e-mail och filer.

10.1 Mål

Målet med att vidta åtgärderna i detta kapitel är att användandet av OpenPGP Message Format sker på ett säkert och korrekt sätt.

10.2 Bakgrund

10.2.1 Omfattning

Detta kapitel beskriver under vilka förutsättningar som OpenPGP Message Format kan användas som ett kryptografiskt protokoll. Åtgärderna gäller för implementationer av OpenPGP som uppfyller RFC 4880 från IETF.

10.2.2 Syfte

OpenPGP är ett protokoll som används för säker överföring av e-post ände-till-ände.

Notera att när e-post krypteras blir det svårare att inspektera och filtrera e-mail som innehåller virus eller skadlig kod.

10.3 Åtgärder

10.3.1	**Användning av OpenPGP Message Format**
Resonemang	Vid misstanke om att privata certifikatet eller tillhörande nyckel har röjts går det inte längre att lita på meddelanden som skickats med sagda nyckel. Det går inte att säkerställa riktighet och faktisk avsändare för signerade meddelanden eller konfidentialitet för krypterade meddelanden.
Rekommendation id	**Rekommendation**

10.3.1.1	Rekommenderade algoritmer (se kapitel 5) ska användas och implementerad OpenPGP-programvara ska konfigureras därefter.

11 Protokoll: Internet Protocol Security (IPsec)

För krypterade tunnlar, (eng. Virtual Private Networks)

11.1 Mål

Målet med att vidta åtgärderna i detta kapitel är att användandet av IPsec sker på ett säkert och korrekt sätt.

11.2 Bakgrund

11.2.1 Omfattning

Detta kapitel beskriver under vilka förutsättningar som IPsec kan användas som ett kryptografiskt protokoll. Åtgärderna gäller implementationer av IPsec som uppfyller RFC 2401 och RFC 4301 från IETF.

11.2.2 Syfte

IPsec är ett protokoll som används för att skapa krypterad trafik på IP-nivån.

IPsec kan användas i två lägen: transportläge (eng. *transport mode*) eller tunnelläge (eng. *tunnel mode*). Transportläget skyddar IP-paket som skickas mellan två parter. Tunnelläget sammanlänkar två skilda nätverk, och skyddar all trafik som färdas via länken.

IPsec består av två olika protokoll: *Encapsulating Security Payload* (ESP) och *Authentication Header* (AH). ESP är det protokoll som tillhandahåller kryptering.

IPsec implementationer stödjer ett flertal kryptografiska algoritmer REF KAP? då protokollet ESP används.

IPsec-implementationer kan stödja olika metoder för utbyte av kryptografiska nycklar. Två vanliga metoder är manuell konfiguration av nycklar (eng. *pre-shared key* eller PSK) eller IKE[11] som båda använder ISAKMP[12]. Båda metoderna är rekommenderade.

ISAKMP använder två lägen för att utbyta nyckelinformation genom IKE: main mode och aggressive mode. Användning av main mode ger extra skydd i förhållande till aggressive mode och är därför rekommenderat.

[11] IKE - Internet Key Exchange Protocol Version 2 (IKEv2), RFC 7296.

[12] ISAKMP - Internet Security Association and Key Management Protocol, RFC 2408.

Forward Secrecy eller Perfect Forward Secrecy (PFS) utgör en funktionalitet där varje session mellan server och klient krypteras med egna unika nycklar. Dessa nycklar är också oberoende av nyckelmaterialet i den privata nyckel som är knuten till certifikatet på servern. Nycklarna sparas inte och används endast till just denna session och kastas sedan. Det innebär att det är mycket svårt att dekryptera alla avlyssnade och sparade sessioner även om de privata nycklarna, eller en sessionsnyckel, blir röjda.

