CERTEZZA

2025-03-31
Version 1.0

VÄGLEDNING VID MIGRERING TILL KVANTDATORSÄKRA ALGORITMER

Framtagen av Certezza AB med projektfinansiering från NCC-SE och MSB.

NCC-SE
MSB Myndigheten för samhällsskydd och beredskap
Medfinansieras av Europeiska unionen
ECCC EUROPEAN CYBERSECURITY COMPETENCE CENTRE

Denna vägledning är tänkt som ett stöd för verksamheter inom såväl privat som offentlig sektor i arbetet med övergången från dagens krypterings- och signeringsalgoritmer till algoritmer som upprätthåller en tillräcklig nivå av säkerhet även i framtidens digitala miljö, där kvantdatorer har en förmåga att knäcka dagens kryptografiska algoritmer. Vägledningen riktar sig i första hand till de personer som utvecklar, hanterar och förvaltar en organisations it-miljö, till exempel it-direktörer, it-chefer, it-säkerhetsansvariga, it-säkerhetsarkitekter och informationssäkerhetsansvariga som i sin roll ansvarar för att säkerställa att tillräckliga säkerhetsåtgärder vidtas för att åstadkomma en långsiktigt säker informationshantering.

I vägledningen beskrivs bakgrunden till varför denna migrering till nya algoritmer är nödvändig, där den drivande faktorn är att utvecklingen av kvantdatorer går snabbt framåt. Inom en snar framtid förväntas det finnas kvantdatorer som kan forcera dagens kryptografiska algoritmer. För att säkerställa att känslig information inte röjs så krävs det att åtgärder vidtas och att det arbetet påbörjas omgående. Målet är att migrera över till nya kvantdatorsäkra algoritmer som har tagits fram för att ersätta dagens algoritmer.

Det finns vissa förutsättningar som krävs för att kunna genomföra denna migrering, såsom standarder kopplade till de nya kvantdatorsäkra algoritmerna och stöd i mjuk- och hårdvara från leverantörssidan. I samband med framtagningen av vägledningen har en mognadsmätning baserad på stickprovskontroll gjorts på marknaden. Mätningen som gjorts presenteras i vägledningen och visar att mognadsgraden hos produktleverantörerna i dagsläget inte är särskilt hög och att mycket arbete kvarstår innan en full migrering är möjlig.

Trots detta är det viktigt att redan nu påbörja arbetet med migreringen genom att få nödvändigt förarbete på plats och, där det är möjligt, även genomföra själva migreringen. Vägledningens huvudsakliga syfte är att beskriva de steg som varje organisation behöver genomföra för att på ett kontrollerat sätt förbereda sig och migrera över till nya kvantdatorsäkra algoritmer.

Det första steget är att ta reda på vilka regulatoriska krav kopplade till kryptografi som ställs på ens organisation. En övergripande redogörelse för regulatoriska krav för privata och offentliga organisationer inom detta område presenteras i vägledningen.

Det andra steget är att genomföra en informationsklassning för att identifiera och värdera organisationens informationstillgångar utifrån deras skyddsbehov – konfidentialitet, riktighet och tillgänglighet. Detta omfattar att identifiera var informationen finns, i vilken form den förekommer (t.ex. i databaser eller

filsystem) samt vilken påverkan ett obehörigt röjande, en otillåten ändring eller ett bortfall skulle kunna få på verksamheten. Klassningen utgör underlag för att prioritera vilka tillgångar som är mest kritiska vid planering av åtgärder, såsom migrering eller införande av nya säkerhetsmekanismer. Vid inventeringen av it-miljön – inklusive protokoll, applikationer och hårdvara som använder kryptografiska algoritmer – är det även viktigt att dokumentera beroenden mellan komponenter för att möjliggöra en strukturerad och kontrollerad migrering.

Det sista steget är själva migreringen och vägledningen beskriver vilka olika metoder som finns för att genomföra en migrering. I huvudsak är alternativen att antingen migrera hela eller delar av sin miljö rakt av från gamla till nya kryptografiska algoritmer eller att använda sig av hybridcertifikat som innehåller certifikat med både gamla och nya algoritmer. Eftersom stöd än så länge saknas i många protokoll och produkter är omvärldsbevakning av marknaden en väsentlig del i arbetet med migreringen. Vilken metod för migrering du väljer blir till stor del beroende på marknadens utveckling.

Målet med vägledningen är att tillhandahålla den kunskap och de verktyg som krävs för att kunna planera, prioritera och genomföra migrering till kvantdatorsäkra algoritmer på ett kontrollerat och säkert sätt och därmed minska risken att värdefull information blir röjd, förändrad eller förvanskad.

CERTEZZA

Innehållsförteckning

Innehåll

1. Inledning

Utvecklingen av kvantdatorer går fort framåt och har accelererat på senare tid. Google lanserade sitt kvantdatorchip Willow i december 2024. I februari 2025 lanserade Microsoft sitt chip Majorana 1 som förväntas kunna skala upp till en miljon qubits (enheten för prestanda för kvantdatorer). Det är ett stort steg på vägen för att kunna forcera de algoritmer som används inom kryptografi idag. I Kina publicerades nyligen information om Zuchongzhi 3.0 som pekar på att den ligger i toppskiktet av de kvantdatorer vi känner till.

Detta är vad vi idag vet baserat på tillgänglig offentlig information. Samtidigt sker det utveckling av kraftfulla kvantdatorer, såväl av privata som statliga aktörer, där allmänheten inte har insyn. Vi bör därför utgå från att det som är allmänt känt är "lägstanivån" för kvantdatorernas kapacitet.

Det finns ännu inga indikationer att en kvantdator kan forcera dagens godkända kryptografiska algoritmer och vi har i arbetet inte funnit någon verifierbar offentlig information om kvantdatorer med sådan kapacitet.

Till skillnad från den snabba utvecklingen av kvantdatorer går framstegen inom utvecklingen av mjuk- och hårdvara som är resistent mot beräkningar av kvantdatorer inte lika fort. I augusti 2024 standardiserades tre algoritmer, av amerikanska National Institute of Standards and Technology (NIST), som är att betraktas som kvantdatorsäkra. Stöd för dessa algoritmer börjar komma i en del programvara men det är inte tillräckligt för att påbörja en migrering (övergång) till kvantdatorsäkra algoritmer. Det saknas för närvarande stöd i Microsoft Windows vilket är ett problem på både server- och klientsidan. I Linux finns stöd men det är inte lika väl integrerat som traditionella algoritmer, vilket till stor del beror på de stora skillnaderna mellan de nya algoritmerna och de vi använder idag. Mycket beror på att det saknas stöd eller att prestandan är bristfällig i applikationer och protokoll som till exempel SSH, RDP, TLS, S/MIME etc. för att kunna använda de nya algoritmerna.

Dagens webbläsare har stöd för de nya algoritmerna men Transport Layer Security (TLS) 1.3 är inte optimerat för detta då mängden dataöverföring som krävs för att etablera en förbindelse ökar mångfalt. En annan utmaning är att Internet Engineering Task Force (IETF) inte har standardiserat hur certifikat baserade på kvantdatorsäkra algoritmer, eller hybridcertifikat med både nya och gamla algoritmer, ska se ut. Det finns idag flera leverantörer som har stöd för kvantdatorsäkra algoritmer i sin mjuk- och/eller hårdvara men dessa produkter är inte baserade på de färdiga standarderna vilket gör det svårt och komplicerat att implementera algoritmerna i leverantörernas produkter.

I de stickprov som har gjorts hos ett urval av leverantörer, i samband med framtagandet av den här vägledningen, varierar leverantörernas mognadsgrad. Inte alla leverantörer har beaktat samtliga aspekter i arbetet med att migrera till kvantdatorsäkra algoritmer utan nöjer sig med att påstå att de har stöd för dessa. Det vill säga att leverantörerna introducerar stöd för att konsumera data som är krypterat eller signerat av kvantdatorsäkra algoritmer, men

de använder till exempel inte kvantdatorsäkra algoritmer för att signera sin egen programvara/kod.

Den i nuläget omogna marknaden gör att du som representant för en verksamhetsutövare än så länge måste ta ett stort eget ansvar baserat på verksamhetens egna krav och behov samt ställa krav på leverantörerna för att driva marknaden framåt. I det som kan räknas som "kärnan" i ett system som hanterar kryptografiskt material, som till exempel Hardware Security Modules (HSM), Certificate Authorities (CA) och Key Management Systems (KMS), finns det stöd, om än begränsat i vissa fall. För annan tillämpning är möjligheterna för användning av kvantdatorsäkra kryptoalgoritmer sämre. Smartcards med stöd för kvantdatorsäkra algoritmer kommer inte att kunna levereras förrän tidigast under 2026, om standarderna för området etableras. Exempelvis har IETF inte standardiserat hur ett certifikat med nyckelmaterial baserat på kvantdatorsäkra algoritmer ska vara utformat, vilket gör det svårt att skapa produkter som ska hantera certifikaten.

Det som just nu gör att tillämpningen för smartcards dröjer är att standardiseringsarbetet inte är klart, inte bara det som rör specifikt smartcards, utan även det som rör olika protokoll. De nya algoritmerna fungerar redan i vissa fall, men algoritmerna kommer att kräva att man optimerar exempelvis protokoll för att de ska ha samma prestanda som de har idag. En av orsakerna till att de kvantdatorsäkra algoritmerna försämrar prestandan för tjänsterna är att certifikaten blir större när de innehåller nyckelmaterial för kvantdatorsäkra algoritmer.

Arbete med att lösa utmaningarna pågår och många leverantörer ligger i startgroparna, men det återstår fortfarande mycket arbete för att kunna tillämpa kvantdatorsäkra kryptoalgoritmer på ett effektivt sätt så att data är säkrad när kvantdatorerna får sitt genombrott.

Det kommer att krävas omfattande arbete för att migrera från dagens godkända algoritmer till den nya eran av kvantdatorsäkra algoritmer. Det kommer sannolikt även att kräva ny hårdvara och ny mjukvara i flertalet sammanhang vilket verksamhetsutövare behöver vara förberedda på. Redan nu rekommenderar vi att verksamhetsutövare som är beroende av kryptering för att skydda sin information gör en inventering och prioritering av sina system. Detta för att ta reda på vad som är mest kritiskt och vilka system som behöver prioriteras för migrering till kvantdatorsäkra algoritmer.

1.1 Tillämpningsområdet och avgränsningar

Vägledningen är en sammanställning av lägesbilden gällande kvantdatorsäker kryptering per den 31:a mars 2025. Utvecklingen går framåt och läget förändras från månad till månad. I flera fall är det inte praktiskt möjligt att migrera annat än mycket avgränsade miljöer. Vägledningen beskriver bland annat olika vägval vid migrering och förslag på strategier för att kunna genomföra en migrering på bästa sätt när förutsättningarna är på plats.

Vägledningen går inte in i detalj på all metodik som krävs för att genomföra samtliga moment som till exempel hur man genomför en riskanalys.

Vägledningen berör inte verksamheter som är av betydelse för Sveriges säkerhet eller som omfattas av ett för Sverige förpliktande internationellt åtagande om säkerhetsskydd (säkerhetskänslig verksamhet). Vissa myndigheter ska med stöd av 16 § förordningen (2015:1053) om totalförsvar och höjd beredskap inneha säkra kryptografiska funktioner. Även verksamheter som omfattas av lagen (2018:585) om säkerhetsskydd kan ha krav på sig att skydda uppgifter med säkra kryptografiska funktioner, jämför 3 kap. 5 § andra stycket säkerhetsskyddsförordningen (2021:955). Säkra kryptografiska funktioner är sådana som godkänts av Försvarsmakten. De kvantdatorsäkra kryptografiska funktioner som behandlas i denna vägledning har, såvitt är känt, ännu inte godkänts av Försvarsmakten för användning i säkerhetskänslig verksamhet vilket gör att denna tillämpning faller utanför vägledningens tillämpningsområde. Frågor om signalskyddstjänsten faller därmed också utanför tillämpningsområdet.

1.2 Syfte och målgrupp

Många verksamhetsutövare står idag handfallna inför insikten om att dagens kryptoalgoritmer börjar närma sig sitt ”bäst före”-datum, samtidigt som det är okänt när detta datum inträffar. Därtill kommer nya regulatoriska krav som bland annat ställer krav på verksamhetsutövare att fastställa strategier och förfaranden för kryptografi. Detta innebär att alla verksamheter bör vara förberedda på och ha en strategi för hur övergången kan göras. Det finns idag godkända kvantdatorsäkra algoritmer som kan användas. Utmaningen för många verksamhetsutövare är hur de ska/bör/kan gå tillväga för att kvantdatorsäkra sin digitala infrastruktur.

Det behövs mer kunskap om betydelsen av att övergå till kvantdatorsäkra algoritmer samt förberedelse för att på ett smidigt sätt genomföra en sådan övergång och därmed öka sin beredskap mot kvantdatorer med förmåga att knäcka dagens godkända algoritmer. Det behövs kännedom om vilka befintliga och kommande regulatoriska krav beträffande kryptering som finns, bland annat för att cybersäkerhetsexpertis ska få gehör hos ledningar så att verksamheten kan genomföra den strategi och de förfaranden för kryptografi som det nya regelverket kräver.

Syftet med denna vägledning är därför att ge verksamhetsutövare i offentlig och privat sektor stöd och vägledning för kunna att påbörja arbetet med att migrera från dagens kryptografiska algoritmer till kvantdatorsäkra algoritmer för kryptering och signering. Vägledningen beskriver metoder för att inventera sin IT-miljö och identifiera behoven av migrering så att arbetet med migrering kan påbörjas där så är möjligt. Områden som innefattas är kryptering av data (vilande och i rörelse), förbindelser och signering av data av olika slag. Vägledningen beskriver inte i detalj hur en migrering kan gå till utan syftar till att skapa en förståelse för vikten av att migrera och hur verksamhetsutövaren på en övergripande nivå kan gå till väga.

Vägledningen är tänkt som ett stöd för till exempel it-direktörer, it-chefer, it-säkerhetsansvariga, it-säkerhetsarkitekter och informationssäkerhetsansvariga att kunna presentera för beslutsfattare inom sina respektive organisationer vilka åtgärder som behöver vidtas och varför. Den kan bidra till att öka medvetenheten och underlätta samarbetet med verksamhetens ledning för att erhålla stöd och förståelse för arbetet, samt för att tydliggöra att det kommer att krävas både insatser och investeringar – inte bara för att skydda verksamheten, utan även för att möta framtida regulatoriska krav. Det underlättar planeringen och genomförandet av åtgärder kopplade till strategin för (kvantdatorsäker) kryptografi. Vägledningen ska även ge kunskap om vilka risker som är förknippade med att verksamhetsutövaren inte har någon strategi för att hantera krypterat data eller krypterade förbindelser i förhållande till de regulatoriska krav som kommer att gälla.

1.3 Disposition

Kapitel 1 presenterar vägledningens tillämpningsområde, syfte och målgrupp.

Kapitel 2 beskriver bakgrunden till behovet av att migrera till nya krypterings- och signeringsalgoritmer

Kapitel 3 presenterar vilka tidsramar som finns att förhålla sig till.

Kapitel 4 är en sammanställning av de regulatoriska krav som organisationer inom privat och offentlig sektor behöver förhålla sig till kopplat till kryptografi.

Kapitel 5 beskriver de förutsättningar man har att förhålla sig till med en nulägesbild för krypteringsalgoritmer och produkter som nyttjar dessa.

Kapitel 6 beskriver den inventering som varje verksamhet behöver göra av sin it-miljö inför migreringen.

Kapitel 7 redogör för de olika metoder som finns för att migrera till nya algoritmer samt i vissa fall hantera befintliga algoritmer på ett säkert sätt.

Kapitel 8 sammanfattar rekommenderade åtgärder för att kvantdatorsäkra sin it-miljö.

Bilaga A innehåller en förteckning med beskrivningar av begrepp som förekommer i dokumentet.

Bilaga B innehåller en referenslista på standarder och andra tekniska och juridiska källor som vägledningen är baserad på.

2. Bakgrund

2.1 Orsak till behovet av nya krypteringsalgoritmer

Idag används kryptografiska algoritmer för att kryptera, signera och autentisera data eller digitala identiteter. Förbindelser mellan datorer är idag allt som oftast krypterade för att inte obehöriga ska kunna läsa data, se vilken information som skickas mellan två enheter eller säkerställa att rätt parter kommunicerar.

Dagens algoritmer är ändamålsenliga, effektiva och välfungerande. De förutses dock bli forcerbara inom en inte alltför avlägsen framtid, antingen på grund av kvantdatorer eller att traditionella halvledarbaserade datorer blir tillräckligt kraftfulla. Av dessa två alternativ verkar kvantdatorer vara det mest sannolika för att knäcka dagens kryptoalgoritmer. Därmed utgör kvantdatorer det största hotet mot skyddet av våra informationstillgångar och system.

