2026

Nationella rekommendationer för övergången till kvantsäker kryptografi

NATIONELLT
CYBERSÄKERHETSCENTER
En del av FRA



2026
Nationellt cybersäkerhetscenter vid FRA.

Innehåll

Inledning 4

Reglering om användning av kryptografi 5

Tidslinje för övergången 6

Färdigt 2035 7

Färdigt 2030 7

Allriskperspektivet och bedömning av kvantdatorhotet 8

Lyft övergången till ledningsnivån 8

Inventera nuvarande kryptologiska lösningar 8

Krav på inventering av kryptografiska lösningar 9

Ta stöd i informationsklassificeringen 9

Rekommenderade algoritmer och protokoll 10

Kryptografiska algoritmer — Post Quantum Cryptography (PQC) 10

PQC-algoritmer i protokoll 10

Rekommenderade kvantsäkra kryptografiska algoritmer 11

Forum som arbetar med kryptografi 12

Samarbetet mellan tillsynsmyndigheter 12

Samarbetet mellan föreskrivande myndigheter 12

Samarbetsgruppen för nät- och informationssäkerhet i EU (NIS CG) 12

Cybernodens kompetensgemenskap 13

Sektorsvisa samarbetsforum 13

Standardiseringsgruppen på NCSC 13

Standardisering i SIS, CEN/CENELEC och ISO 13

Standardisering i ETSI/3GPP 14

Standardisering i IETF 14

Europeiska gruppen för cybersäkerhetscertifiering - subgrupp kryptografi 14

Litteraturlista 15



Nationella rekommendationer för övergången till kvantsäker kryptografi

Denna skrift är en vägledning från Nationellt cybersäkerhetscenter (NCSC) och syftar till att orientera, informera och ge råd kring ett visst ämne. NCSC:s nationella rekommendationer för övergången till kvantsäker kryptografi riktar sig till de företag och myndigheter som omfattas av cybersäkerhetslagen[1]. Den kan även läsas av andra intresserade aktörer.

Inledning

Vårt digitala samhälle bygger på krypterade lösningar och utgör en central del av cybersäkerheten för alla organisationer. Stark kryptografi är avgörande för att förhindra stöld av känslig eller konfidentiell information, säkerställa informationens integritet och förhindra att obehörig får åtkomst till informationen. En stor del av den kryptografi som används idag riskerar att försvagas eller bli helt underminerad när kvantdatorer med tillräcklig kapacitet utvecklats.

För närvarande är kvantdatorer ännu inte tillräckligt kraftfulla för att forcera de kryptografiska system som används i dag, men utvecklingen går snabbt framåt. Kvantdatorer bedöms att inom tio till tjugo år ha kapacitet att bryta delar av den kryptografi som i dag är allmänt förekommande. Kryptografi som står emot kvantattacker benämns kvantsäker kryptografi (post-quantum cryptography – PQC).

1 Cybersäkerhetslag (2025:1506).

Med kvantdatorernas intåg behöver delar av dagens kryptografi uppdateras. Den enskilt viktigaste aspekten under de närmaste tio åren är hur övergången till kvantsäker kryptografi ska ske.

Verksamheter som vidtar de nödvändiga åtgärderna för att övergå till kvantsäker kryptografi på ett strukturerat sätt kommer vara på god väg att uppfylla cybersäkerhetslagens krav på kryptografi och kryptering. En anledning till detta är att övergången inleds med en fullständig genomlysning av verksamheters nuvarande kryptografiska situation, vilket korrekt uppföljt leder till att svagheter förutom kvantosäker kryptografi också åtgärdas.