11.3 Åtgärder

11.3.1	**Generellt om IPsec-konfiguration**
11.3.1.1	Rekommenderade algoritmer (se kapitel 5) ska användas och implementerad IPsec-programvara ska konfigureras därefter.
11.3.2	**IPsec-lägen**
Resonemang	Tunnelläget tillhandahåller kryptering för hela IP-paketet medan transportläget enbart krypterar IP-paketens innehåll.
Rekommendation id	**Rekommendation**
11.3.2.1	För IPsec-förbindelser ska tunnelläget aktiveras.
11.3.3	**IPsec protokoll**
Resonemang	För att säkra en VPN förbindelse krävs både autentisering och kryptering. Både AH och ESP tillhandahåller autentisering och integritet för innehållet i IP-paket. Det är dock endast ESP som även tillhandahåller konfidentialitet genom kryptering. Network Address Translation (NAT) innebär begränsningar för AH. ESP är det protokoll som rekommenderas. För maximal säkerhet kan ESP användas tillsammans med AH, eftersom att AH även tillhandahåller autentisering för hela IP-paketet och inte bara paketets innehåll (eng. *payload*).
Rekommendation id	**Rekommendation**

11.3.3.1	Vid användning av IPsec ska ESP protokollet aktiveras.
11.3.4	**ISAKMP-lägen**
Resonemang	Användning av *main mode* ger extra skydd i förhållande till *aggressive mode*.
Rekommendation id	**Rekommendation**
11.3.4.1	Vid användning av ISAKMP ska *aggressive mode* inaktiveras.
11.3.5	**Livslängd för Security Associations**
Resonemang	En livslängd för Security Associations (SA) på fyra timmar eller-14 400 sekunder utgör en god balans mellan säkerhet och användbarhet.
Rekommendation id	**Rekommendation**
11.3.5.1	Livslängden för SAs ska konfigureras till maximalt fyra timmar eller 14 400 sekunder.
11.3.6	**Diffie-Hellman**
Resonemang	Diffie-Hellman grupper (eng. *DH-group*) fastställer nyckelns styrka, där större grupper leder till ökad entropi vid nyckelutbytet. Exempel på grupper är: • 1: 768-bit DH **(legacy)** • 2: 1024-bit DH **(legacy)** • 5: 1536-bit DH **(legacy)** • 14: 2048-bit DH group. • 15: 3072-bit DH group. • 16: 4096-bit DH group. • 19: 256-bit elliptic curve DH (ECDH) group. • 20: 384-bit elliptic curve DH (ECDH) group. • 24: 2048-bit elliptic curve DH (ECDH) group.
Rekommendation id	**Rekommendation**

11.3.6.1	Det största möjliga modulusvärdet ska användas vid nyckelutbyte.
11.3.7	**Framåtsäkerhet (PFS)**
Resonemang	Tillämpning av framåtsäkerhet (PFS) minskar konsekvenserna ifall en Security Associations (SA) röjs.
Rekommendation id	**Rekommendation**
11.3.7.1	Framåtsäkerhet (eng. *PFS, Perfect Forward Secrecy*) ska aktiveras för IPsec anslutningar.
11.3.8	**IKE Extended Authentication (XAUTH)**
Resonemang	XAUTH genom IKEv1 är sårbar mot attacker.
Rekommendation id	**Rekommendation**
11.3.8.1	Vid användning av IPsec förbindelser som använder IKEv1 ska XAUTH inaktiveras.

12 Nyckelhantering

12.1 Mål

Målet med att vidta åtgärderna i detta kapitel är att hanteringen av nycklar sker på ett säkert och korrekt sätt.

12.2 Bakgrund

12.2.1 Omfattning

Detta kapitel beskriver regler och rutiner vilka är nödvändiga för en säker hantering av kryptografiska nycklar.