Historiskt har utveckling och implementation av kryptoalgoritmer gått relativt långsamt och vissa sårbara kryptoalgoritmer som t.ex. Secure Hash Algoritm 1, (SHA1) används fortfarande. Den tekniska utvecklingen på området sker i allt snabbare takt vilket innebär att medvetenheten om riskerna och förmågan att säkra system och informationstillgångar måste öka.

Arbetet med att byta ut sårbara algoritmer är omfattande och behöver påbörjas snarast för att undvika att informationstillgångar som fortfarande är aktuella och/eller innehåller konfidentiella uppgifter kan dekrypteras och avslöjas för obehöriga när förmåga finns.

För att uppnå säkerhet krävs mer än att bara kryptera om data med en ny algoritm. Det krävs bland annat organisatoriska åtgärder såsom inventering av krypterade data och en förändring i hur verksamheten i övrigt använder kryptografi. Det är viktigt att komma ihåg att det inte bara är krypterad data som ligger i riskzonen utan även digitala signaturer och autentiseringar mot system. Därför behöver verksamhetsutövare även se över den befintliga teknik som använder kryptografi idag. Det kan vara allt från smarta kort, nätverksutrustning, skrivare och TV-apparater till stordatorer och molntjänster.

2.2 Grunderna i kryptering

Det finns idag i två huvudsakliga kryptografiska metoder som används, asymmetrisk kryptering och symmetrisk kryptering. Metoderna har olika användningsområden där asymmetrisk kryptering huvudsakligen används för transport av symmetriska krypteringsnycklar. Användare kommer dagligen i kontakt med kryptering - exempelvis när en person ansluter till en webbsida som har Transport Layer Security (TLS) aktiverat (krypterad anslutning till hemsida), vilket är normen idag, eller vid användning av e-legitimation.

Asymmetrisk kryptering bygger på ett nyckelpar där den ena nyckeln är den privata, som är just privat och måste skyddas från obehörig åtkomst, och den andra publik, som vem som helst kan få tillgång till. I fallet med webbsidor använder webbservern, mycket förenklat, nyckelparet för att skapa en krypterad förbindelse mellan server och klient. Även signaturer och elektroniska underskrifter använder asymmetriska nyckelpar. Den vanligaste algoritmen för detta idag är Rivest–Shamir–Adleman (RSA), även om det finns alternativ i till exempel algoritmer som bygger på elliptiska kurvor (Elliptic Curve Cryptography, ECC).

Symmetrisk kryptering bygger på att båda parter har samma nyckel för att kryptera och dekryptera data. En vanlig algoritm för detta är Advanced Encryption Standard (AES). Problemet med symmetrisk kryptering är att på ett säkert sätt göra nyckeln tillgänglig för båda och enbart dessa parter. Detta brukar ofta lösas genom att man börjar med att upprätta en krypterad förbindelse, med hjälp av asymmetrisk kryptering, vars syfte är att föra över den symmetriska nyckeln till den andra parten. När nyckeln är delad mellan parterna sker sedan krypteringen av informationen med symmetrisk nyckel. TLS är till exempel baserat på en sådan lösning.

Algoritmerna har beroende på nyckellängd, som definieras i sektion 5.6.1.1 i National Institute of Standards and Technology (NIST) SP 800-57 part 1 rev 5 för symmetriska och asymmetriska algoritmer, en säkerhetsnivå som används i olika skrivningar från NIST och i Commercial National Security Algorithm Suite (CNSA) 2.0. När man pratar om säkerhetsnivån på en nyckellängd använder man symmetriska nyckellängder som måttstock, till exempel motsvarar en symmetrisk nyckel på 112 bitar en RSA nyckel på 2048 bitar vilket har säkerhetsnivå 2. Observera att kryptering upp till och med 80 bitars kryptering har fasats ut, liksom 3TDEA ("3DES").

Tabellerna nedan visar vilken säkerhetsnivå en nyckellängd för olika algoritmer motsvarar. Det är brukligt att beskriva styrkan i en kryptografisk algoritm i mängden bitar för symmetrisk kryptering. Notera att det är de vanligaste algoritmerna som är inkluderade i tabellerna nedan.

Säkerhetsnivå	Antal bitars symmetrisk kryptering	RSA-nyckellängd	ECC-nyckellängd	Övriga symmetriska algoritmer
1	Upp till 80 bitar	1024 bitar	160-223 bitar	2TDEA
2	112 bitar	2048 bitar	224-255 bitar	3TDEA eller AES112
3	128 bitar	3072 bitar	256-383 bitar	AES128
4	192 bitar	7680 bitar	384-511 bitar	AES192
5	256 bitar	15360 bitar	>512 bitar	AES256

För hash och hash-baserade funktioner ser nivåerna ut enligt följande, där SHA1 är under utfasning eftersom den inte längre betraktas som tillförlitlig.

Säkerhetsnivå	Antal bitars symmetrisk kryptering	SHA-algoritm
1	Upp till 80 bitar	SHA1
2	112 bitar	SHA-224, SHA512/224, SHA3-224
3	128 bitar	SHA-256, SHA512/256, SHA3-256
4	192 bitar	SHA-384, SHA3-384
5	256 bitar	SHA-512, SHA3-512

Som ett alternativ till RSA finns algoritmer som baseras på ECC där nyckellängden är markant kortare än jämförbar längd på en RSA-nyckel. Fördelen med ECC är att nycklarna är kortare vilket för att beräkningarna blir enklare. ECC är inte så vanligt förekommande, vilket beror på att det i många fall saknas stöd för den i många system samt att den inte ger så stora fördelar jämfört med RSA ur ett säkerhetsperspektiv. Varken RSA eller ECC är motståndskraftiga mot attacker med kvantdatorer.

Utöver ovan nämnda krypteringsmetoder finns det algoritmer som ligger till grund för funktioner som används för att räkna ut kontrollvärden (hash-värden) och därav saknar de kryptografiska nycklar. Hash-värdet kan beskrivas som en datamängds fingeravtryck. Hash-algoritmer används inte för kryptering, men är en viktig funktion inom kryptografi av andra anledningar. Hash-värdet används till exempel för att kontrollera att installationsfiler för en applikation inte har modifierats sedan de lämnade leverantören. Hash-värdet för texten "Sommar 2024" och hash-värdet för texten "sommar 2024" är helt olika trots att skillnaden bara är att första bokstaven i huvudorden är versal respektive gemen.

2.3 Kryptografisk utveckling

De algoritmer som används idag har sina rötter i 70-talet då RSA började användas. Därefter kom hash-algoritmer och på 90-talet introducerades SHA1 som en form av standard. Den modernaste versionen av "klassisk" hash-algoritm, SHA3, lanserades redan 2015, men har tagits i bruk endast i ytterst liten omfattning. Redan 2005 ansågs SHA1 vara osäker, men det faktum att algoritmen fortfarande används i olika system visar på hur trögt det går att byta ut algoritmer till säkrare alternativ.

Användarna har fram till nu kompenserat svagheter i algoritmerna med att använda längre nycklar. För till exempel RSA är den rekommenderade kortaste nyckellängden 3072 bitar, men de flesta använder fortfarande nyckellängder på 2048 bitar. Det här beror till stor del på att många system inte kan hantera längre nyckellängder i kombination med att det är kostsamt att byta ut systemen.

För närvarande består det största hotet mot skyddet av krypterade data i att verksamheten använder algoritmer och nyckellängder som är sårbara för olika former av angrepp samt hur nycklarna skyddas. Målet för angriparen är att läsa krypterad kommunikation eller data, alternativt att förvanska data. Risken för att man med hjälp av kvantdatorer ska kunna dekryptera data ökar, även om data som är krypterad med godkända algoritmer och nyckellängder ännu anses säkra. Det är huvudsakligen asymmetriska krypteringsmetoder som bedöms vara sårbara för attacker med kvantdatorer. En förutsättning för att en kvantdator ska kunna användas för att angripa algoritmer är att den också kan programmeras för sådana uppgifter. Symmetriska krypteringsmetoder anses idag inte vara sårbara på samma vis som asymmetriska krypteringsmetoder.

Det bedöms inte som troligt att konventionella datorer inom en rimlig framtid kommer att utvecklas till att bli kraftfulla nog att kunna angripa kryptering på samma sätt som en kvantdator anses kunna. Även om den risken är låg, är den dock inte obefintlig.

2.4 Risker och konsekvenser

Som tidigare nämnts går utvecklingen av kvantdatorer allt snabbare vilket påverkar hur man behöver hantera sin data. Fram till och med 2030 bedömer NIST i skrivande stund att motsvarande 112 bitars kryptering räcker, men nyckellängden behöver från och med 2031 öka till 128 bitar. Detta är baserat på vad vi känner till idag och kan komma att ändras om det sker tekniska framsteg med kvantdatorer som gör dem kraftfullare än vad de är idag. I bedömningen av hur långa kryptografiska nycklar som krävs behöver man ta hänsyn till vad det är för data som ska krypteras och för hur lång tid skyddet behöver vara effektivt.

Det finns två hot som är avgörande för byte av algoritmer för asymmetrisk kryptering samt ökning av nyckellängden för symmetrisk kryptering. I det första fallet handlar det om kvantdatorer som är tillräckligt kraftfulla, och kan implementera Shors eller Grovers algoritm, vilket möjliggör den forcering av kryptering som leder till att hotaktören kan läsa krypterat data. I det andra fallet handlar det om förmåga att påverka signerad data, samt att manipulera data utan att det upptäcks.

För det andra fallet är hotet idag det mest akuta och går under benämningen "harvest now, decrypt later", vilket innebär att data inhämtas idag och lagras i väntan på att det kan dekrypteras längre fram i tiden. Hotaktörer kan alltså redan nu, på olika sätt, inhämta krypterade informationstillgångar för att, när tillräcklig kapacitet i kvantdatorer finns, forcera krypteringen och ta del av den tidigare inhämtade och krypterade informationstillgången. Behöver du som verksamhetsutövare kryptera känsliga informationstillgångar, oavsett om informationen befinner sig i vila eller under transport, bör du vidta åtgärder redan nu. Algoritmen som idag primärt används för detta är AES. Observera att det inte räcker med att öka nyckellängden på nya nycklar. Även den information som redan är krypterad måste dekrypteras och sedan krypteras om med en ny nyckel som har en större nyckellängd. Att bara kryptera det krypterade datat igen kommer att ge en mer komplex hantering då det är två krypteringsnycklar som behöver hanteras vilket även komplicerar hanteringen för detta i applikationer som behöver läsa datat. Detta arbete innebär ytterligare en risk eftersom

informationstillgången behöver vara i klartext när den krypteras om samt att den tidigare krypterade informationen måste förstöras på ett säkert sätt.

I ett system där information, som egentligen inte är känslig, krypteras under transport är 128 bitars kryptering tillräcklig. Det kan till exempel handla om sensorer som skickar information till en central punkt för analys. Har du informationstillgångar som måste skyddas under en längre tid bör du överväga att använda längre kryptografiska nycklar för att säkerställa informationens säkerhet över tid.

Anledningen till att längre kryptografiska nycklar, än vad som anses nödvändigt, bör användas är för att skydda mot "harvest now, decrypt later". Detta är inte något potentiellt hot utan en metod som hotaktörer använder sig av redan idag. AES med 128 bitars nyckellängd anses vara komprometterad rent matematiskt, men i dagsläget finns det inte datorer med tillräckligt stor beräkningskapacitet för att dekryptering ska vara praktiskt genomförbart. Kryptering med 256 bitar istället för 128 bitar ger inte en linjär försämring av prestanda, utan ligger på ca 40%. Den allmänna uppfattningen idag är att 128 bitars kryptering kommer att vara tillräckligt säker under en längre tid, men som nämnts ovan kan denna ståndpunkt snabbt förändras.

Riskerna berör även andra typer av kryptografiska operationer. Till exempel kan en signatur som ska säkerställa ursprunget eller integriteten hos informationen, baserad på dagens algoritmer, framöver manipuleras så att en förändring av informationen inte upptäcks utan signaturen ser ut att vara giltig. Informationstillgången i det här fallet kan vara avtal med mer eller mindre lång livslängd där parterna över tid inte kan garantera dokumentets oavvislighet eller dess elektroniska underskrift. Signaturer används även i andra sammanhang, till exempel vid uppdateringar av applikationer och operativsystem som görs med exekverbara filer. En sådan signatur kan manipuleras för att därefter ges en signatur som ser ut att komma från en avsändare som du litar på, vilket gör att en hotaktör kan lägga till eller förändra kod utan att det upptäcks.

3. Tidsramar

Migreringen till kvantdatorsäkra algoritmer påverkar både statliga och privata aktörer världen över vilket gör att det finns olika tidslinjer för när olika steg på vägen till kvantdatorsäker kryptering ska vara genomförda. Utöver det finns även mer eller mindre strikta krav på vilken nivå av kryptering som ska implementeras för att uppfylla kraven, där ett av de striktare är Commercial National Security Algorithm Suite (CNSA) 2.0 utfärdat av USAs National Security Agency (NSA). Enskilda länder kan även de ha sina egna regler för migrering till kvantdatorsäkra algoritmer.

Vilken riktlinje och tidsram du bör följa beror dels på vilken marknad ni verkar inom dels hur skyddsvärd er information är.

I vilket fall bör du agera redan nu eftersom det dagligen sker intrång i it-miljöer i syfte att komma över krypterad information med förhoppningen att kunna dekryptera den så snart det finns tekniska förutsättningar att göra det.

3.1 NIST

National Institute of Standards and Technology (NIST) är det standardiseringsorgan som leder mycket av arbetet kring att ta fram standarder och riktlinjer och deras rekommendationer brukar vara det många följer.

NIST rekommenderar att efter år 2030 ska krypteringen vara minst motsvarande 128 bitar för RSA och ECC och efter år 2035 ska det inte tillåtas. Rent praktiskt innebär det att du bör använda åtminstone RSA nycklar på 3072 bitar och minst 256 bitar för ECC. Beträffande signaturer gäller minst SHA-224 fram till och med år 2030 och därefter bör SHA-256 eller bättre algoritmer användas.

3.2 CNSA 2.0

Ramverket Commercial National Security Algorithm Suite (CNSA) 2.0 är mycket striktare än NISTs rekommendationer, de algoritmer som tillåts ligger alla på högsta säkerhetsnivån för Federal Information Processing Standard (FIPS) 203, 204 och 205 och SHA-384 eller SHA-512 för signaturer. För signering av mjukvara och firmware är Leighton-Micali Hash-Based Signatures (LMS) och Extended Merkle Signature Scheme (XMSS) godkända samt SHA3-384 eller SHA3-512 för att beräkna hash-värden på firmware i hårdvara. I övrigt är allt annat otillåtet. Enligt CNSA 2.0 ska all utrustning vara migrerad från och med år 2031 och ny utrustning som tas in ska följa ramverket från och med 1 januari 2027.

3.3 EU

Inom EU finns ingen fastslagen tidslinje för EU-gemensam övergång till kvantdatorsäkra algoritmer. I april 2024 publicerade EU-kommissionen en rekommendation om en samordnad färdplan för genomförandet av övergången till postkvantkryptografi, (C(2024) 2393 final). Enligt avsnitt 2 i rekommendationen bör en samordnad färdplan finnas tillgänglig efter två år från offentliggörandet av rekommendationen, dvs efter april 2026.

4. Rättsliga krav på kryptering

Kryptering är en viktig säkerhetsåtgärd för att skydda konfidentialitet och riktighet för information såväl vid vila som i rörelse (överföring). Det har länge varit upp till varje verksamhetsutövare att själv avgöra om kryptering ska användas eller inte, samtidigt har det länge ansetts vara vedertagen branschpraxis att tillämpa kryptering, jämför till exempel ISO 27000 standarden. Mot bakgrund av att incidenter uppmärksammats har lagstiftaren sett behov av att tydligare reglera hur verksamhetsutövare ska tänka kring frågorna, jämför skäl 51, 98 och 104 i Europaparlamentets och Rådets direktiv (EU) 2022/2555 av den 14 december 2022 om åtgärder för en hög gemensam cybersäkerhetsnivå i hela unionen, om ändring av förordning (EU) nr 910/2014 och direktiv (EU) 2018/1972 och om upphävande av direktiv (EU) 2016/1148 (NIS 2-direktivet).

Beroende på vilken verksamhet som du bedriver kan regleringen avseende kryptering se olika ut. Trenden går mot ökad reglering med krav på verksamhetsutövarna att ha en genomtänkt krypteringsstrategi för att skydda sina informationstillgångar. De flesta regler som ställer krav på kryptering har formulerats på en generell nivå, det vill säga reglerna är inte detaljerade eller ställer krav på användning av viss teknik för vissa användningsområden. I allmänhet kan sägas att du som verksamhetsutövare ska tillämpa använda den senaste tekniken med beaktande av kostnaden. När det inte längre är osannolikt att det finns kvantdatorer som kan knäcka krypteringsalgoritmerna som du använder i din verksamhet måste den aktuella riskhanteringsåtgärden (krypteringen) förstärkas eller kompletteras med andra säkerhetsåtgärder för att uppfylla de regulatoriska kraven.