Denna vägledning ger en tidplan och annan information för när och hur det ska göras. Vägledningen beskriver närmare tidslinjen för övergången till kvantsäker kryptografi. Övergången behöver vara klar till slutet av 2035 och i vissa känsliga fall redan till slutet av 2030. Vägledningen anger även vilka åtgärder som ska vidtas omedelbart, nämligen rörande att ansvaret för övergången lyfts till ledningsnivån inom organisationen och att inventera de kryptografiska tillgångarna. Nya, kvantsäkra algoritmer och protokoll anges. Alla kryptografiska algoritmer som används idag behöver inte bytas ut. Avslutningsvis presenteras olika forum som arbetar med kryptografi i allmänhet och även med frågan om kvantsäker kryptografi.

Kryptologi
Studien om kryptografi och kryptoanalys samt om metoder för autentisering.

Kryptografi
Metoder för att förvanska meddelanden så att obehöriga inte kan läsa dem. Detta är det operativa utförandet av det som studeras inom kryptologi.

Kryptoanalys
En delvetenskap inom kryptologi som studerar hur man kan forcera krypton utan tillgång till kodnyckeln och en gren av tillämpad matematik.

Reglering om användning av kryptografi
Cybersäkerhetslagen föreskriver att ett antal säkerhetsåtgärder för cybersäkerhet ska vidtas. Särskilt viktigt för denna vägledning är regleringen i cybersäkerhetslagen 2 kap. 3 § om att ”verksamhetsutövare ska vidta lämpliga och proportionella tekniska, driftsrelaterade och organisatoriska åtgärder för att skydda nätverks- och informationssystem som de använder för sin verksamhet eller för att tillhandahålla sina tjänster och systemens fysiska miljö mot incidenter (säkerhetsåtgärder)”. Sådana säkerhetsåtgärder ska åtminstone avse strategier och förfaranden för användning av kryptografi och kryptering.

Lagstiftning om kryptografi i Sverige har tidigare endast funnits för speciella verksamheter med höga säkerhetskrav och specialtillverkade kryptografiska lösningar. Denna färdplan handlar inte om signalskyddet utifrån säkerhetsskyddslagen. Cybersäkerhetslagen driver på mot en högre kryptografisk nivå i samhället i stort. Huvudsakligen sker det genom att klargöra hur ledningen i verksamheter kvalitetssäkrar upphandlandet av solida allmänt tillgängliga kommersiella lösningar.

> **"Verksamhetsutövare ska vidta lämpliga och proportionella tekniska, driftsrelaterade och organisatoriska åtgärder för att skydda nätverks- och informationssystem som de använder för sin verksamhet eller för att tillhandahålla sina tjänster och systemens fysiska miljö mot incidenter."**

EU:s förordning 2022/2554 om digital operativ motståndskraft för finanssektorn (DORA) syftar till att uppnå en hög nivå av operativ motståndskraft inom finanssektorn. DORA kräver att finansiella institut tillämpar lämpliga skyddsåtgärder, inklusive krypteringsmetoder (artiklarna 9 och 15).

Den Europeiska unionen (EU) arbetar med en färdplan till medlemsländerna om hur övergången till kvantsäker kryptografi ska ske. Den första delen[2] publicerades den 11 juni 2025 och innehåller framför allt råd kring tidslinjen för övergången och vilka åtgärder som bör vidtas omedelbart.

Tidslinje för övergången

Det råder bred internationell konsensus kring när övergången till kvantsäker kryptografi ska ske i stora drag. Det är av vikt att övergången sker koordinerat i Sverige och i EU[3] . Länder som Storbritannien[4] och USA[5] har rekommenderat en liknande tidslinje. Kina har inte publicerat några årtal, men de har 2025 utlyst en tävling för kvantsäkra algoritmer[6] som kan användas nationellt[7].

Nu–2030	2030	2035
Organisationens ledning orienterar sig kring övergången till kvantsäker kryptografi och tar fram strategi och plan för övergången	Övergången till kvantsäker kryptografi klar för användarfall med hög risk (t.ex. affärshemligheter, känsliga personuppgifter, hälsodata)	Övergången till kvantsäker kryptografi klar för alla användarfall, även de med lägre risk.
Inventering av organisationens användning av krypton	Implementering av kvantsäker kryptografi i övrigt i organisationen för användarfall med lägre risk.	