12.2.2 Syfte

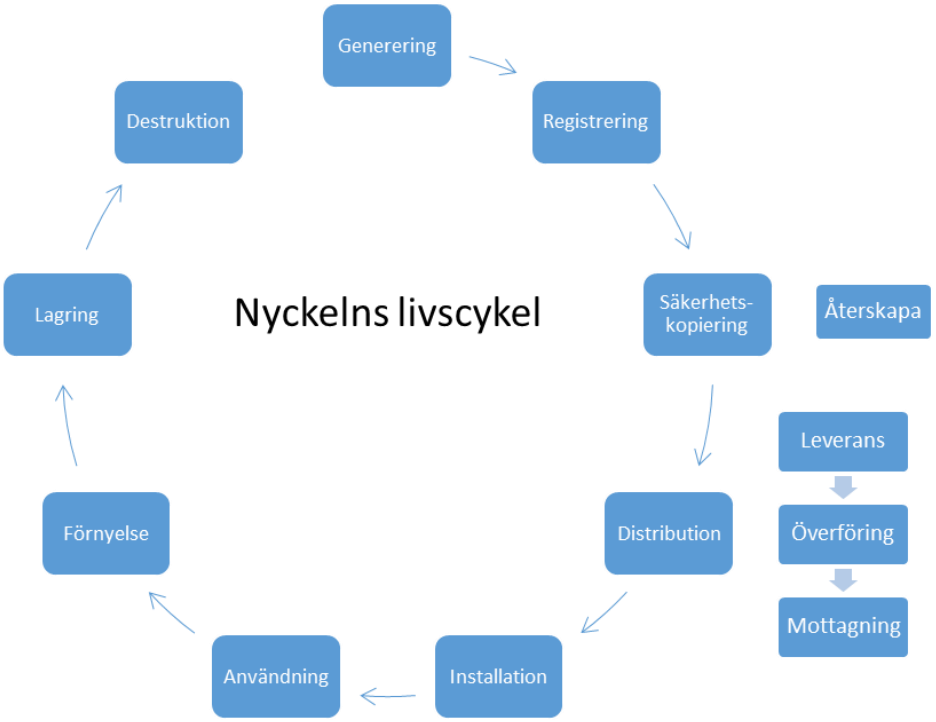
I teorin kan de flesta kryptografiska algoritmer forceras genom kryptoanalys. Detta kräver i realiteten en ytterst svåråtkomlig mängd datorkraft och resurser. Därför blir en forcering av algoritmen i praktiken en omöjlighet – såvida rätt algoritm, protokoll och nyckellängd väljs och är korrekt implementerade. 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.

12.2.3 Om nyckelhantering

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). omfattar följande:



12.2.4 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

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

12.2.5 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 återskapa

vid en situation där den går förlorad. Här ställs behoven av att skydda tillgängligheten till en informationstillgång mot att skydda konfidentialiteten av den samma.

12.2.6 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.

12.2.7 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, se kap 4.3.5.1. • Eventuell övrig relevant dokumentation över funktion eller användning

12.3 Åtgärder

12.3.1	**Nyckelhanteringsplan**
Resonemang	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 skyddet av kryptonycklar beskrivs i.
Rekommendation id	**Rekommendation**
12.3.1.1	Regler för användning, skydd och giltighetstid för kryptografiska nycklar för deras hela livscykel ska utvecklas och införas i organisationen.
12.3.2	**Kryptonycklars livslängd**
Resonemang	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.
Rekommendation id	**Rekommendation**
12.3.2.1	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.
12.3.2.2	Beslut om livslängden för kryptonycklar ska dokumenteras.
12.3.2.3	Beslutade livslängder för olika typer av kryptonycklar ska finnas för alla organisationens krypteringslösningar.
12.3.3	**Vid röjande av nycklar**
Resonemang	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.
Rekommendation	**Rekommendation**

[13] Amerikanska NIST (National Institute of Standards and Technology) tillhandahåller riktlinjer för att bestämma livslängd på nycklar i dokumentet *”NIST SP 800-57 rev 4”* i avsnitt ”5.3 Cryptoperiods”.

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

13 Hardware Security Modules

13.1 Mål

Målet med att vidta åtgärderna i detta kapitel är att kryptografiska hårdvarumoduler (eng. *Hardware Security Modules, HSM*) används där sådant behov finns och att det sker på ett säkert och korrekt sätt.