Regelverket bygger i allmänhet på att du som verksamhetsutövare ska implementera proportionella skyddsåtgärder med hänsyn till den senaste tekniken (State-of-the-Art) och genomförandekostnaderna, jämför art 21 1 andra stycket NIS 2-direktivet). Vad som utgör den senaste tekniken är således många gånger avgörande för vilka regulatoriska krav som gäller för verksamheten när det kommer till kryptering. Vad som utgör den senaste tekniken är föränderligt och därför något som är svårt att tillämpa inte bara för verksamhetsutövare men också för domstolarna. Klart är i varje fall att användning av kryptoalgoritmer som idag anses vara knäckta eller osäkra ur ett regulatoriskt perspektiv inte betraktas som tillräcklig säkerhetsåtgärd.

4.1 Gällande regler om kryptografiska åtgärder

4.1.1 Privat och offentlig sektor

4.1.1.1 Alla verksamheter som behandlar personuppgifter

Alla verksamheter, oavsett om de hör till offentlig eller privat sektor behöver förhålla sig till de krav på säkerhetsåtgärder som gäller enligt Europaparlamentets och rådets förordning (EU) 2016/679 av den 27 april 2016 om skydd för fysiska personer med avseende på behandling av personuppgifter och om det fria flödet av sådana uppgifter och om upphävande av direktiv 95/46/EG (dataskyddsförordningen).

Dataskyddsförordningen innehåller dels så kallade "skäl" som ska hjälpa till vid tolkningen av dataskyddsförordningens bestämmelser, dels "artiklar" som innehåller de bindande regler som gäller för alla som är skyldiga att tillämpa dataskyddsförordningen.

Rätten till skydd av personuppgifter är inte en absolut rättighet; den måste förstås från sin uppgift i samhället och vägas mot andra grundläggande rättigheter som erkänns av Europeiska unionens stadga om de grundläggande rättigheterna i enlighet med proportionalitetsprincipen, (skäl 4 i dataskyddsförordningen).

För att upprätthålla säkerheten och förhindra personuppgiftsbehandling som bryter mot dataskyddsförordningen bör personuppgiftsansvariga eller personuppgiftsbiträden utvärdera riskerna med behandlingen och vidta åtgärder, såsom kryptering, för att minska dem. Åtgärderna bör säkerställa en lämplig säkerhetsnivå, inbegripet konfidentialitet, med beaktande av den senaste utvecklingen och genomförandekostnader i förhållande till riskerna och vilken typ av personuppgifter som ska skyddas, (skäl 83 i dataskyddsförordningen).

Personuppgiftsbehandling är endast laglig om den uppfyller ett eller flera av sex villkor:

1. Den vars personuppgifter som behandlas har lämnat sitt samtycke för ett eller flera specifika ändamål.
2. Behandlingen är nödvändig för att fullgöra ett avtal med den vars personuppgifter behandlas.
3. Behandlingen är nödvändig på grund av en rättslig förpliktelse för den personuppgiftsansvarige.
4. Behandlingen är nödvändig för att skydda intressen av grundläggande betydelse för den vars personuppgifter behandlas eller för annan fysisk person.
5. Behandlingen är nödvändig för att utföra en uppgift av allmänt intresse eller som ett led i en personuppgiftsansvarigs myndighetsutövning.
6. Behandlingen är nödvändig för ändamål som rör den personuppgiftsansvariges eller tredje parts berättigade intressen - om inte den registrerades intressen eller grundläggande rättigheter och friheter väger tyngre och kräver skydd av personuppgifter, särskilt när personuppgiftsbehandlingen rör barn, (artikel 6. 1 a-f dataskyddsförordningen).

Alla som behandlar personuppgifter är - med beaktande av den senaste utvecklingen, genomförandekostnaderna och behandlingens art, omfattning, sammanhang och ändamål samt riskerna - skyldiga att säkerställa en lämplig säkerhetsnivå i förhållande till risken, inbegripet när det är lämpligt pseudonymiseringar och kryptering av personuppgifter, (artikel 32 1. a dataskyddsförordningen).

Integritetsskyddsmyndigheten (IMY) har på sin webbplats beskrivit hur personuppgiftsansvariga ska arbeta med kryptering och vad som förväntas av en verksamhet som tillämpar kryptering för att begränsa riskerna med personuppgiftsbehandlingen:

- Analysera behovet.

  Analysera behovet av kryptering, det vill säga ta reda på vilken information som i olika situationer kan behöva krypteras samt vilken typ av krypteringsskydd som är lämpligt, till exempel vid användning av molntjänster för lagring av personuppgifter.

- Dokumentera analysen.

  Resultatet av analysen ska dokumenteras om det gäller behandling av skyddsvärda personuppgifter, till exempel i form av en policy.

- Ta fram interna regler och utbilda.

  Användarna hos verksamhetsutövaren ska ges tydliga riktlinjer eller instruktioner samt få utbildning om när, var, hur och vilken kryptering som ska användas.

- Använd tillräckligt säker kryptering.

  Den kryptering som används ska vara tillräckligt säker. Ett sätt att försäkra sig om detta är att bara använda allmänt erkända starka krypteringsalgoritmer och krypteringsnycklar av tillräcklig längd.

- Skydda krypteringsnycklarna.

  Det gäller också att säkerställa att krypteringsnycklarna lagras och hanteras på ett säkert sätt och därmed skyddas mot obehöriga. Om lagringen till exempel sker i en molntjänst i tredjeland som inte kan erbjuda likvärdig skyddsnivå ska krypteringsnycklarna endast vara tillgängliga för den personuppgiftsansvarige. Detsamma gäller i situationer där det finns anledning att skydda personuppgifterna i förhållande till ett personuppgiftsbiträde.

- Säkerställ kryptering hela vägen vid överföring.

  Om kryptering används för att skydda känsliga personuppgifter vid överföring ska det säkerställas att kryptering sker hela vägen från avsändaren till mottagaren.

- Kryptera innan obehöriga kan ta del av uppgifterna.

  Vid lagring av personuppgifter ska kryptering ske innan obehöriga har möjlighet att ta del av dem. Detta gäller till exempel vid användning av molntjänster i tredjeland som inte kan garantera en likvärdig skyddsnivå som kan garanteras inom EU/EES.

Kryptering som åtgärd när man behandlar personuppgifter för nya ändamål

Om en verksamhetsutövare som är ansvarig för en viss verksamhet som behandlar personuppgifter vill använda personuppgifterna för andra ändamål än de som personuppgifterna ursprungligen inhämtades för så är det tillåtet endast om ändamålen med den nya behandlingen är förenliga med de ursprungligen angivna ändamålen vid inhämtningen av personuppgifterna. Vid bedömningen av om de nya ändamålen är förenliga med de ursprungliga ska den som ansvarar för personuppgiftshantering bland annat beakta förekomsten av lämpliga skyddsåtgärder, vilket kan inbegripa kryptering eller pseudonymisering, (artikel 6 4. e dataskyddsförordningen).

Kryptering vid behandling av personuppgifter

I november 2013 publicerade Europiska unionens cybersäkerhetsbyrå (Enisa) en rapport om rekommenderade kryptografiska åtgärder för att säkerställa skyddet för personuppgifter, Recommended cryptographic measures – Securing personal data. Av rapporten framgår bland annat att myndigheter och leverantörer bör rekommendera och implementera säkerhetsåtgärder för att skydda personuppgifter och bör förlita sig på de främsta lösningarna och konfigurationerna. De kan i detta arbete använda Enisas referensrapport om algoritmer, nyckelstorlek och parametrar, Algorithms, key size and parameters report – 2014. Enisa hade ambitionen att uppdatera denna rapport varje år. Senaste utgåvan av rapporten är från 2014. Myndigheter och leverantörer bör referera till den senaste versionen av rapporten i sina rekommendationer. Noterbart i detta sammanhang är att Enisa redan 2014 rekommenderade att dåtidens system kan behöva designas så att en övergång till kvantdatorsäkra system blir smidig, (s.17). Det framgår att om utvecklingen av kvantdatorer med förmåga att knäcka dagens godkända kryptoalgoritmer är nära förestående måste alla rekommendationer allvarligt övervägas på nytt, särskilt alla algoritmer som baseras på publika nycklar i rekommendationen bör betraktas som osäkra, (s. 37). I januari 2019 publicerade MSB en vägledning för grundläggande kryptering och i maj 2023 publicerade IT Security Association Germany (TeleTrusT) i samarbete med Enisa Guideline "State of the art", se allmän vägledning nedan.

4.1.1.2 NIS-aktörer

Vilka leverantörer som omfattas av lagstiftningen har förtydligats i Myndigheten för samhällsskydd och beredskaps föreskrifter (MSBFS 2024:4) om anmälan och identifiering av leverantörer av samhällsviktiga tjänster. I december 2022 beslutade Europaparlamentet och rådet om ett nytt direktiv om åtgärder för en hög gemensam cybersäkerhetsnivå i hela unionen (NIS 2-direktivet). Samtidigt upphävdes NIS-direktivet som legat till grund för NIS-lagen. Det nya direktivet (NIS 2-direktivet) utvidgar tillämpningsområdet till fler sektorer och aktörer. Det innebär att den lagstiftning och de föreskrifter som nu gäller kommer att ersättas inom en inte alltför avlägsen framtid. Läs mer om kommande lagstiftning och krav i avsnittet nedan.

NIS-lagen ställer övergripande krav på leverantörer av samhällsviktiga tjänster. Såsom att leverantörerna ska bedriva systematiskt och riskbaserat informationssäkerhetsarbete, göra riskanalyser och vidta ändamålsenliga och proportionella tekniska och organisatoriska åtgärder för att hantera risker som hotar säkerheten i nätverk och informationssystem som de använder för att tillhandhålla samhällsviktiga tjänster. Åtgärderna ska säkerställa en nivå på säkerheten i nätverken och informationssystemen som är lämplig i förhållande till risken, (11-13 §§ lagen (2018:1174) om informationssäkerhet för samhällsviktiga och digitala tjänster).

Av förordningen (2018:1175) om informationssäkerhet för samhällsviktiga och digitala tjänster framgår att tillsynsmyndigheterna får meddela föreskrifter inom sina respektive sektorer. Vissa NIS-sektorer kan beröra såväl offentliga som privata verksamheter såsom hälso- och sjukvård och dricksvatten medan andra är huvudsakligen privata. För de NIS-sektorer som är huvudsakligen privata se avsnittet nedan.

Energisektorn

För samhällsviktiga aktörer som är verksamma inom energisektorn och som omfattas av NIS-lagstiftningen har Statens energimyndighet meddelat kompletterande föreskrifter, Statens energimyndighets föreskrifter och allmänna råd (STEMFS 2021:3) om riskanalys och säkerhetsåtgärder för nätverk och informationssystem inom energisektorn. Dessa föreskrifter reglerar dock inte något specifikt rörande kryptering.

Transportsektorn

För samhällsviktiga aktörer som är verksamma inom transportsektorn och som omfattas av NIS-lagstiftningen gäller att leverantören ska ta fram, fastställa och tillämpa dokumenterade interna regler och arbetssätt för att hantera behovet av kryptering, i syfte att skydda information mot obehörig åtkomst och obehörig förändring vid överföring och lagring, 19 § Transportstyrelsens föreskrifter och allmänna råd (TSFS 2022:14) om säkerhetsåtgärder för leverantörer av samhällsviktiga tjänster inom transportsektorn.

Bank- och finanssektorn

Inom bank- och finanssektorn gäller sedan den 1 januari 2025 Europaparlamentets och rådets förordning (EU) 2022/2554 av den 14 december 2022 om digital operativ motståndskraft för finanssektorn (Dora-förordningen).

Enligt Dora-förordningen ska finansiella entiteter införa lämpliga verktyg, riktlinjer och förfaranden för IKT-säkerhet. Finansiella entiteter ska utforma och genomföra IKT-relaterade säkerhetsstrategier, förfaranden, protokoll och verktyg som syftar till att säkerställa IKT-systemens motståndskraft, kontinuitet och tillgänglighet. I synnerhet för de system som stöder kritiska eller viktiga funktioner, och upprätthålla höga standarder för tillgänglighet, äkthet, integritet och konfidentialitet avseende data, oberoende av om de är i vila, i bruk eller under överföring, artikel 9. 1 och 2 Dora-förordningen.

Finansiella entiteter ska bland annat genomföra strategier och protokoll för starka äkthetsmekanismer, baserade på relevanta standarder och särskilda kontrollsystem, samt skyddsåtgärder för kryptografiska nycklar där data krypteras baserat på resultat från godkända processer för klassificering och IKT-riskbedömning, artikel 9.3 d) Dora-förordningen.

Enligt Dora-förordningen ska de europeiska tillsynsmyndigheterna genom en gemensam kommitté och i samråd med Europeiska unionens cybersäkerhetsbyrå (Enisa), utarbeta gemensamma förslag till tekniska standarder för tillsyn bland annat i syfte att möjliggöra lämpliga skyddsåtgärder mot intrång och missbruk av uppgifter, bevara uppgifternas tillgänglighet, äkthet, integritet och konfidentialitet, inbegripet krypteringsmetoder, artikel 15 a) Dora-förordningen. Tillsynsmyndigheterna (Finansinspektionen) har också befogenhet att utfärda rekommendationer om bland annat kryptering, art 35 1. d) i) Dora-förordningen. Några sådana rekommendationer har dock ännu inte utfärdats.

Sektorn leverans och distribution av dricksvatten

För samhällsviktiga aktörer som är verksamma inom sektorn leverans och distribution av dricksvatten och som omfattas av NIS-lagstiftningen har Livsmedelsverket meddelat kompletterande föreskrifter. Livsmedelsverkets föreskrifter (LIVSFS 2022:2) om informationssäkerhetsåtgärder för samhällsviktiga tjänster inom sektorn leverans och distribution av dricksvatten. Dessa föreskrifter reglerar dock inte något specifikt rörande kryptering.

Hälso- och sjukvårdssektorn

Enligt 4 kap. 6 § patientdatalagen (2008:355) är regioner som tar emot krypterade uppgifter från E-hälsomyndigheten enligt 6 kap. 3 § lagen (2018:12112) om nationell läkemedelslista skyldiga att kryptera uppgifter om en patients identitet så att dessa uppgifter skyddas vid behandlingen.

Socialstyrelsen får, efter att ha gett Integritetsskyddsmyndigheten tillfälle att yttra sig, bland annat meddela föreskrifter om verkställigheten av de krav på säkerhetsåtgärder för vissa delar av patientdatalagen, 2-3 §§ patientdataförordningen (2008:360). Av 3 kap. 1 och 2 §§ Socialstyrelsens föreskrifter och allmänna råd (HSLF-FS 2016:40) om journalföring och behandling av personuppgifter i hälso- och sjukvården framgår att varje vårdgivare ansvarar för att ha ett ledningssystem som säkerställer att verksamheten uppfyller kraven i föreskrifterna. Genom ledningssystemet ska vårdgivaren säkerställa att:

1. Dokumenterade personuppgifter hos vårdgivaren är åtkomliga och användbara för den som är behörig (tillgänglighet).
2. Personuppgifterna är oförvanskade (riktighet).
3. Obehöriga inte ska kunna ta del av personuppgifterna (konfidentialitet).
4. Åtgärder kan härledas till en användare (spårbarhet) i informationssystem som är helt eller delvis automatiserade.

Av 3 kap. 15 och 19 §§ HSLF-FS 2016:40 framgår att om vårdgivaren använder öppna nät vid behandling av personuppgifter ska denne ansvara för att överföring av uppgifterna görs på ett sådant sätt att inte obehöriga kan ta del av dem. Elektronisk åtkomst eller direktåtkomst till uppgifterna ska föregås av stark autentisering samt att vårdgivare som tillåter flyttbart medium för lagring av personuppgifter ska säkerställa att obehöriga inte kan ta del av dem och att uppgifterna inte går förlorade.

Socialstyrelsen har därtill publicerat en handbok för tillämpningen av Socialstyrelsens föreskrifter och allmänna råd (HSLF-FS 2016:40) om journalföring och behandling av personuppgifter i hälso- och sjukvården. Av handboken framgår bland annat att öppna nät kan beskrivas som datornätverk som en enskild användare har tillgång till, exempelvis internet. Internet gör det möjligt att enkelt och effektivt kommunicera text, ljud och bild. Om inte vårdgivaren vidtar särskilda skyddsåtgärder kommer dock informationen att överföras oskyddad. Om en vårdgivare gör uppgifter om patienter tillgängliga över öppna nät, exempelvis för att hälso- och sjukvårdspersonalen ska kunna utföra arbetsuppgifter på distans, måste det göras på ett sådant sätt att ingen obehörig kan nå uppgifterna. I praktiken innebär det bland annat att uppgifter om patienter måste överföras genom en krypterad förbindelse eller genom att kryptera uppgifterna. Teknikutvecklingen medför att krypteringsmetoderna hela tiden kan behöva förbättras för att minimera risken för obehörig åtkomst, (s. 25-26). Där det är tillämpbart kan vårdgivaren kräva kryptering för flyttbart medium, (s. 29).