2 NIC CG (2025). A Coordinated Implementation Roadmap for the Transition to Post-Quantum Cryptography, Part 1, June 2025. https://digital-strategy.ec.europa.eu/en/policies/nis-cooperation-group

3 NIS CG (2025). A Coordinated Implementation Roadmap for the Transition to Post-Quantum Cryptography, Part 1, June 2025. https://digital-strategy.ec.europa.eu/en/policies/nis-cooperation-group

4 UK NCSC (2025). Timelines for migration to post-quantum cryptography. https://www.ncsc.gov.uk/guidance/pqc-migration-timelines. Se även AIVD 2024. The PQC Migration Handbook.

5 Biden, J. (2022). National Security Memorandum on Promoting United States Leadership in Quantum Computing While Mitigating Risks to Vulnerable Cryptographic Systems. (The White House, Washington, DC), National Security Memorandum 10.

6 ICCS (2025). Announcement on Launching the Next-generation Commercial Cryptographic Algorithms Program (NGCC). Institute of Commercial Cryptography Standards, China.

7 Kinesiska kryptografilagen (2019). http://en.npc.gov.cn.cdurl.cn/2019-10/26/c_674669.htm

Färdigt 2035

Hela övergången till kvantsäker kryptografi ska vara klar till slutet av år 2035. Med det avses att hela processen, även de slutgiltiga utvärderingarna och finjusteringarna, ska vara avklarade.

Tio år kan framstå som en lång tid, men detta kommer att krävas för att kunna upprätta en bra balans mellan att arbeta medvetet och strukturerat framåt med uppdatering av it-miljön, samtidigt som riskerna med kvantdatorer hanteras. Det bör inte krävas större omprioriteringar i organisationers verksamhet, men om arbetet inte kommer i gång i tid så riskerar det att bli mer kostsamt senare.

Att inte genomföra övergången till kvantsäker kryptografi i tid skapar inte bara risker med att krypteringen blir osund, utan riskerar också att en verksamhet inte kan bedriva sitt arbete på grund av att kommunikationen med andra verksamheter slutar att fungera. I slutet av övergången till kvantsäker kryptografi så kommer gamla och olämpliga lösningar att fasas ut. Det betyder exempelvis, att de som inte har genomfört sin övergång i tid inte längre kan korrespondera via e-post med myndigheter som fasat ut gammal kryptografi.

Färdigt 2030

För viss information är det dock bråttom och övergången ska vara klar till slutet av 2030. Det gäller information som är känslig mer än tio år framåt i tiden, exempelvis sådan som rör individers hälsodata.

Bakgrunden till denna kortare tidslinje är att information som skickas på nätet kan sparas undan nu och potentiellt dekrypteras med kvantdatorer i framtiden. Det är ett problem eftersom informationen fortfarande är känslig om tio år.

Hotet att känslig information kan komma att kunna läsas i framtiden är ett reellt problem redan idag och övergången till kvantsäker kryptografi för sådan information bör ske så fort som möjligt. Slutet av 2030 är endast satt som tidsgräns eftersom det bedömts att genomförandet troligtvis inte kan ske tidigare än så.

Om information främst är känslig med avseende på riktighet, snarare än konfidentialitet, så finns vissa möjligheter att säkerställa riktigheten över tid. Upprätthållandet av konfidentialitet bör vanligtvis prioriteras framför autentisering i övergången till kvantsäker kryptografi. Oavsett detta ska dock övergången ske enligt ovan nämnda tidslinje.

Symmetrisk kryptering

Den äldsta typen av kryptering är symmetrisk. Parterna som ska skicka och ta emot meddelandet har tidigare i hemlighet kommit överens om en nyckel som används för att kryptera och dekryptera.