13.2 Bakgrund

13.2.1 Omfattning

En HSM är hårdvara avsedd för att utföra kryptografiska operationer. HSM:er kan integreras i en kryptolösning, installeras på en dator, server eller kopplas in externt. HSM:er kan förekomma som separata enheter, PCI-kort, USB enheter eller smarta kort.

HSM:er kan användas för kryptering, dekryptering, generering av nycklar, digital signering, hashning eller för att snabba upp kryptografiska funktioner.

13.2.2 Syfte

HSM:er erbjuder hög säkerhet och tillförlitlighet då de är slutna system med lägre risk för oupptäckt manipulation eller annan extern påverkan. De har också hög effektivitet tack vare att hårdvaruimplementationer ofta kan vara snabbare än mjukvara, i de fall den använda datorns huvudsyfte är ett annat än kryptering. HSM:er innebär dock högre kostnader och ökade krav på underhåll och administration.

Traditionellt används HSM:er i uttagsautomater, elektroniska banköverföringar och point of sale-nätverk. HSM:er kan även användas inom *Public Key Infrastructure* (PKI) för att säkra CA-nycklar eller för att bistå med kryptografisk funktionalitet för öka effektivitet hos webbservrar som använder TLS.

13.2.3 Fysisk säkerhet

En HSM har ofta fler lager av skydd som tillsammans skyddar nyckelmaterialet. Det mest grundläggande skyddet är att nyckelmaterialet kan utplånas efter ett givet antal misslyckade aktiveringsförsök.

13.2.3.1 Upptäckande av manipulering

HSM:en är utformad så att försök till manipulation ska gå att upptäcka. Exempelvis används förseglingar och etiketter som går sönder eller visar ett annars osynligt meddelande efter manipulationsförsök gjorts på hårdvaran. För att upptäcka manipulationsförsök krävs regelbundna kontroller av dessa förseglingar.

13.2.3.2 Manipuleringsskydd

Skyddet mot manipulering ska begränsa möjligheten att fysiskt manipulera,

bryta sig in i eller utvinna användbar information ur en HSM. Ofta är kretskorten och dess komponenter inneslutna i en epoxi-liknande material. Det kan också finnas skydd som förstör komponenter då den borras i, skrapas på eller på annat sett manipuleras. Till exempel kan ett elektriskt ledande material användas i epoxin som sedan övervakas av interna sensorer. Ifall sensorerna känner av en förändring kan det vara ett bevis på manipulationsförsök. Enheter kan också utrustas med sensorer som känner av förändringar i exempelvis temperatur, radioaktiv strålning, ljus eller luft.

13.2.3.3 Försvarsmekanismer

HSM:er kan innehålla försvarsmekanismer som aktiveras om eventuella manipulationsförsök upptäcks. Exempelvis kan alla kryptonycklar och annan känslig data rensas eller skrivas över.

13.2.3.4 Aktiveringsskydd

HSM:er kan erbjuda möjlighet att implementera M-of-N (se kapitel 12) vid aktivering av lagrade kryptonycklar.

13.3 Åtgärder

13.3.1	**Hardware Security Modules**
Resonemang	För att möta krav på hög assurans, hög säkerhet, och/eller för att möjliggöra en effektiv kryptering av stora mängder data, ska användning av en HSM övervägas.
Rekommendation id	**Rekommendation**
13.3.1.1	
13.3.1.2	
13.3.1.3	
13.3.1.4	Användningen av HSM ska dokumenteras enligt 4.3.1.2 och om den används för nyckelhantering också enligt 12.2.7.
13.3.1.5	En HSM som används bör ha genomgått en oberoende granskning, t.ex. enligt Common Criteria eller FIPS PUB 140-2.

14 DNSSEC

14.1 Mål

Målet är att säkra DNS från missbruk och man-in-the-middle-attacker.