4.1.2 Privat sektor

4.1.2.1 NIS och NIS 2-aktörer

Sektorn digital infrastruktur

Vissa av aktörerna inom sektorn digital infrastruktur omfattas av EU-kommissionens genomförandeförordning om fastställande av regler för tillämpningen av NIS 2-direktivet, C(2024) 7151 final (genomförandeförordningen), som beslutades den 17 oktober 2024. Genomförandeförordningen började gälla den 7 november 2024 och är direkt tillämplig för de aktörer som omfattas. Det vill säga:

- Registreringsenheter för toppdomäner.
- Tillhandahållare av betrodda tjänster.
- Leverantörer av:
    - molntjänster
    - datacentraltjänster
    - nätverk för leverans av innehåll
    - utlokaliserade driftstjänster
    - utlokaliserade säkerhetstjänster
    - marknadsplatser online
    - sökmotorer
    - plattformar för sociala nätverkstjänster

Enligt artikel 2 i genomförandeförordningen ska de berörda entiteterna genomföra och tillämpa de tekniska och metodologiska specifikationerna för riskhanteringsåtgärder för cybersäkerhet som fastställs i bilagan genomförandeförordningen. De ska ta hänsyn till sin riskexponeringsgrad, sin storlek, sannolikheten för att incidenter ska inträffa och incidenternas allvarlighetsgrad, inklusive de samhälleliga och ekonomiska konsekvenserna, när de uppfyller de tekniska och metodologiska specifikationer för riskhanteringsåtgärder för cybersäkerhet. Om det i bilagan anges att en riskhanteringsåtgärd ska tillämpas ”när så är lämpligt”, ”om tillämpligt” eller ”i den mån det är genomförbart” och verksamhetsutövaren (entiteten) inte anser det vara lämpligt, tillämplig eller genomförbart ska skälen för detta dokumenteras.

Av avsnitt 9 i bilagan till genomförandeförordningen framgår bland annat att de berörda entiteterna ska fastställa, införa och tillämpa en strategi och förfaranden för kryptografi, för att säkerställa en ändamålsenlig och effektiv användning av kryptografi för att skydda konfidentialiteten, autenticiteten och integriteten för data i enlighet med de berörda entiteternas klassificering av tillgångar och resultaten av den riskbedömning som entiteten är skyldig att utföra. Det framgår vidare att den strategi och de förfaranden för kryptografi som ska upprättas ska innehålla följande:

1. Typ, styrka och kvalitet när det gäller de kryptografiska åtgärder som krävs för att skydda verksamhetsutövarens tillgångar, inklusive data i vila och data vid transitering, i enlighet med den berörda verksamhetsutövarens klassificering av sina tillgångar.
2. Baserat på p 1 ovan, de protokoll eller protokollfamiljer som ska antas, liksom kryptografiska algoritmer, krypteringsstyrka, kryptografiska lösningar och användningspraxis som ska godkännas och krävas för användning hos verksamhetsutövaren, med kryptoföljsamhet när så är lämpligt.
3. Hantering av nycklar, inbegripet när så är lämpligt, metoder för följande:

    a) Generering av olika nycklar för kryptografiska system och applikationer.
    b) Utfärdande och erhållande av certifikat för öppen nyckel.
    c) Distribution av nycklar till avsedda entiteter, inklusive hur nycklarna ska aktiveras när de mottagits.
    d) Lagring av nycklar, inklusive hur behöriga användare får tillgång till nycklar.
    e) Ändring eller uppdatering av nycklar, inklusive regler för när och hur nycklar ska ändras.
    f) Hantering av nycklar som komprometterats.
    g) Upphävande av nycklar, inklusive hur man drar in eller avaktiverar nycklar.
    h) Återställande av nycklar som förlorats eller korrumperats.
    i) Säkerhetskopiering eller arkivering av nycklar.
    j) Förstörelse av nycklar.
    k) Loggning och revision av aktiviteter förbundna med nyckelhantering.
    l) Fastställande av aktiverings- och avaktiveringsdatum för nycklar för att säkerställa att nycklarna endast kan användas under den angivna tidsperioden i enlighet med verksamhetens regler om nyckelhantering.

Verksamhetsutövaren ska även, när så är lämpligt, uppdatera sina strategier och förfaranden med planerade intervall, med beaktande av den senaste tekniken när det gäller kryptografi.

Samtidigt gäller även för aktörer inom sektorn digital infrastruktur och som omfattas av NIS-lagstiftningen att leverantören ska eliminera eller reducera identifierande risker och bland annat vidta åtgärder för att upprätthålla ett effektivt skydd av säkerheten i nätverk och informationssystem mot brister i fysiskt och logiskt skydd. Åtgärderna ska ge skydd mot logiska intrång, logiska överbelastningsattacker och andra identifierade logiska hot, 6 och 8 §§ Post- och telestyrelsens föreskrifter och allmänna råd (PTSFS 2021:3) om säkerhetsåtgärder för samhällsviktiga tjänster inom sektorn digital infrastruktur. Av de allmänna råden i anslutning till bestämmelsen framgår bland annat att åtgärderna bör omfatta logiska hot i den egna verksamheten, såsom hot som leder till obehörig åtkomst till DNS-data, autentiseringsuppgifter, tilldelade behörigheter, loggningsinformation och privata krypteringsnycklar i det fall asymmetrisk kryptering används.

Leverantören ska även säkerställa spårbarhet genom att bland annat logga all läsning av sådana uppgifter som är konfidentiella, 14 § PTSFS 2021:3. Med uppgifter som är konfidentiella avses exempelvis autentiseringsuppgifter och privata krypteringsnycklar i det fall asymmetrisk kryptering används. Denna reglering gäller fullt ut för de aktörer som omfattas av PTS föreskrifter men som inte omfattas av genomförandeförordningen, såsom andra registreringsenheter än sådana som registrerar toppdomäner. För de som omfattas av genomförandeförordningen föreligger dock en viss dubbelreglering eftersom PTS ännu inte justerat sina föreskrifter. PTS har lämnat sin syn på tillämpningen på PTS webbplats "Vad gäller innan NIS 2-direktivet har genomförts i svensk rätt?".

4.1.2.2 Aktörer inom sektorn elektronisk kommunikation

Den som tillhandahåller ett allmänt elektroniskt kommunikationsnät eller en allmänt tillgänglig elektronisk kommunikationstjänst ska vidta ändamålsenliga och proportionella tekniska och organisatoriska åtgärder för att på ett lämpligt sätt hantera risker som hotar säkerheten i nät och tjänster, (8 kap 1 § lagen (2022:482) om elektronisk kommunikation. Åtgärderna ska säkerställa en nivå på säkerheten i nät och tjänster som är lämplig i förhållande till riskerna. Åtgärder ska vidtas särskilt för att förebygga och minimera säkerhetsincidenters påverkan på användare och på andra nät och tjänster. Post- och telestyrelsen (PTS) har meddelat föreskrifter i anslutning till bestämmelsen av vilka det bland annat framgår att behandlade uppgifter som överförs via internet ska skyddas genom kryptering. Uppgifterna behöver dock inte skyddas genom kryptering om det med hänsyn till uppgifternas art och sammanhang är osannolikt att överföring utan kryptering kan leda till en säkerhets- eller integritetsincident, (10 kap. 1 § Post- och telestyrelsens föreskrifter och allmänna råd (PTSFS 2022:11) om säkerhet i nät och tjänster). Kryptering ska ske med en allmänt erkänd krypteringsmetod med tillräcklig nyckellängd. Krypteringsnycklar ska hanteras på ett säkert sätt, (10 kap. 4 § PTSFS 2022:11). Vad PTS menar med allmänt erkänd krypteringsmetod med tillräcklig nyckellängd framgår inte men vägledning kan hittas i det som betraktas som den senaste tekniken och kryptoalgoritmer som allmänt anses osäkra kan inte tillämpas för att uppfylla regelverkets krav.

4.1.3 Offentlig sektor

Offentlig upphandling

I upphandlingssammanhang är myndigheterna skyldiga att tillhandahålla information om nödvändiga specifikationer för elektronisk inlämning av anbudsansökningar och anbud, inbegripet kryptering, för alla berörda parter, (12 kap. 6 § lagen (2016:1145) om offentlig upphandling, 10 kap. 3 § lagen (2011:1029) om upphandling på försvars- och säkerhetsområdet, 10 kap. 6 § lagen (2016:1147) om upphandling av koncessioner samt 12 kap. 6 § lagen (2016:1146) om upphandling inom försörjningssektorerna.

Offentlighet- och sekretess

Sekretess innebär ett förbud att röja en uppgift, vare sig det sker muntligen, genom utlämnande av en allmän handling eller på annat sätt, 3 kap. 1 § offentlighets- och sekretesslagen (2009:400), (OSL). Av 20 kap. 3 § brottsbalken framgår bland annat att den som röjer en uppgift som han eller hon är skyldig att hemlighålla enligt lag eller annan författning, döms, för brott mot tystnadsplikt till böter eller fängelse i högst två år. Den aktör som behandlar sekretessbelagda uppgifter är således skyldig att vidta sådana skyddsåtgärder att uppgifterna inte röjs. OSL ställer dock inga regulatoriska krav på kryptering för skydd av sekretessbelagda uppgifter eller i övrigt vilka säkerhetsåtgärder som en verksamhetsutövare ska vidta. Det är upp till varje verksamhetsutövare själv att avgöra vilka åtgärder som är tillräckliga för att skydda sekretessbelagda uppgifter men klart är att fungerande kryptering kan vara en sådan åtgärd.

Enligt 18 kap. 9 § OSL gäller sekretess för uppgift som lämna eller kan bidra till upplysning om chiffer, kod eller liknande metod, om det kan antas att syftet med metoden motverkas om uppgiften röjs och metoden har till syfte att underlätta befordran eller användning i allmän verksamhet av uppgifter utan att föreskriven sekretess åsidosätt eller göra det möjligt att kontrollera om data i elektronisk form har förvanskats.

Uppgifter om kryptering, krypteringsmetoder, krypteringsnycklar med mera kan därigenom omfattas av sekretess hos de myndigheter som innehar sådana uppgifter.

Statliga myndigheter

För alla statliga myndigheter gäller förordning (2022:524) om statliga myndigheters beredskap. Enligt denna förordning ansvarar varje myndighet för att egna informationshanteringssystem uppfyller sådana grundläggande och särskilda säkerhetskrav att myndighetens verksamhet kan utföras på ett tillfredsställande sätt. Myndigheten för samhällsskydd och beredskap (MSB) som i januari 2026 byter namn till Myndigheten för civilt försvar har meddelat föreskrifter i anslutning till denna bestämmelse.

Av 4 kap. 7-9 §§ Myndigheten för samhällsskydd och beredskaps föreskrifter om säkerhetsåtgärder i informationssystem för statliga myndigheter (MSBFS 2020:7) framgår bland annat att myndigheter ska identifiera och hantera behovet av kryptering för att skydda information mot obehörig åtkomst och obehörig förändring vid överföring och lagring och använda Domain Name System Security Extensions (DNSSEC) för samtliga domännamn som myndigheten registrerat i domännamnssystemet (DNS). Myndigheten ska även upprätta interna regler för hantering av krypteringsnycklar, godkännande och förvaltning av krypteringslösningar och hur krypteringsalgoritmer, krypteringsprotokoll och nyckellängder ska väljas.

Av MSBs allmänna råd i anslutning till detta framgår bland annat att kryptering bör användas för att skydda säkerhetsloggar och autentiseringsuppgifter mot obehörig åtkomst och obehörig förändring. Kryptering bör också användas för att skydda annan information i behov av utökat skydd mot obehörig åtkomst och obehörig förändring vid överföring till informationssystem utanför myndighetens kontroll.

Försäkringskassan ska se till att personnummer, samordningsnummer, organisationsnummer och tandvårdsmottagningsnummer är krypterade innan de lämnas ut till Tandvårds- och läkemedelsförmånsverket enligt 19 a § förordningen (2008:193) om statligt tandvårdsstöd.

Av 6 kap. 3 § lagen (2018:12112) om nationell läkemedelslista framgår bland annat att E-hälsomyndigheten ska lämna ut uppgifter till regionerna om expedieringar av föreskrivna läkemedel och andra varor som omfattas av lagen (2002:160) om läkemedelsförmåner m.m. Uppgifterna om patientens identitet ska i dessa fall vara krypterade på ett sådant sätt att dennes identitet skyddas. Integritetsskyddsmyndigheten (IMY) har mandat att meddela föreskrifter om sådan kryptering men några sådana är ännu inte beslutade eller planerade.

Av 14 § tredje stycket lagen (1996:1156) om receptregister framgår att uppgifter om patientens identitet ska vara krypterade.

Den krypteringsmetod som ska användas vid utlämnande från E-hälsomyndigheten ska vara s.k. envägskryptering. Krypteringen med denna krypteringsmetod är icke-reversibel, dvs. det går inte att tillämpa algoritmen på den unika koden och därmed erhålla det krypterade personnumret i läsbar form. Används samma algoritm över tid bibehålls en möjlighet för uppföljningssystemet att följa enskilda individer, dock endast i form av en unik kod. Används samma algoritm i regionerna (dåvarande landstingen) är det möjligt att koppla ihop uppgifter om en och samma person från olika källor genom att samma metod för kryptering och algoritm används för samma uppgifter. Genom detta förfarande uppnås alltså inte en total avidentifiering. Integritetsskyddsmyndigheten (dåvarande Datainspektionen) varnade för en övertro på det skydd som uppnås genom användandet av icke-reversibla krypteringsmetoder och påtalade betydelsen av att krypteringen ska bestå. Vilket också fått genomslag i lagstiftningen, (Regeringens proposition för ökad kvalitet vid läkemedelsförskrivning. prop. 2009/10:138, s. 32 f.)

Allmän vägledning

I januari 2019 publicerade Myndigheten för samhällsskydd och beredskap en vägledning för grundläggande kryptering. Vägledningen är en sammanställning av rekommendationer för att säkerställa ett tillräckligt skydd av information genom kryptering från Sveriges Certifieringsorgan för IT-säkerhet (CSEC), Senior Officials Group - Information Security (SOG-IS), Europeiska unionens cybersäkerhetsbyrå (Enisa) och National Institutes of Standards and Technology (NIST). Vägledningen beskriver säkerhetsåtgärder för att införa och upprätthålla säkra kryptolösningar. Rekommendationerna i vägledningen är inte tvingande. IT Security Association Germany (TeleTrusT) publicerade i maj 2023 en vägledning om vad som är bästa möjliga teknik inom it-säkerhet, Guideline "State of the Art". TeleTrusTs vägledning beskriver vad som i maj 2023 anses vara godtagbara metoder och algoritmer för olika användningsområden, s. 24-34).

4.2 Kommande regler

NIS 2-direktivet skulle enligt EU:s beslut ha införlivats i nationell lagstiftning senast den 18 oktober 2024. I Sverige har det i skrivande stund (mars 2025) ännu inte lämnats någon remiss till lagrådet eller proposition till riksdagen för beslut om den nya lagen. I mars 2024 lämnade utredningen om genomförande av NIS2- och CER-direktiven över sitt delbetänkande till regeringen, Nya regler om cybersäkerhet, SOU 2024:18. Utredningen föreslår en ny lag om cybersäkerhet som ska ersätta lagen (2018:1174) om informationssäkerhet för samhällsviktiga och digitala tjänster. NIS 2-direktivet och därigenom även lagen kommer att innebära en ökning av de sektorer och entiteter (verksamhetsutövare) som ska tillämpa det kommande regelverket.

Såsom förslaget ser ut ska verksamhetsutövare vidta tekniska, driftsrelaterade och organisatoriska riskhanteringsåtgärder för att skydda nätverks- och informationssystem och systemens fysiska miljö mot incidenter. Åtgärderna ska utgå från ett allriskperspektiv och en riskanalys och vara proportionella i förhållande till risken. De ska utvärderas och bland annat innefatta strategier och förfaranden för användning av kryptografi, 3 kap. 1 § 5 p. förslag till lag om cybersäkerhet, s. 41 i SOU 2024:18. Vad detta i praktiken innebär förtydligas inte av utredningen utan överförs direkt från direktivet till svensk lagstiftning och kommer troligen att regleras mer i detalj i de myndighetsföreskrifter som tillsynsmyndigheterna kommer att utfärda efter att den nationella lagstiftningen har trätt i kraft. Under tiden kan det dock vara klokt att förbereda sig genom att i vart fall arbeta i enlighet med de krav och förslag som kommissionen beslutat i genomförandeförordningen, se avsnittet om sektorn digital infrastruktur ovan.

5. Förutsättningar

Det finns ett antal faktorer som påverkar möjligheten till migrering till kvantdatorsäkra algoritmer och som din verksamhet bör vara medveten om vid planeringen av er migrering. Dels hur status ser ut kring framtagande och fastställande av nya algoritmer och tillhörande standarder och dels i vilken takt utvecklare och leverantörer av hård- och mjukvara anpassar sina produkter därefter.

5.1 Befintliga och nya algoritmer för kryptering och signering

Inom området kryptografiska algoritmer är utveckling och övergång till nyare algoritmer generellt en relativt långsam process. Det beror framför allt på två faktorer. Den första är att det historiskt har krävts ganska stora tekniska framsteg för att utveckla datorer med tillräcklig kapacitet för att kunna "knäcka" en algoritm. Den andra är att det krävs mycket arbete för att dels utveckla nya algoritmer, dels implementera nya algoritmer i olika typer av applikationer, kryptografiska bibliotek och protokoll.

5.1.1 Dagens algoritmer

De algoritmer som används idag är väl inarbetade och testade och de har modifierats genom åren när tekniska framsteg har gjorts eller när svagheter har upptäckts. De varianter som används idag erbjuder ett gott skydd för närvarande.

Nedan beskrivs de idag vanligast förekommande algoritmerna.

Algoritm	Beskrivning
RSA	RSA är en asymmetrisk krypteringsalgoritm som bygger på svårigheten med att med faktorisera stora heltal som är produkten av två stora primtal.. Vid signering används den privata nyckel för att signera data och man kan verifiera den signaturen genom den publika nyckeln. Vid kryptering används istället den publika nyckeln för att kryptera data och det kan sedan enbart dekrypteras av den som har den privata nyckeln.
ECC	Elliptic Curve Cryptography (ECC) är en asymmetrisk kryptografi som erbjuder samma säkerhet som RSA men med kortare nyckellängder, vilket gör den mer effektiv för mobila enheter och IoT samt elektroniska underskrifter.
SHA2	En familj av kryptografiska hash-funktioner som används för att skapa unika, fasta hash-värden från data. SHA2 används ofta för lösenordslagring och digitala signaturer.
AES	Advanced Encryption Standard (AES) är en symmetrisk blockkrypteringsalgoritm som används för att skydda data. Den är känd för sin hastighet och säkerhet och används i allt från filkryptering till VPN. AES är en de facto-standard för att kryptera data och då det är en symmetrisk algoritm måste båda parter känna till nyckeln för att kunna kryptera och dekryptera data. Eftersom båda parter måste känna till samma nyckel är utmaningen att säkert distribuera nyckeln till de parter som behöver den. Traditionellt används RSA för att göra detta. Algoritmen är en blockalgoritm och hanterar data i en bestämd blocklängd om 128 bitar. Krypteringsnyckeln är antingen i längden 128, 192 eller 256 bitar, trots de förutsättningarna fungerar AES alldeles utmärkt att använda även om det är mindre data att kryptera än blocklängden.

5.1.2 Utmaningen från kvantdatorer

Kvantdatorer utgör en utmaning för vår användning av kryptografi eftersom de algoritmer vi förlitar oss på för asymmetrisk kryptering kan bli sårbara när kvantdatorer blir tillräckligt kraftfulla. Anledningen att kvantdatorer är så bra på att räkna ut kryptografiska hemligheter är inte att de är mycket snabbare än en vanlig dator utan att de algoritmiskt kan minska komplexiteten i det problem som en krypteringsalgoritm utgör.

RSA och Shors algoritm

RSA bygger på faktorisering av stora heltal. Den grundläggande idén är att det är enkelt att multiplicera två stora primtal men att det blir mycket svårt att återställa faktorerna från produkten. Säkerheten i RSA beror på att klassiska datorer inte kan faktorisera tillräckligt stora tal inom rimlig tid.

Med dagens bästa algoritmer tar faktoriseringen av mycket stora tal så lång tid att den blir praktiskt ogenomförbar, vilket gör RSA säkert vid stora nyckellängder (t.ex. 2048 eller 4096 bitar). En tillräckligt kraftfull kvantdator kan dock använda Shors algoritm som utför faktoriseringen betydligt mer effektivt och kan minska beräkningstiden från tusentals år till timmar eller minuter.

ECDSA och diskreta logaritmproblemet

Elliptic Curve Digital Signature Algorithm (ECDSA) bygger på den elliptiska kurvans diskreta logaritmproblem (ECDLP). Detta problem innebär kort att det är mycket svårt att göra beräkningar med klassiska datorer för att komma åt data.

På klassiska datorer är den bästa kända metoden för att lösa ECDLP Pollards rho-algoritm, som växer i komplexitet snabbt nog för att stora nycklar (t.ex. 256-bitars kurvor) ska anses säkra. En tillräckligt kraftfull kvantdator kan dock använda Shors algoritm för att lösa problemet betydligt mer effektivt och kan minska beräkningstiden från tusentals år till timmar eller minuter.

SHA-256 och Grovers Algoritm

SHA-256 är en kryptografisk hash-funktion som genererar ett 256-bitars hash-värde från en given indata. Den grundläggande idén är att det är enkelt att beräkna hash-värdet för indata men mycket svårt att återställa ursprunglig indata från hash-värdet. Säkerheten i SHA-256 bygger på att det är mycket svårt att hitta indata som ger ett specifikt hash-värde, vilket gör den resistent mot kollisions- och preimageattacker. En kollisionsattack är en attack där en antagonist försöker hitta värden som ger samma hash som den hash man söker och i en preimageattack försöker antagonisten hitta ett meddelande som motsvarar ett visst hash-värde.

Med klassiska datorer krävs det ett enormt antal beräkningar för att hitta specifikt indata eller kolliderande värde, vilket gör SHA-256 mycket säker vid vanliga användningsområden. En tillräckligt kraftfull kvantdator kan dock använda Grovers algoritm, som effektivt kan halvera säkerheten i SHA-256. Detta innebär att en kvantdator kan hitta matchande indata som ger samma hash-värde mycket snabbare än en klassisk dator, vilket gör SHA-256 svagare mot kvantattacker.

Att Shors algoritm effektivt kan knäcka både RSA och ECDSA betyder att hela säkerheten hos vissa system faller om tillräckligt kraftfulla kvantdatorer byggs. Därför utvecklas nu kvantdatorsäker kryptografi som använder algoritmer som inte på samma sätt kan forceras av kvantdatorer.

AES, Shors algoritm och Biclique attack

AES anses för närvarande vara en säker algoritm vid användande av en nyckellängd på minst 128 bitar. Den är i huvudsak känslig för två typer av attacker där den ena är realiserbar idag med klassiska datorer, metoden kallas "Biclique attack" men är fortfarande med dagens datorers prestanda inte tillräckligt effektiv för att kunna forcera krypteringen. När det gäller kvantdatorer så är det Shors algoritm som gör den känslig. Det råder idag delade meningar om hur känslig AES är för detta, Shors algoritm halverar nyckellängden men måste exekveras seriellt för att den effekten ska nås. Om man försöker parallellisera beräkningarna sjunker prestanda avsevärt. Däremot är prestandaförlusten inte linjär om man till exempel dubblar nyckellängden från 128 till 256 bitar, förlusten är ca 40%.

5.1.3 Kvantdatorsäkra algoritmer

För att hantera de säkerhetsrisker som kvantdatorer medför har nya kryptografiska algoritmer godkänts av NIST. Tre stycken algoritmer godkändes 13 augusti 2024 (FIPS 203, 204 och 205) och fyra stycken 10 oktober 2020 (SP800-208). Dessa kallas kvantdatorsäkra algoritmer och är särskilt utformade för att motstå angrepp från kvantdatorer. Till skillnad från traditionella krypteringsmetoder är de inte sårbara för Shors algoritm och kan därför inte forceras med kvantbaserad faktorisering eller diskret logaritmberäkning.

Nedan följer en beskrivning av de nya kryptografiska algoritmerna. För beskrivning av säkerhetsnivåer kap. 2.2.

ML-KEM

Federal Information Processing Standard (FIPS) 203 introducerar Module-Lattice-Based Key-Encapsulation Mechanism (ML-KEM), en nyckelinkapslingsmekanism baserad på CRYSTALS-Kyber-algoritmen. ML-KEM är utformad för att motstå framtida attacker från kvantdatorer och används för att etablera delade hemliga nycklar mellan två parter över ett offentligt nätverk, tänkt användningsområde är till exempel för TLS-anslutningar.

ML-KEM finns med tre olika nyckellängder för olika säkerhetsnivåer:

- ML-KEM 512 för säkerhetsnivå 1
- ML-KEM 768 för säkerhetsnivå 3
- ML-KEM 1024 för säkerhetsnivå 5

Ovan klassificering innebär att det är rekommenderat att använda nivå 3 eller 5.

ML-DSA

FIPS 204, även den publicerad den 13 augusti 2024, specificerar Module-Lattice-Based Digital Signature Algorithm (ML-DSA), baserad på CRYSTALS-Dilithium-algoritmen. ML-DSA används för att skapa digitala signaturer som säkerställer dataintegritet och autentisering, och erbjuder motståndskraft mot kvantdatorattacker. ML-DSA är snabbare än SLH-DSA vad gäller generering av signaturer och validering av dessa samt även storleken på signaturerna vilket gör den lämpligare för att till exempel användas till certifikat för Certificate Authorities (CA), certifikatutfärdare.

Detta är, enligt NIST, den primära algoritmen för signaturer att använda.

ML-DSA finns med tre olika nyckellängder för olika säkerhetsnivåer:

- ML-DSA 44 för säkerhetsnivå 3
- ML-DSA 65 för säkerhetsnivå 4
- ML-DSA 87 för säkerhetsnivå 5

SLH-DSA

FIPS 205, också publicerad den 13 augusti 2024, beskriver Stateless Hash-Based Digital Signature Algorithm (SLH-DSA), baserad på SPHINCS+-algoritmen. SLH-DSA är utformad för att erbjuda kvantdatorsäkerhet för digitala signaturer utan att kräva tillståndshantering, vilket gör den särskilt användbar i vissa applikationer där tillståndshantering är opraktisk. På grund av att nyckelstorleken i SLH-DSA är mindre än i ML-DSA lämpar sig SLH-DSA bättre för lövcertifikat, dvs certifikat som används på till exempel webbservrar eller klienter av olika slag på grund av att de är effektivare för autentisering i realtid för till exempel TLS.

Säkerhetsnivåerna är enligt följande där f står för fast och s för small där de används för olika syften. F är optimerat för nyckelgenerering och signering och s är optimerad för verifiering.

- SLH-DSA-SHA-128f/s och SLH-DSA-SHAKE-128f/s för säkerhetsnivå 1
- SLH-DSA-SHA-192f/s och SLH-DSA-SHAKE-192f/s för säkerhetsnivå 3
- SLH-DSA-SHA-256f f/s och SLH-DSA-SHAKE-256f/s för säkerhetsnivå 5

FN-DSA (kommande)

FIPS 206 är en kommande standard som förväntas specificera FN-DSA (FFT (Fast-Fourier Transform) över NTRU-Lattice-Based Digital Signature Algorithm), baserad på FALCON-algoritmen. Algoritmen är som namnet antyder en algoritm för signaturer. Denna standard är under utveckling och förväntas publiceras under första halvåret 2025 efter att pågående ytterligare granskning och testning slutförts. Algoritmen förväntas komma i varianter för säkerhetsnivå 1 och 5 och målgruppen är applikationer som kräver en mindre signatur än vad ML-DSA kan erbjuda.

XMSS, XMSS^{MT}, LMS, HSS

NIST SP800-208 (publicerad 10 oktober 2020) godkänner användningen av två stateful hash-baserade signaturscheman: eXtended Merkle Signature Scheme (XMSS) och Leighton-Micali Signature system (LMS) tillsammans med multi-tree varianterna XMSS^{MT} och Hierarchical Signature Scheme (HSS). Dessa algoritmer erbjuder digitala signaturer som är säkra mot kvantdatorattacker men kräver noggrann hantering av tillstånd för att säkerställa deras säkerhet. Rekommendationen är att nycklar och signaturer genereras i en HSM som inte tillåter export av nyckelmaterialet oavsett om det är krypterat eller inte.

HQC (kommande)

HQC är tänkt som en reservalgoritm till ML-KEM om den skulle visa sig ha brister. Den är baserad på en annan typ av matematiskt problem. Algoritmen har passerat det fjärde urvalet och är ensam kvar som kandidat och den ger samma funktionalitet som ML-KEM och beräknas om allt går väl att standardiseras under 2027. ML-KEM är fortfarande rekommenderat som den primära algoritmen för nyckeldelning.

Andra algoritmer

Det finns andra algoritmer såsom Classic McEllice, SHA3 och SHAKE som brukar nämnas i sammanhanget kvantdatorsäkra algoritmer. Classic McEllice är en KEM-algoritm som introducerades 1978. Den har klarat av otaliga försök till attacker och kan enkelt skalas upp för att möta hot från allt kraftfullare klassiska datorer och kvantdatorer.

SHA3 och SHAKE är varianter av hash-algoritmer som beroende på parameterset anses kvantdatorsäkra.

5.2 Marknadens mognadsgrad

Vid framtagandet av den här vägledningen har frågan ställts till ett urval av leverantörer kring vilken deras strategi är för övergången till kvantdatorsäkra algoritmer, gällande vad de har för tankar och planer kopplat till detta. Av de 15 leverantörer som tillfrågats har en avstått att svara av "säkerhetsskäl". Av övriga leverantörer har några valt att inte svara alls och andra har svarat mer eller mindre detaljerat. I vissa fall har de uppfattats som avvaktande och har inte gett några tydliga svar. Nedan följer en summering av de svar som har inkommit. En del av svaren har varit av karaktären marknadsföringsmaterial och då innehållet inte bedömts vara relevant för ändamålet har dessa därför inte tagits med i sammanställningen. Microsoft har inte lämnat några svar, men eftersom de har en så stor marknadsandel och användning har vi tagit med underhandsinformation samt en bloggpost om deras produkter då vi anser att den är av stort allmänt intresse.

5.2.1 Hardware Security Modules (HSM)

En HSM är en kryptografisk hårdvara vars syfte är att generera och lagra kryptografiskt material på ett säkert sätt. Den har funktionalitet som gör att nyckelmaterial inte behöver lämna den vid utförande av nyckeloperationer. Detta gör en HSM till en vital del i till exempel ett PKI eller ett Key Management System (KMS). En HSM har en ganska lång produktcykel vilket innebär att förändringar tar tid.

Vissa leverantörer har implementerat stöd för kvantdatorsäkra algoritmer i nuvarande versioner av hårdvaran, men då prestandan är optimerad utifrån nuvarande algoritmer så är den inte tillräcklig för de nya algoritmerna. Stöd finns dessutom enbart för att generera nyckelmaterial baserat på de nya algoritmerna medan signering av mjukvara och firmware fortfarande sker med klassiska algoritmer.

Tillverkare	Beredskap för kvantdatorsäkra algoritmer
Entrust	I Entrust nShield finns stöd via tillägg för kvantdatorsäkra algoritmer och fullt stöd kommer tillsammans med hårdvarustöd. Först ut via tillägg är ML-DSA som följs av ML-KEM. SLH-DSA kommer därefter. Det är oklart när mjukvara och firmware börjar signeras med kvantdatorsäkra algoritmer. För Entrust Edge (USB-HSM) kommer sannolikt stöd i nästa version.
IBM	IBM levererar HSM:er till egna system, till exempel stordator eller PowerPC-baserade system. I dagsläget är det bara den senaste versionen som är avsedd för stordator som har stöd för kvantdatorsäkra algoritmer.
Thales	Stöd finns via tillägg för kvantdatorsäkra algoritmer. Under 2025 kommer stöd för kvantdatorsäkra algoritmer i ordinarie mjukvara. Stöd kommer för ML-KEM, ML-DSA och SLH-DSA. Utöver det kommer stöd för LMS under 2025.
Yubico	Yubico har i ett första steg lagt till stöd för RSA-nycklar på 3072 och 4096 bitar. Man tittar just nu på implementation av kvantdatorsäkra algoritmer.

5.2.2 Certificate Authorities

Ett Certificate Authority (CA) används för att utfärda digitala certifikat med tillhörande privata och publika nycklar och är därför grunden till att kunna göra en migrering till kvantdatorsäkra algoritmer. Om ett CA inte kan skapa certifikat som är antingen av typen hybridcertifikat eller certifikat med nycklar baserade helt på kvantdatorsäkra algoritmer så går det inte att använda detta för att migrera till kvantdatorsäkra algoritmer.

Idag finns hos de leverantörer som tillfrågats ett varierande stöd för kvantdatorsäkra algoritmer. Det finns fler CA-system som inte omfattas av denna sammanställning och rekommendationen är att tillfråga nuvarande och potentiella leverantörer av intresse om deras förmåga att stödja kvantdatorsäkra algoritmer. Om du har en HSM kopplad till sitt CA

för lagring av nyckelmaterial så behöver du även tillse att den har stöd för kvantdatorsäkra algoritmer.

Observera att ett stöd för kvantdatorsäkra algoritmer inte innebär att de certifikat som utfärdas följer en av Internet Engineering Task Force (IETF) fastslagen standard då en sådan inte finns klar i skrivande stund.

Flera leverantörer erbjuder CA som tjänst och där går det i regel lite fortare att få in stöd för nya algoritmer.