14.2 Bakgrund

14.2.1 Omfattning

Mycket av nätverkstrafiken är beroende av korrekta och tillförlitliga DNS-uppslag. DNS som utvecklades på 1980-talet är dock sårbart för ett antal olika attacker som kan manipulera svar på DNS-frågor. Några av de mest kända och största hoten mot DNS är cacheförgiftning (cache poisoning)[14] och farmning (pharming)[15].

14.2.2 Syfte

DNSSEC är säkerhetsåtgärd som innebär att det går att avgöra om det svar som ges på en DNS-fråga kommer från rätt källa och att det inte manipulerats på vägen. Detta görs genom att validera en digital signatur som medföljer svaret. Det blir alltså svårt att förfalska information i DNS som är signerad med DNSSEC utan att det upptäcks.

Funktionen är endast konstruerad för att förhindra attacker där angriparen manipulerar svar på DNS-frågor för att uppnå sitt mål.

Rekommendationerna nedan är endast på en övergripande nivå. Mer detaljerade åtgärder och förslag på krav vid upphandling och utveckling av DNSSEC-tjänster finns beskrivna i ”Rekommendationer för införande av DNSSEC i kommuner och motsvarande verksamheter” från IIS[16].

[14] Cacheförgiftning innebär att en situation skapas, antingen genom en attack eller oavsiktligt, som förser en namnserver med DNS-data som inte kommer från en auktoritativ källa. Ett av de mest välkända exemplen på detta är den under 2008 mycket uppmärksammade Kaminskybuggen. (Källa: IIS.se)

[15] Farmning innebär att någon får själva innehållet i DNS att peka på felaktiga servrar. Rent konkret innebär det att en webbadress för exempelvis en bank kan pekas om till en helt annan webbserver, men för besökaren ser det fortfarande i adressfältet ut som att det är rätt server i andra änden. (Källa: IIS.se)

[16] Rekommendationer för införande av DNSSEC i kommuner och motsvarande verksamheter, IIS.se, 2014

14.3 Rekommendationer

14.3.1	**DNSSEC**
Resonemang	För att möjliggöra att de som efterfrågar ett namnuppslag från organisationens DNS ska kunna lita på att svaret är korrekt och inte kan manipuleras vid transport kan DNSSEC användas. Rekommenderade kryptografiska algoritmer ska användas i de fall inte bakåtkompabilitet i protokollet kräver annat.
Rekommendation id	**Rekommendation**
14.3.1.1	De domäner som organisationen publicerar extern (t.ex. organisation.se) ska säkras med hjälp av DNSSEC.
14.3.1.2	Signeringssystemet ska stödja DNSSEC enligt RFC 4033, RFC 4034 och RFC 4035.
14.3.1.3	Signeringssystemet ska stödja signering med följande algoritmer: • RSA/SHA-256, • RSA/SHA-512 såsom beskrivet i RFC 5702.
14.3.2	**Nyckellängder i DNSSEC**
Resonemang	En separation av nycklar mellan nyckelsigneringsnyckel (KSK) och zonsigneringsnyckel (ZSK) rekommenderas. Anledningen är att det i dagsläget är den vanligast förekommande och mest beprövade modellen för nyckelhantering. Signeringsalgoritmen som används ska vara RSA/SHA-256, då detta är den algoritm som idag används av roten för domännamnssystemet (DNS).

14.3.2.1	Följande nyckellängder rekommenderas för nycklarna i DNSSEC: • KSK: 2048-bit RSA/SHA-256 • ZSK: 2048-bit RSA/SHA-256