Tillverkare	Beredskap för kvantdatorsäkra algoritmer
Keyfactor EJBCA	Stöd för kvantdatorsäkra algoritmer finns implementerat och tillgängligt på samma sätt som klassiska algoritmer. EJBCA implementerar stöd för detta genom BouncyCastle som de själva utvecklar.
Microsoft ADCS	Ej tillräcklig information från leverantör. Underhandsinformation har angett att stöd kommer, men påståendet har inte kunnat bekräftas. Det är även osäkert på vilket sätt stöd implementeras samt när i tiden ett eventuellt stöd kommer.
Nexus CM	Stöd är under utveckling men oklart hur det kommer att se ut och hur det kommer att fungera.

5.2.3 Key Management System

Likt ett CA har ett Key Management System (KMS) en grundläggande roll i migreringen mot kvantdatorsäkra algoritmer. Ett KMS skapar kryptografiskt nyckelmaterial med symmetriska nycklar som används för att till exempel kryptera eller signera data. En åtgärd som du kan vidta i närtid är att öka nyckellängden för de nycklar som genereras för att försvåra för en kvantdator att beräkna vilka nycklar som använts för att kryptera data. I dagsläget finns det inte några nya godkända algoritmer för symmetrisk kryptering utan rekommendationen är att tillse att nycklarna har adekvat längd.

Ett KMS genererar oftast symmetriska nycklar men de nycklarna distribueras över en krypterad förbindelse som skapas med asymmetriska algoritmer vilket gör att man behöver tillse att den förbindelsen upprättas med motsvarande 128 bitars kryptering till dess att kvantdatorsäkra algoritmer kan användas.

Tillverkare	Beredskap för kvantdatorsäkra algoritmer
Thales Ciphertrust	Stöd för ML-KEM kommer under 2025 för etablering av TLS-anslutningar, SSH, och SNMP och arbetet fortsätter sedan med stöd för kvantdatorsäkra kryptoalgoritmer internt i produkten, gällande lagring samt för kvantdatorsäker kodsignering av produktens firmware etc.
Fortanix KMS	Fortanix KMS har idag stöd för de algoritmer som rekommenderas i CNSA 2.0 vilket är samtliga idag godkända algoritmer.
Entrust KeyControl	Stödjer AES-256 men det är just nu oklart om kvantdatorsäkra algoritmer för transport av nyckelmaterial till klienter stöds.
Keyfactor Command	Stöd för kvantdatorsäkra algoritmer finns implementerat och tillgängligt på samma sätt som klassiska algoritmer.

5.2.4 Elektroniska underskrifter

Som nämnts tidigare så påverkas även elektroniska underskrifter av övergången till kvantdatorsäkra algoritmer. När dagens algoritmer knäcks kommer dokument som är signerade med dagens algoritmer kunna manipuleras och få en ny giltig signering och därmed har riktigheten avseende dokumentet gått förlorad.

Tillverkare	Beredskap för kvantdatorsäkra algoritmer
PhenixID Signing	PhenixID bygger sin applikation på färdiga bibliotek för kryptografiska operationer vilket gör att de snabbt kan införa kvantdatorsäkra algoritmer så snart biblioteken stödjer det och signaturerna kan konsumeras av de som behöver det. Detta gäller även TLS-anslutningar till programvaran, där de stödjer TLS 1.3 och har därmed möjlighet att utnyttja ML-KEM. De tittar även på hur signering av programpaket ska göras för att vara kvantdatorsäkert.
Keyfactor SignServer	Stöd för kvantdatorsäkra algoritmer finns implementerat och är tillgängligt på samma sätt som för klassiska algoritmer.

5.2.5 Brandväggar

En brandvägg har ofta, utöver att skydda nätverket från otillbörlig åtkomst, uppgiften att hantera VPN-anslutningar från klienter eller andra nätverk. En risk som finns i samband med etablering av VPN-anslutning är att mängden data som skickas blir för stor och att paket därför tappas bort. Eftersom trafiken ofta sker över UDP-protokollet, som är ett så kallat tillståndslöst protokoll, håller det inte reda på om paket försvinner på vägen. Detta är redan idag ett problem hos vissa internetleverantörer då anslutningen inte slutförs som avsett på grund av att även vanliga certifikat innehåller för mycket data och blir för stora.

Utöver detta kan det bli problem med vanliga anslutningar när kvantdatorsäkra algoritmer används för till exempel webbsidor där storleken på certifikaten blir för stora och anslutningar tar för lång tid eller inte slutförs innan time-out.

Tillverkare	Beredskap för kvantdatorsäkra algoritmer
Clavister	Clavister är en svensk leverantör av brandväggar med VPN-funktionalitet. På förfrågan svarar de att de under 2025 planerar att ha stöd för kvantdatorsäkra algoritmer i sina brandväggar och VPN-klienter men att de inte kommer att vara aktiverade som standard utan att de behöver slås på manuellt. Från 2030 kommer de kvantdatorsäkra algoritmerna vara standard och aktiverade per default. Från 2030 börjar sedan dagens algoritmer att avvecklas. Produkten är baserad på WolfSSL-kryptobibliotek.

5.2.6 Operativsystem

För att kunna få en bred spridning av nya algoritmer behöver operativsystem förstå och hantera de nya algoritmerna. Beroende på typ av operativsystem varierar metoden för att få tillgång till kvantdatorsäkra algoritmer. Utöver det som nämns nedan används OpenSSL i olika versioner och Java för kryptografisk funktionalitet där OpenSSL får formellt stöd i version 3.5 och Java i version 24.

Tillverkare	Beredskap för kvantdatorsäkra algoritmer
MacOS	Ej tillräcklig information från leverantör. Bristfällig information på publika webbsidor. Man har publicerat information om att man har implementerat kvantdatorsäkra algoritmer i iMessage. Visst stöd kan fås genom Java 24 och OpenSSL 3.5.
Microsoft Windows	Ej tillräcklig information från leverantör. En bloggpost säger att stöd kommer, det är osäkert på vilket sätt stöd implementeras, samt när i tiden ett eventuellt stöd kommer. Stöd kommer att implementeras genom Schannel. Stöd för FIPS 203, 204 och 205 samt LMS och XMSS finns.

Linux	Det finns ett antal olika distributioner av Linux där ändringar och uppdateringar hanteras lite olika och det kan i viss mån även skilja i hur ny funktionalitet kommer in i distributionen. Samarbetsorganet The Linux Foundation har samarbetat med NVIDIA för att i sitt projekt Open Quantum Safe (OQS) implementera stöd för hårdvaruacceleration i GPU för ML-KEM och ML-DSA för att på det sättet öka prestanda. Oavsett GPU kommer OQS ha stöd för kvantdatorsäkra algoritmer. Rekommendationen är att undersöka vad som gäller för den distributionen man själv använder. Microsoft är även med i projektet Symcrypt-OpenSSL som ska förse Linux med stöd för kvantdatorsäkra algoritmer.

5.2.7 Webbläsare

De vanligaste webbläsarna har redan idag stöd för ML-KEM över TLS 1.3.

Tillverkare	Beredskap för kvantdatorsäkra algoritmer
Chromium-baserade webbläsare	Stöd för kvantdatorsäker algoritm (ML-KEM) finns.
Firefox	Stöd för kvantdatorsäker algoritm (ML-KEM) finns.

5.2.8 Smartcards och tokens

Ett smartcard är tämligen begränsat i sin förmåga att lagra och göra beräkningar och de behöver anpassas för att kunna hantera det större nyckelmaterialet. Utöver det så behöver de relevanta standarder som används för att till exempel fastställa certifikatformat.

Tillverkare	Beredskap för kvantdatorsäkra algoritmer
Thales smartcards	Thales har för avsikt att släppa sitt första smartcard med stöd för kvantdatorsäkra algoritmer sent 2026 med stöd för ML-KEM och ML-DSA65 samt att de även då ska vara bakåtkompatibla. Planerna för detta kan komma att ändras då de standarder som detta baseras på inte är beslutade.
Yubico Yubikeys	Yubico har i ett första steg lagt till stöd för RSA nycklar på 3072 och 4096 bitar. Man tittar just nu på implementation av kvantdatorsäkra algoritmer.

5.2.9 Elektroniska legitimationer

Elektroniska legitimationer är baserade på dagens algoritmer och även de påverkas av hotet från kvantdatorer. I Sverige är användandet av elektroniska legitimationer utbrett både hos privatpersoner och inom organisationer. Inom organisationer kan det både vara i form av ett eget system för elektroniska identiteter eller att anställda använder sina egna privata elektroniska legitimationer. Här finns utmaningar i det att om man har signerat ett avtal med till exempel ett BankID som är giltigt över längre tid kan innehållet i avtalet förändras utan att det märks för den som signerat avtalet.

Tillverkare	Beredskap för kvantdatorsäkra algoritmer
Finansiell ID-teknik	Från BankID:s håll har man börjat titta på att migrera till kvantdatorsäkra krypton och är i en analysfas. Man tittar dels på själva BankID som användaren har samt de TLS-förbindelser som är mellan BankID och deras förlitandeparter där det troligtvis kommer att ta längre tid att genomföra migreringen på grund av antalet förlitandeparter.

5.2.10 Lagring

Data som lagras och har ett skyddsvärde behöver ett adekvat skydd för att säkerställa att det inte kan förändras utan att det märks.

Tillverkare	Beredskap för kvantdatorsäkra algoritmer
IBM - flera produkter	IBM har olika produkter som är förberedda för kvantdatorsäkra algoritmer som till exempel lagringslösningar för disk eller band.

6. Inventering av verksamhetens tillgångar

Ett viktigt steg i förberedelsen innan migrering till kvantdatorsäkra kryptografiska algoritmer är att genomföra en inventering. Du behöver ha kontroll på de rättsliga krav som gäller för er verksamhet och du behöver analysera riskerna om informationstillgångar skulle hamna hos obehöriga eller obehörigen manipuleras. Som verksamhetsutövare bör du även göra en inventering av vilka informationstillgångar verksamheten har som är krypterade eller signerade samt vilka system som hanterar detta. Det är också viktigt att se över vilka applikationer och hårdvara i verksamheten som tillämpar kryptografiska funktioner och vilka som inte gör det. De senare kan då uteslutas från arbetet. Inventeringen ska ge svar på vilken funktionalitet applikationerna har och vilka protokoll som tillämpas av applikationerna.

Generellt kan sägas att mognadsgraden beträffande kvantdatorsäkra kryptolösningar på marknaden är begränsad, och det stöd som finns för kvantdatorsäkra algoritmer i till exempel kryptografisk hårdvara (HSM) prestandamässigt inte är optimerad för kvantdatorsäkra algoritmer. Inom vissa områden saknas produkter som klarar av dessa algoritmer, ett sånt område är smartcards. Detta gör att det för vissa användningsområden kan vara utmanande att implementera kvantdatorsäkra algoritmer idag. Därför måste du på egen hand göra en inventering av era system för att ha kontroll över vad som används och vad som därmed behöver hanteras och säkras upp. Inventeringen ger dig det underlag som ni behöver för att kunna ställa krav på dina leverantörer av produkter som kan användas för detta ändamål.

Resultatet av inventeringen bör ge dig en lista över vilka applikationer och vilken data som är mest kritiskt, som du också kan använda som stöd för prioritering. Inventeringen och prioriteringen av systemen kan även ligga till grund för att fastställa, införa och tillämpa er strategi och era förfaranden för kryptografi som kommande lagstiftning väntas kräva.

6.1 Produkternas mognadsgrad för kvantdatorsäkra algoritmer

Vid bedömningen av en produkts mognadsgrad för hantering av kvantdatorsäkra algoritmer finns det flera omständigheter att uppmärksamma. Den mest uppenbara omständigheten är om produkten kan hantera de specifika kvantdatorsäkra algoritmer som du önskar använda. Men du behöver även undersöka om produktens egna binärer och/eller skript är signerade med kvantdatorsäkra algoritmer och framför allt, produktens förmåga att hantera flera olika algoritmer om behov uppstår för olika syften eller om du av annan anledning behöver byta algoritm, så kallad kryptoagilitet.

6.2 Mognadsgrad för kvantdatorsäkra protokoll

Det finns ett antal protokoll som är beroende av kryptografiska algoritmer för att kryptera och signera data. Dessa protokoll är vanligt förekommande i en normal it-miljö. Du behöver inventera detta i er it-miljö för att veta vad som behöver säkerställas för just er verksamhet. Utöver själva applikationsprotokollen påverkas även Transmission Control Protocol (TCP) och User Datagram Protocol (UDP) då kvantdatorsäkra algoritmer innehåller större datamängder, vilket påverkar applikationernas prestanda.

Generellt kan sägas att de nya algoritmerna kommer att innebära en ökad trafikmängd vad gäller upprättande av förbindelser på grund av framförallt större nyckelpar och signaturer. Detta leder till en ökad dataöverföring som, beroende på hur it-miljön ser ut, kan leda till trafikstockningar och potentiella Denial of Service-attacker (DoS). Den större datamängden innebär också en risk i att data fragmenteras vilket kan orsaka förlust av paket eller paket som kommer fram i felaktig ordning, vilket främst är ett problem för tjänster som använder UDP som protokoll.

I flertalet fall finns det i teorin möjlighet att olika typer av attacker sker, som till exempel side-channel attacks, vilka bygger på olika möjligheter att samla läckt information för att komma åt det nyckelmaterial som används. De skydd som finns mot side-channel attacks och andra typer av attacker byggs in i implementationerna av de olika kvantdatorsäkra algoritmerna.

Nedan redogörs för ett urval av protokoll som är beroende av kryptografiska algoritmer och hur status ser ut för att nyttja kvantdatorsäkra algoritmer.

Protokoll	Beredskap för kvantdatorsäkra algoritmer
Transport Layer Security (TLS)	Många protokoll som använder kryptografi, utöver vanlig webbtrafik, använder i grund och botten protokollet Transport Layer Security (TLS). Det gör att det är ett av de viktigaste protokollen att migrera till kvantdatorsäkra algoritmer. Migreringen kommer att innebära dels en ökad trafikmängd på grund av de längre nycklarna och dels en försämring av prestanda för de enheter som ska hantera dessa protokoll. På sikt kommer den tekniska utvecklingen att förbättra den situationen. TLS version 1.3 stödjer kvantdatorsäkra algoritmer även om protokollet inte är optimerat för dessa. Arbete pågår inom Internet Engineering Task Force (IETF) för att ta fram riktlinjer för detta.
File Transfer Protocol Secure (FTPS)	File Transfer Protocol Secure (FTPS) som är ett protokoll för säker filöverföring som bygger på TLS vilket innebär att om TLS kan utnyttja kvantdatorsäkra algoritmer så blir även FTPS kvantdatorsäkert.

Protokoll	Beredskap för kvantdatorsäkra algoritmer
Secure SHell (SSH)	Secure SHell (SSH) är ett protokoll utvecklat inom IETF och det finns idag inga planer på att introducera kvantdatorsäkra algoritmer till protokollet. Det finns däremot redan nu implementationer av kvantdatorsäkra algoritmer i SSH i till exempel implementationerna OQS OpenSSH och i WolfSSH och arbetet gör det möjligt att i efterhand standardisera olika algoritmer i protokollet.
Secure File Transfer Protocol (SFTP)	Secure File Transfer Protocol (SFTP) bygger på SSH och kan hanteras på samma sätt som SSH.
DNSSEC	DNSSEC som används för att signera data i Domain Name System (DNS) så att klienter eller servrar som kontaktar DNS-servern kan validera att det kommer från rätt DNS och att informationen kommer från korrekt källa, använder inte certifikat utan enbart kryptografiska nycklar för att signera DNS-data med ett publikt/privat nyckelpar. I och med att nyckelparen kommer att bli större riskerar man fragmentering av den data som skickas, som tidigare kunde skickas i ett enda UDP- eller TCP-paket. Detta kan leda till att lasten på DNS-servern blir högre på grund av mer overhead. Dels på grund av det större nyckelmaterialet och dels på grund av att mängden paket som ska skickas ökar. Resultatet kan bli överbelastning i och med att det blir en större datamängd att hantera per DNS-fråga.
SAML	Security Assertion Markup Language (SAML)-protokollet, som används för signering och kryptering av SAML-intyg, har inga direkta begränsningar i nyckellängder men som övriga protokoll kräver det en väl byggd implementation av de kryptografiska algoritmerna för att skydda nyckelmaterialet. Används TLS för att ansluta till tjänsten behöver man ta det i beaktning också.
Oauth	I open authorization (Oauth) v2 behöver man byta algoritm för tokensignering till en som är kvantdatorsäker. Det kommer att leda till längre nycklar, vilka ska rymmas i de 2048 bytes som är tillåtet i protokollet för detta. Används TLS för att ansluta till tjänsten behöver man ta det i beaktning också.
Kerberos	Kerberos-protokollet använder symmetriska nycklar och man behöver tillse att nyckellängden är tillräcklig för att inte vara känslig för Grovers algoritm eller "Birthday attacks". Det är inte tillräckligt att bara öka nyckellängden utan man behöver även tillse att man har god entropi (källa till slumpmässighet) när nyckeln skapas och att nycklarna inte är baserade på lösenord.

Protokoll	Beredskap för kvantdatorsäkra algoritmer
LDAPS	Lightweight Directory Access Protocol (LDAPS)-protokollets förmåga att använda kryptering bygger på TLS och även dess förmåga att använda kvantdatorsäkra algoritmer.
PGP (Pretty Good Privacy)	Det pågår arbete i IETFs regi att standardisera hur OpenPGP ska använda kvantdatorsäkra algoritmer, både vad gäller asymmetrisk kryptering och symmetrisk kryptering.
S/MIME	Det pågår arbete i till exempel Open Quantum Safe för att i OpenSSL implementera stöd för kvantdatorsäkra algoritmer i Secure/Multipurpose internet Mail Extensions (S/MIME).
IPSec och IKEv2	Internet Protocol Security (IPSec) används för säkra anslutningar mellan datorer bland annat i en del Virtual private Network (VPN)-lösningar. För att sätta upp förbindelsen används protokollet Internet Key Exchange version 2 (IKEv2) för kryptografiska nycklar. Request for Comments (RFC) 8784 beskriver hur IKEv2 kan göras kvantdatorsäkert och om man använder protokollet bör man undersöka hur nämnda RFC stöds av de applikationerna och/eller de operativsystem man använder.

Andra protokoll och funktioner

Det finns många andra protokoll och funktioner som också kommer att påverkas av utvecklingen av kvantdatorer som inte är listade ovan och det varierar hur långt gången planering och arbete har kommit för att kunna utnyttja kvantdatorsäkra algoritmer för dessa. En viktig funktion där det kvarstår arbete är Trusted Platform Module (TPM)-chip, som har en viktig funktion i alla moderna datorer för att lagra kryptografiskt data och tillhörande "Secure Boot". Ett annat vanligt protokoll för till exempel mobila enheter är Simple Certificate Enrollment Protocol (SCEP). SCEP har idag inget stöd för kvantdatorsäkra algoritmer utan använder enbart RSA, och beroende på implementation, ECC-nycklar.

6.3 Metod för att inventera era informationstillgångar och er it-miljö

Inventering av verksamhetens informationstillgångar och it-miljö inbegriper flera olika delar där vilka kryptografiska algoritmer som används naturligtvis är en del, och en annan del vilka applikationer som används och vad de har för förutsättningar att använda andra algoritmer. Utöver det behöver du undersöka vilka protokoll som används för att kommunicera till och från applikationen och till sist om det finns hårdvara som använder kryptografiska algoritmer för att kryptera och signera. Metoden för inventering nedan bör tillämpas i prioritetsordning där de för verksamheten mest kritiska tillgångarna inventeras först för att analyseras i fallande prioritetsordning. Migreringen av kritiska tillgångar behöver påbörjas så snart dessa är inventerade, förutsatt att det inte finns beroenden till andra tillgångar/system.

6.3.1 Risk- och konsekvensanalys

En del av inventeringen är att bedöma riskerna om ingen migrering över till kvantdatorsäkra algoritmer genomförs. Grunden till riskinventeringen är verksamhetens informationstillgångar, vilka applikationer verksamheten använder, vilka protokoll som används samt vilka system och vilken hårdvara som används för detta. Den här vägledningen beskriver ingen exakt metod för hur en riskanalys ska genomföras då vi utgår från att varje organisation har en metodik för detta, däremot lyfts de områden som behöver riskbedömas. Frågan du behöver ställa dig är hur verksamheten påverkas om informationstillgångar blir tillgängliga för obehöriga eller om signerat data eller programkod obehörigen ändras eller förvanskas. Om du bedömer att det finns en risk kopplat till detta behöver verksamheten vidta åtgärder. Resultatet av riskanalysen bör bli en lista som är sorterad utifrån risknivå så att ni kan prioritera därefter och hantera de mest kritiska systemen först och sedan gå vidare i fallande ordning.

6.3.2 Inventering och klassificering

En viktig del av inventeringen är kännedom om verksamhetens informationstillgångar, vad det är för sorts information, hur skyddsvärd den är och framförallt var den finns och i vilken form - till exempel i en databas eller i ett filsystem. Informationstillgångar med högt skyddsvärde behöver prioriteras därefter. Inventeringen bör dokumenteras och innehålla uppgifter om:

- Var informationstillgångarna finns.
- Hur stort skyddsvärde, vilken klassificering, informationstillgångarna har.
- Hur sker access till informationstillgångarna.
- Applikationer som behandlar eller behövs för informationstillgångarna.

6.3.3 Inventering av applikationer och protokoll

Det är nödvändigt att titta på de applikationer som ni använder och hur de kommunicerar, och vilka protokoll de använder för att kunna bedöma om det går att migrera till kvantdatorsäkra algoritmer. Inventeringen bör dokumenteras och innehålla uppgifter om:

- Leverantör av programvara.
- Uppgift om applikationen krypterar och/eller signerar data.
- Uppgift om applikationen använder krypterade förbindelser för att kommunicera och i sådant fall vilka protokoll som används.
- Eventuella beroenden till andra programvaror.

För att inventeringen ska bli fullständig är det även viktigt att ta reda på vilka applikationer som inte berörs och som därför kan lämnas utanför strategin.

6.3.4 Inventering av hårdvara

Utöver programvara och protokoll behöver du även analysera den hårdvara som verksamheten använder för att bedöma om den på något sätt använder kryptografiska algoritmer. Exempel på detta kan vara vid autentisering mot utrustning med hjälp av certifikat på till exempel smartcards, nätverksutrustning, HSMer eller annan kryptografisk utrustning. Observera att hela it-miljön behöver analyseras eftersom användningen av denna typ av funktioner förekommer i ökande grad hos it-miljöns olika komponenter. Inventeringen bör innehålla dokumenterade uppgifter om:

- Leverantör av hårdvara.
- Uppgift om hårdvaran krypterar och/eller signerar data.
- Uppgift om hårdvaran använder krypterade förbindelser för att kommunicera.
- Eventuella beroenden till andra programvaror eller annan hårdvara.

6.3.5 Inventering av lösningar

Baserat på informationen om applikationer och hårdvara bör ni kontakta leverantören för att få information om hur de arbetar med de här utmaningarna och efterfråga möjligheterna att övergå till kvantdatorsäkra algoritmer. Beroende på status på produkten kan ni vara tvungna att byta ut hela eller delar av lösningen för att uppnå detta. Det är viktigt att vara medveten om att det inte bara är data i applikationen som berörs utan även signerade programpaket, för att påvisa att de inte har förändrats sedan leverantören gjorde dem tillgängliga. Du behöver även fråga hur kryptoagila de är för att veta om du kan byta kryptografiska algoritmer om behov uppstår.

I första hand behöver ni vända er till leverantören av det eller de system som berörs för stöd i processen.

6.4 Rekommendationer inventering

Att inventera hela sin it-miljö, ur perspektivet kvantdatorsäkra algoritmer, kan vara en omfattande uppgift. På grund av detta rekommenderar vi att lägga upp en plan för inventeringen och tänka igenom vad den ska innefatta och vad ni vill ha ut av den, så att ni kan fatta nödvändiga beslut baserat på resultatet av inventeringen. Utöver prioritetsordning kan resultatet av inventeringen utgöra ett stöd för fastställande av er strategi och förfaranden för kryptografi och genomförandet av migrering.

När du kommit så långt i processen att ni inventerat alla system och kontaktat leverantörerna till dessa bör du ha en strategi för att hantera system där leverantören inte har förmåga att uppgradera för migrering till kvantdatorsäkra algoritmer. Detta innebära att du behöver ta ställning till vad det innebär att fortsätta med programvaran i ett potentiellt sårbart utförande alternativt om det går att byta ut systemet mot ett annat system som har stöd för kvantdatorsäkra algoritmer.

7. Migrering till kvantdatorsäkra algoritmer

Efter genomförd inventering, riskanalys och lägesbedömning av er verksamhets it-miljö, i syfte att avgöra vad som är möjligt och lämpligt att genomföra, behöver du bestämma hur migreringen ska genomföras. När du vet vad du bör göra och vad det finns för möjligheter kan verksamheten fatta beslut om metod för migrering.

Det finns två huvudsakliga tillvägagångssätt för migrering till kvantdatorsäkra algoritmer. De två tillvägagångsätten kan variera lite. Det enklaste - men också svåraste - är att migrera alla de komponenter som använder nuvarande kryptoalgoritmer på en gång. Den metoden är idag inte möjlig eftersom det saknas fullständiga förutsättningar för det, i form av mjuk- och hårdvara med tillräckligt stöd för kvantdatorsäkra algoritmer. En variant är att migrera enskilda system till kvantdatorsäkra algoritmer, vilket är möjligt så länge de inte har några externa beroenden. För enskilda system kan detta göras om de tekniska förutsättningarna finns, men att migrera en hel miljö blir svårare.

Det andra tillvägagångssättet är att gå mellanvägen och använda hybridcertifikat där det finns både ett nyckelpar med dagens algoritmer och ett med en kvantdatorsäker algoritm. För de system som inte förstår den kvantdatorsäkra algoritmen så ignorerar systemet den och använder istället en algoritm som systemet eller applikationen känner till. Utmaningen med denna lösning är att det än så länge inte finns någon etablerad standard för hur ett hybridcertifikat ska se ut.

För data krypterad med symmetrisk kryptering är det lite enklare eftersom det då handlar om att kryptera om data med en längre nyckel. Det kan i sig leda till problem om den längre nyckeln inte får plats i de datafält den behöver lagras i samt att det krävs planering för hur du genomför arbetet med att kryptera om data med en längre nyckel.

7.1 Kryptering av data med AES

Om du krypterar data med hjälp av Advanced Encryption Standard (AES) behöver du analysera nyckellängden. För att kunna bemöta hotet från kvantdatorer så kan du behöva öka nyckellängden på de nycklar som används för att kryptera data. Idag bedöms 128 bitars nyckellängd på vissa håll vara otillräckligt och rekommendationen i bland annat Commercial National Security Algorithm (CNSA) 2.0 är att utöka den till 256 bitar. Det innebär att du behöver dekryptera det data som berörs samt kryptera det på nytt med nya nycklar.

När du gör detta behöver du ha några saker i åtanke:

- Nyckelmaterialet behöver skyddas och förvaras på ett adekvat sätt, till exempel i en HSM.
- Det lagringsutrymme som används när du dekrypterar och krypterar data, dvs det som tillfälligt förekommer i klartext, behöver hanteras på ett säkert sätt både under och efter dekryptering/kryptering. Det är möjligt att utvinna raderat data från olika former av lagringsmedia så du måste säkerställa att det har förstörts på ett korrekt sätt så att informationen inte kan återskapas.

7.2 Metoder för att migrera till kvantdatorsäkra algoritmer

För att migrera behöver du fatta beslut baserat på er inventering om vilka system som ska migreras först och vad det finns för förutsättningar för att göra det. Sannolikt kommer du inte att kunna migrera hela miljön på en gång utan du behöver göra det i flera steg. I och med att det innebär förändringar i miljön har du även möjligheten i och med migreringen att införa andra förändringar som behövs.

Har du ett eget PKI för att förse er interna miljö med certifikat är det en prioriterad aktivitet att hantera det systemet. För att få en hållbar lösning för detta är det bästa alternativet att sätta upp ett parallellt PKI att migrera till. En del av arbetet i detta är att analysera systemets möjligheter. Kan det till exempel utfärda hybridcertifikat eller kan det endast utfärda certifikat baserat på kvantdatorsäkra algoritmer utöver klassiska algoritmer. En del system kan ha flera CA-kedjor i samma system och i andra system behöver du sätta upp ett helt nytt system med nya servrar. Har du ett nytt PKI baserat på kvantdatorsäkra algoritmer kan du migrera era system bit för bit.

Har systemet möjlighet att utfärda hybridcertifikat, det vill säga certifikat med dubbla nyckelpar där det primära paret är baserat på klassiska algoritmer av kompabilitetsskäl, kan även det vara en väg framåt. Då kan de system som konsumerar certifikaten välja vilket nyckelpar de använder efter vilken operation som ska utföras. Målet med detta är sedan att så snart som möjligt gå ifrån hybridcertifikaten till certifikat baserade på enbart kvantdatorsäkra algoritmer.

Viktigast är att säkerställa att den metod du väljer inte skapar andra problem. Du måste till exempel kunna hantera den ökade datamängden som blir följden av att nyckelmaterialet är större, vilket blir särskilt märkbart i hybridscenariot. I det sammanhanget får du inte glömma bort att CA-certifikaten i de fall de behöver skickas till klienten också kommer att vara större, vilket innebär att en större mängd data ska transporteras mellan klient och server.

Parallellt PKI

Som ett led i att påbörja tester i den interna miljön är det, för de verksamheter som redan har ett eget PKI, en bra start att sätta upp en ny CA-kedja baserad på kvantdatorsäkra algoritmer. Beroende på produkt kan detta göras med hjälp av nya servrar (till exempel Microsoft ADCS) eller som en ny kedja i en befintlig installation (till exempel Keyfactor EJBCA och Nexus CM). I den mån det går kan du även sätta upp en miljö som kan utfärda hybridcertifikat. Observera att du behöver säkerställa att den programvara du använder för CA stödjer de algoritmer och certifikatformat du behöver samt att de är utformade enligt definierad standard. Än så länge finns inget heltäckande stöd för alla algoritmer och format, vilket till stor del beror på att alla standarder inte är klara.

Hybridcertifikat

Tanken med hybridcertifikat är att det för en klient som inte kan hantera kvantdatorsäkra algoritmer och certifikat fungerar som ett "vanligt" certifikat. Det innebär att den primära nyckeln baserad på RSA eller ECC och det sekundära nyckelparet som är baserat på en kvantdatorsäker algoritm utgör ett tillägg i certifikatet som kan ignoreras av de system eller funktioner som inte förstår den. De klienter som kan hantera nyckelmaterial som är baserat på kvantdatorsäkra algoritmer väljer det sekundära nyckelparet och ignorerar det som är baserat på RSA eller ECC.

Observera att du behöver säkerställa att du tillämpar en kvantdatorsäker signeringsalgoritm för certifikaten samt att storleken på certifikaten blir större.

Certifikat med kvantdatorsäkra algoritmer

Om/när det finns möjlighet att använda certifikat med kvantdatorsäkra algoritmer bör du enbart använda dessa. Det kan finnas möjlighet att i begränsad skala använda den här typen av certifikat redan idag under förutsättning att de system som behöver kommunicera stödjer det och det inte finns något beroende till system som inte gör det.

Kryptografiska nycklar

Användning av enbart kryptografiska ("råa") nycklar utan ett certifikat är väldigt vanligt när det gäller signering eller kryptering. Även inom detta användningsområde gäller att de algoritmer som används för att ta fram nyckelmaterialet använder kvantdatorsäkra algoritmer, eller för symmetrisk kryptering att de använder tillräckligt långa nycklar.

8. Rekommenderade åtgärder för att kvantdatorsäkra er it-miljö

I den här sektionen summeras de rekommenderade åtgärderna för att migrera till en kvantdatorsäker it-miljö. Ytterligare bakgrund och information finns i tidigare sektioner.

Det finns idag inga färdiga produkter och standarder för allt för att kunna genomföra en komplett migrering till kvantdatorsäkra algoritmer men det innebär inte att du bör vänta med arbetet. Att byta ut kryptografiska algoritmer är oftast tidskrävande och resurskrävande. Det kan behöva bytas ut både utrustning och programvara mot nya versioner eller till och med byta dessa helt och hållet.

8.1 Regulatoriska krav

Du behöver ha kontroll på om det finns några lagregler som ställer krav på kryptering beträffande din verksamhet eller dina informationstillgångar. När det finns krav på kryptering gäller i allmänhet att verksamhetsutövaren ska använda den senaste tekniken. Samtidigt finns ofta i de gällande regelverken betydande utrymme för verksamhetsutövare att själva bedöma vilken kryptering som är lämplig att använda baserat på risk och kostnad. Det har ännu inte publicerats några avgöranden som underkänt en befintlig kryptering som otillräcklig. Hittills har myndighetsbesluten lett till sanktionsavgifter vid situationer där kryptering helt och hållet har saknats.

8.2 Inventering av informationstillgångar

Du behöver göra en informationsklassning och riskbedömning för de system verksamheten har som berörs av migreringen för att kunna prioritera och skydda de mest skyddsvärda informationstillgångarna. Riskinventeringen behöver även kopplas till krav vad gäller lagar och förordningar som påverkar organisationen. I inventeringen bör du även beakta de möjliga ekonomiska förlusterna av att inte vidta åtgärder.

8.3 Inventering av system och data

Även om du arbetar i en prioritetsordning baserad på vilka system som är viktigast att migrera först, baserat på riskanalysen och informationsklassificering, kan detta även påverka mindre viktiga system om de använder samma utrustning eller programvara. Med andra ord behöver du även ha en ordentlig systemkarta som inkluderar beroenden.

8.4 Omvärldsbevakning

Som tidigare nämnts saknas en hel del vitala förutsättningar för att kunna genomföra en full migrering idag. Baserat på den egna inventeringen kommer det att vara nödvändigt att bevaka marknaden för att veta när de standarder, mjuk- och/eller hårdvara du behöver finns tillgängliga på marknaden och det därmed öppnas en möjlighet att genomföra en migrering. Tyvärr finns ingen sammanhållen bevakning för detta som gör att kan du kan få all information från en och samma källa för att få en aktuell bild utan det krävs att aktivt sökande, antingen med hjälp av leverantörer eller på egen hand.