Bilaga A - Referenser

NIST SP 800-57	Rev. 4, Recommendation for Key Management: Part 1: General. E. Barker	Januari 2016
NIST SP 800-38A	Recommendation for Block Cipher Modes of Operation: Methods and Techniques, M. Dworkin	December 2001
NIST SP 800-38B	Recommendation for Block Cipher Modes of Operation: The CMAC Mode for Authentication, M. Dworkin	Maj 2005
NIST SP 800-38D	Recommendation for Block Cipher Modes of Operation: Galois/Counter Mode (GCM) and GMAC, M. Dworkin	November 2007
FIPS 46-3	Data Encryption Standard (DES), NIST	Oktober 1999
FIPS 140-2	Security Requirements for Cryptographic Modules, NIST	Maj 2001
FIPS 180-4	Secure Hash Standard, NIST	Augusti 2015
FIPS 186-4	Digital Signature Standard (DSS), NIST	Juli 2013
FIPS 197	Advanced Encryption Standard, NIST	November 2001
FIPS 202	SHA-3 Standard: Permutation-Based Hash and Extendable-Output Functions, NIST	Augusti 2015
PKCS #1 v2.2	PKCS#1: RSA Cryptography Standard, RSA Laboratories	Oktober 2012
RFC 2313	PKCS#1: RSA Encryption, Version 1.5, RSA Laboratories EAST	Mars 1998
ISO 9797-1	Information technology – Security techniques – Message Authentication Codes (MACs) Part 1: Mechanisms using a block cipher	Mars 2011
ISO 9797-2	Information technology – Security techniques – Message Authentication Codes (MACs) Part 2: Mechanisms using a dedicated hash-function	Maj 2011
ISO 10116	Information technology – Security techniques – Modes of operation for an n-bit block cipher	Februari 2006

ISO 10118-3	Information technology – Security techniques – Hash-functions – Part 3: Dedicated hash-functions	Mars 2004
ISO 14888-3	Information technology – Security techniques – Digital signatures with appendix – Part 3: Discrete logarithm based mechanisms	Mars 2016
ISO 15408	Information technology – Security techniques – Evaluation criteria for IT security	December 2009
BSI TR-03111	Elliptic Curve Cryptography ver. 2.0, BSI	Juni 2012
RFC 2104	HMAC: Keyed-Hashing for Message Authentication, H. Krawczyk, M. Bellare and R. Canetti.	Februari 1997
RFC 2401	Security Architecture for the Internet Protocol, S. Kent and R. Atkinson.	November 1998
RFC 3602	The AES-CBC Cipher Algorithm and Its Use with IPsec, Frankel, et al.	September 2003
RFC 4106	The Use of Galois/Counter Mode (GCM) in IPsec Encapsulating Security Payload (ESP), Viega & McGrew	Juni 2005
RFC 4252	The Secure Shell (SSH) Authentication Protocol, T. Yionen and C. Lonvick.	Januari 2006
RFC 4880	OpenPGP Message Format, J. Callas, et. al.	Maj 2008
RFC 5246	The Transport Layer Security (TLS) Protocol Version 1.2, T. Dierks and E. Rescoria.	Augusti 2008
RFC 5288	AES Galois Counter Mode (GCM) Cipher Suites for TLS, Salowey, et al.	Augusti 2008
RFC 5639	Elliptic Curve Cryptography (ECC) Brainpool Standard Curves and Curve Generation, Lochter & Merkle	Mars 2010
RFC 5751	Secure/Multipurpose Internet Mail Extensions (S/MIME) Version 3.2 Message Specification, B. Ramsdell and E. Turner.	Januari 2010
RFC 6379	Suite B Cryptographic Suites for IPsec, Law & Solinas, NSA	Oktober 2011
RFC 8446	The Transport Layer Security (TLS) Protocol Version 1.3	Augusti 2018

SP-188	188 Scheme Crypto Policy, Issue 7.0, CSEC	April 2017
SOG-IS	SOG-IS Crypto Evaluation Scheme Agreed Cryptographic Mechanisms, version 1.1	Juni 2018
JO-0241 ANSSI	"*Avis relatif aux paramètres de courbes ellitpiques définis pas l'État français*", ANSSI, Journal Officiel 0241	Oktober 2011
ENISA	Algorithms, Key Sizes and Parameters Report, 2013 recommendations	Oktober 2013