Du behöver beakta att en leverantör som uppger att deras produkt klarar en viss sak, till exempel utfärda certifikat, kanske inte följer standarderna alternativt säger att den klarar av att göra det innan standarderna för detta har slagits fast. Att implementera något som är baserat på en standard/teknik som inte är fastslagen kan leda till att du behöver göra om hela eller delar av migreringen när den färdiga standarden och/eller tekniken är beslutad.

8.5 Migrering

I och med att det finns flera olika algoritmer med olika säkerhetsnivåer att använda bör du börja med att titta på vilka som passar för det avsedda syftet, som i sin tur kan vara beroende på prestanda, kompatibilitet eller nivån på skydd som eftersträvas. Finns möjlighet bör du, i de fall att det finns val, testa hur de olika valen påverkar den informationstillgång som hanteras med avseende på prestanda och kompatibilitet.

Utan ett bra underlag i form av en inventering blir det svårt att fatta beslut om hur du ska gå till väga. Inventeringen behöver du påbörja snarast för att tillse att du har god tid att slutföra migreringen då den sannolikt kommer att ta tid.

De sätt du kan göra migreringen på är att migrera hela eller delar av miljön eller att använda hybridcertifikat och i fallet med symmetrisk kryptering att använda längre nycklar.

Att implementera nya algoritmer innebär att tillse att det finns stöd i alla komponenter som berörs, i applikationer och i hårdvara. Om den applikation du migrerar använder operativsystemets funktionalitet för att kryptera, signera etc. blir det sannolikt enklare att genomföra än om applikationen behöver anpassas.

Som vid alla förändringsprojekt i en it-miljö behöver du säkerställa att du har möjlighet att backa förändringar. Om du misslyckas med att använda kvantdatorsäkra algoritmer av kompabilitetsskäl eller med att kryptera om information så bör det finnas möjligheter att backa tillbaka till senast kända fungerande tidpunkt, beträffande vilka algoritmer du använder eller för det data du har krypterat eller signerat om med ny algoritm. Det innebär till exempel att om du krypterar om data med en annan, längre, nyckel kan du behöva behålla det ursprungliga datat i krypterad form, innan det förstörs på ett säkert sätt, för att tillse att det data som hanterats kan användas korrekt med de nya algoritmerna i den eller de applikationer som det ska användas i.

Bilaga A: Begreppsförklaring

Begrepp	Beskrivning
AES	Symmetrisk algoritm för att kryptera data, finns med tre olika nivåer på nyckellängd 128, 192 och 256 bitar.
Asymmetrisk kryptering	Kryptering av data sker med den publika nyckeln av ett nyckelpar, enbart den med den privata nyckeln kan dekryptera och läsa data.
Birthday attack	Genom att med många försök försöka hitta kollisioner baserat på födelsedagsparadoxen.
CA	Certificate Auhority, tjänst för att utfärda certifikat och därmed en del av ett PKI.
CNSA	Commercial National Security Algorithm Suite, en samling algoritmer som godkänts för användning av NSA för hantering av säkerhetsklassad information.
Digital signatur	Efter att ha signerat data (dokument, fil, installationspaket etc.) kan den användas för att validera att data inte har förändrats.
DNS	Domain Name System, system som översätter hostnamn till IP-adresser.
DNSSEC	Domain Name System Security Extensions, av Internet Engineering Task Force (IETF) godkänd standard för dataintegritet i DNS för att förhindra manipulation av DNS-data.
DSA	Digital Signature Algorithm, familj av kryptografiska algoritmer tänkt för signering av data.
ECC	Elliptic Curve Cryptography, krypteringsalgoritm som bygger på elliptiska kurvor.
Faktorisering	Inom matematiken innebär en faktorisering (faktoruppdelning) att man uttrycker ett objekt som en produkt av flera objekt, eller faktorer.
FTP	File Transfer Protocol, protokoll för att överföring av filer.
FTPS	File Transfer Protocol Secure, FTP med stöd för TLS.
Hash-funktion/ hash-värden	En enkelriktad funktion för att skapa kontrollvärden eller enkelriktad kryptering där data inte kan dekrypteras. Används till exempel för lösenord som då kan lagras hashade i en databas och sedan användas för jämförelse av senare inmatat och hashat indata.

Begrepp	Beskrivning
HSM	Hardware Security Module, enhet för säker lagring av kryptografiskt material. Finns både anslutet via USB, som instickskort till dator eller nätverksansluten.
IETF	Internet Engineering Task Force, standardiseringsorgan för tekniska standarder för IP-protokollet.
IKEv2	Internet Key Exchange version 2, protokoll för att skapa säkerhetsassociationer för IPsec-protokollet.
IPsec	Internet Protocol Security, autentisering och kryptering av data mellan två noder.
ISO	International Organization for Standardization, internationellt standardiseringsorgan för industriell och kommersiell standardisering.
KEM	Key Exchange Module, funktion för att kunna utbyta nyckel tänkt för till exempel symmetrisk kryptering.
Kerberos	Protokoll för autentisering av olika entiteter i ett datornätverk baserat på symmetrisk kryptering.
KMS	Key Management Service, tjänst för att hantera kryptografiskt nyckelmaterial och användningen därav på anslutna klienter.
Kryptering	Att göra data oläsligt för obehöriga, data kan enbart läsas av de som innehar korrekt nyckel för att kunna göra data läsligt igen.
Kvantdatorchip	Kvantdatorprocessor, hjärtat i en kvantdator.
Kvantdatorsäkra algoritmer	Kryptografiska algoritmer som inte är känsliga för Shors eller Grovers algoritmer.
McElice	En KEM-algoritm tänkt för att kunna utbyta symmetriska nycklar.
NIS/NIS2	NIS-direktivet och NIS2-direktivet är EU-direktiv som ställer krav på säkerhet i nätverk och informationssystem.
NIST	National Institute of Standards and Technology, amerikanskt standardiseringsorgan.
NSA	National Security Agency, amerikansk myndighet för signalspaning.
Oauth	Open authorization, öppen standard för åtkomstdelegering.
Oavvislighet	Omöjliggörande av förnekande av att data skickats eller mottagits alternativt datas äkthet.
PGP	Pretty Good Privacy, standard för kryptering av e-post.

Begrepp	Beskrivning
PKI	Public Key Infrastructure, baseras på asymmetrisk kryptering och är en uppsättning av processer, tekniker och policyer som används för att skapa, hantera, distribuera och använda digitala certifikat.
RDP	Remote Desktop Protocol, protokoll för säker nätverkskommunikation som är utformat för fjärrhantering och åtkomst till fjärrskrivbord och applikationer.
SAML	Security Assertion Markup Language, öppen standard för utbyte av autentiserings- och auktorisationsdata.
SCEP	Simple Certificate Enrollment Protocol, protokoll för att distribuera certifikat.
SFTP	Secure File Transfer Protocol, protokoll för att överföra krypterad data mellan dator och lagringsutrymme med hjälp av SSH.
SHA1, SHA2, SHA3, SHAKE	Kryptografiska algoritmer för att skapa hash-värden av data för att kunna kontrollera om data har ändrats.
S/MIME	Standard för kryptering av e-post.
SSH	Secure Shell, protokoll för som används för att ansluta sig säkert mot andra datorer över nätverket.
Symmetrisk kryptering	Kryptering och dekryptering av data sker med samma nyckel.
TCP	Transmission Control Protocol, protokoll för dataöverföring som upprättar en förbindelse mellan två parter för överföring av data.
TLS	Transport Layer Security, kryptografiskt kommunikationsprotokoll för säkert utbyte av krypterad information mellan datorsystem.
TPM-chip	En kryptografisk modul i en dator avsedd för att lagra kryptografiskt nyckelmaterial för exempelvis diskkryptering samt att validera att datorn startar från en betrodd kombination av hård- och mjukvara.
UDP	User Datagram Protocol, protokoll för att skicka data mellan två parter utan en upprättad förbindelse.

Bilaga B: Referenser

EU-kommissionens rekommendation om en samordnad färdplan för genomförandet av övergången till postkvantkryptografi
https://eur-lex.europa.eu/legal-content/SV/TXT/HTML/?uri=OJ:L_202401101

Commercial National Security Algorithm Suite (CNSA) 2.0 and Quantum Computing FAQ
https://media.defense.gov/2022/Sep/07/2003071836/-1/-1/0/CSI_CNSA_2.0_FAQ_.PDF

Post Quantum Government Initiatives by Country and Region
https://www.gsma.com/newsroom/post-quantum-government-initiatives-by-country-and-region/

Guidelines for cryptography (Australian Signals Directorate)
https://www.cyber.gov.au/resources-business-and-government/essential-cybersecurity/ism/cybersecurity-guidelines/guidelines-cryptography

FIPS 203 Module-Lattice-Based Key-Encapsulation Mechanism Standard
https://csrc.nist.gov/pubs/fips/203/final

FIPS 204 Module-Lattice-Based Digital Signature Standard
https://csrc.nist.gov/pubs/fips/204/final

FIPS 205 Stateless Hash-Based Digital Signature Standard
https://csrc.nist.gov/pubs/fips/205/final

NIST SP 800-208 Recommendation for Stateful Hash-Based Signature Schemes
https://csrc.nist.gov/pubs/sp/800/208/final

NIST SP 800-57 Part 1 Rev. 5 Recommendation for Key Management: Part 1 – General
https://csrc.nist.gov/pubs/sp/800/57/pt1/r5/final

Transition to Post-Quantum Cryptography Standards (initial public draft)
https://csrc.nist.gov/pubs/ir/8547/ipd

Internet Engineering Task Force (IETF)
https://datatracker.ietf.org/wg/tls/documents/

wolfSSL Support for Post-Quantum
https://www.wolfssl.com/products/wolfcrypt-post-quantum/

Mixing Preshared Keys in the Internet Key Exchange Protocol Version 2 (IKEv2) for Post-quantum Security
https://datatracker.ietf.org/doc/html/rfc8784

Apple Blog
https://security.apple.com/blog/imessage-pq3/

Microsoft's quantum-resistant cryptography is here
https://techcommunity.microsoft.com/blog/microsoft-security-blog/microsofts-quantum-resistant-cryptography-is-here/4238780

OpenSSL 3.5: Upcoming Release Announcement
https://openssl-library.org/post/2025-02-04-release-announcement-3.5/

SymCrypt-OpenSSL
https://github.com/microsoft/SymCrypt-OpenSSL

wolfSSL Support for Post-Quantum
https://www.wolfssl.com/products/wolfcrypt-post-quantum/

Oqs-provider
https://github.com/open-quantum-safe/oqs-provider

PQC Capabilities Matrix (PQCCM)
https://pkic.org/pqccm/

Significant Changes in JDK 24 Release
https://docs.oracle.com/en/java/javase/24/migrate/significant-changes-jdk-24.html

Europaparlamentets och Rådets direktiv (EU) 2022/2555 av den 14 december 2022 om åtgärder för en hög gemensam cybersäkerhetsnivå i hela unionen, om ändring av förordning (EU) nr 910/2014 och direktiv (EU) 2018/1972 och om upphävande av direktiv (EU) 2016/1148 (NIS 2-direktivet)
https://eur-lex.europa.eu/legal-content/SV/TXT/?uri=OJ:L:2022:333:TOC

Tredjelandsöverföring
https://www.imy.se/verksamhet/dataskydd/det-har-galler-enligt-gdpr/overforing-till-tredje-land/

Recommended cryptographic measures – Securing personal data
https://www.enisa.europa.eu/sites/default/files/publications/Securing%20personal%20data.%20Recommended%20cryptographic%20measures.pdf

Algorithms, key size and parameters report – 2014
https://www.enisa.europa.eu/sites/default/files/publications/Algorithms%2C%20key%20size%20and%20parameters%20report%20%20-%202014.pdf

Enisa Guideline "State of the art"
https://www.teletrust.de/fileadmin/user_upload/2023-05_TeleTrusT_Guideline_State_of_the_art_in_IT_security_EN.pdf

Myndigheten för samhällsskydd och beredskaps föreskrifter (MSBFS 2024:4) om anmälan och identifiering av leverantörer av samhällsviktiga tjänster
https://www.msb.se/contentassets/b15833b9aaa0425ca0c898cc0a120c81/myndigheten-for-samhallsskydd-och-beredskaps-foreskrifter-om-anmalan-och-identifiering-av-leverantorer-av-samhallsviktiga-tjanster-2024-4-pdf.pdf

Statens energimyndighets föreskrifter och allmänna råd (STEMFS 2021:3) om riskanalys och säkerhetsåtgärder för nätverk och informationssystem inom energisektorn
https://energimyndigheten.a-w2m.se/System/TemplateView.aspx?p=Arkitektkopia&id=4429022018d9456486992de94c10bbe0&q=STEMFS%202021%3A3&lstqty=1

Transportstyrelsens föreskrifter och allmänna råd (TSFS 2022:14) om säkerhetsåtgärder för leverantörer av samhällsviktiga tjänster inom transportsektorn
https://www.transportstyrelsen.se/TSFS/TSFS%202022_14.pdf

Europaparlamentets och rådets förordning (EU) 2022/2554 av den 14 december 2022 om digital operativ motståndskraft för finanssektorn (Dora-förordningen)
https://eur-lex.europa.eu/legal-content/SV/TXT/?uri=celex%3A32022R2554

Livsmedelsverkets föreskrifter (LIVSFS 2022:2) om informationssäkerhetsåtgärder för samhällsviktiga tjänster inom sektorn leverans och distribution av dricksvatten
https://www.livsmedelsverket.se/globalassets/om-oss/lagstiftning/dricksvatten---naturl-mineralv---kallv/livsfs-2022-2_t.pdf

Handbok för tillämpningen av Socialstyrelsens föreskrifter och allmänna råd (HSLF-FS 2016:40) om journalföring och behandling av personuppgifter i hälso- och sjukvården
https://www.socialstyrelsen.se/globalassets/sharepoint-dokument/artikelkatalog/handbocker--juridisk-handbok/2017-3-2.pdf

Statens energimyndighets föreskrifter och allmänna råd (STEMFS 2021:3) om riskanalys och säkerhetsåtgärder för nätverk och informationssystem inom energisektorn
https://energimyndigheten.a-w2m.se/System/TemplateView.aspx?p=Arkitektkopia&id=4429022018d9456486992de94c10bbe0&q=STEMFS%202021%3A3&lstqty=1

Transportstyrelsens föreskrifter och allmänna råd (TSFS 2022:14) om säkerhetsåtgärder för leverantörer av samhällsviktiga tjänster inom transportsektorn
https://www.transportstyrelsen.se/TSFS/TSFS%202022_14.pdf

EU-kommissionens genomförandeförordning om fastställande av regler för tillämpningen av NIS 2-direktivet, C(2024) 7151 final (genomförandeförordningen)
https://eur-lex.europa.eu/legal-content/SV/TXT/PDF/?uri=OJ:L_202402690

Post- och telestyrelsens föreskrifter och allmänna råd (PTSFS 2021:3) om säkerhetsåtgärder för samhällsviktiga tjänster inom sektorn digital infrastruktur
https://pts.se/contentassets/a3910642583e472799262c9b7951e073/ptsfs-2021-3-allmanna-rad-om-sakerhetsatg-for-samhallsvikt-tjanst-inom-sektorn-dig-infrastruktur.pdf

PTS Webbplats Vad gäller innan NIS 2-direktivet har genomförts i svensk rätt?
https://pts.se/internet-och-telefoni/central-lagstiftning2/informationssakerhet-for-samhallsviktiga-och-digitala-tjanster-nis/nis2-eu-regler-for-cybersakerhet/vad-galler-innan-nis2-direktivet-har-genomforts-i-svensk-ratt/

Myndigheten för samhällsskydd och beredskaps föreskrifter om säkerhetsåtgärder i informationssystem för statliga myndigheter (MSBFS 2020:7)
https://www.msb.se/siteassets/dokument/regler/forfattningar/msbfs-2020-7-foreskrifter-om-sakerhetsatgarder-i-informationssystem-for-statliga-myndigheter.pdf

prop. 2009/10:138, s. 32 f.
https://www.regeringen.se/contentassets/1d9a0b3fed0d463aacddb3813b333578/okad-kvalitet-vid-lakemedelsforskrivning-prop.-200910138

Myndigheten för samhällsskydd och beredskaps Vägledning för grundläggande kryptering.
https://kryptera.se/assets/uploads/2019/02/vacc88gledning-grundlacc88ggande-kryptering-focc88r-kommentarer.pdf

Nya regler om cybersäkerhet, SOU 2024:18
https://www.regeringen.se/contentassets/1e56bf5cad214fc78eb80d91c11cccb6/nya-regler-om-cybersakerhet-sou-202418.pdf

Kontakta Certezza om ni önskar en detaljerad genomgång av 5.2 Marknadens mognadsgrad.