Asymmetrisk kryptering

För ungefär femtio år sedan uppfanns asymmetrisk kryptering. Till skillnad från i symmetrisk kryptering så har parterna som vill utväxla ett meddelande inte tidigare kommit överens om en nyckel i hemlighet. Istället får de utbyta publika nycklar och hålla sina privata nycklar hemliga. Säkerheten hos sådan krypteringg bygger ofta på att vissa matematiska beräkningar tar lång tid att utföra.

Allriskperspektivet och bedömning av kvantdatorhotet

Enligt cybersäkerhetslagen så ska verksamheterna ha ett allriskperspektiv. Att anlägga ett fullständigt allriskperspektiv kan dock vara komplext. Gällande hotet från kvantdatorer skulle det vara nödvändigt att inom varje enskild verksamhet analysera hur kvantdatorerna utvecklas och hotar delar av klassisk kryptografi. Sedan skulle slutsatserna av den hotbilden vägas mot andra i en allriskansats, för att ta fram en tidsplan för övergången till kvantsäker kryptografi.

De flesta verksamheter bör följa den plan för övergången som rekommenderas i detta avsnitt istället för att försöka analysera kvantdatorernas utveckling. Årtalen 2030 och 2035 har valts utifrån en svensk och europeisk kontext[8] där riskerna som hanteras i cybersäkerhetslagen har vägts mot riskerna från utvecklingen av kvantdatorer och hur snabbt man rimligen kan hantera dem på ett proportionellt vis.

Det kan uppstå problem med legacy-system i vilka man inte kan övergå till ny kryptografi. Strategier för att isolera dem, föra över information till nya system, eller att övergå till vissa kvantsäkra klassiska kryptografiska metoder, som exempelvis med distribution av symmetriska nycklar, bör då övervägas.

Lyft övergången till ledningsnivån

För att lyckas med övergången inom tidsramarna angivna i denna vägledning krävs att det strategiska arbetet inleds omedelbart. Det är centralt eftersom alla delar av en verksamhet behöver vara involverade och samverka utifrån olika tidshorisonter samt tilldelas budgetutrymme.

Det är av största vikt att ledningen har en strategisk förståelse för övergången till kvantsäker kryptografi. Samtidigt ska en lärare som skickar e-post till föräldrar inte behöva bekymra sig om att krypteringen är kvantsäker. Däremot behöver den som kravställer upphandlingen av e-postlösningar i kommunal skola och den informationssäkerhetsansvariga kunna förstå vad som krävs i övergången till kvantsäker kryptografi, samt rapportera uppåt i organisationen om hur genomförandet fortskrider.

Ledningen behöver tidigt få rapporter om var i verksamheten det hanteras information känslig nog att övergången behöver vara klar till slutet av 2030. För många myndigheter kommer det handla om att förstå vilka delar av verksamheten som hanterar känslig information och prioritera. Dessa strategiska beslut kräver underlag som bör tas fram snabbt.

Inventera nuvarande kryptologiska lösningar

De nuvarande kryptologiska lösningarna i organisationen behöver inventeras på ett systematiskt sätt. All nuvarande kryptografi behöver inte bytas ut. Exempelvis är det mesta av symmetrisk kryptologi knappt påverkat och det finns utmärkta sätt att distribuera nycklar i och mellan organisationer som inte alls påverkas av kvantdatorer. Mycket behöver dock bytas ut, framförallt den kryptering som bygger på metoder som hotas av Shors algoritm. För att kunna förstå till vilken grad man behöver kvantsäkra sin kryptografi så behöver en ordentlig genomlysning göras.

Därför rekommenderas det att upprätta en förteckning över de kryptografiska funktioner som används. För att göra det så behövs antagligen både att man utgår från sin

8 NIS CG (2025). A Coordinated Implementation Roadmap for the Transition to Post-Quantum Cryptography, Part 1, June 2025. https://digital-strategy.ec.europa.eu/en/policies/nis-cooperation-group

organisations dokumentation av kryptografiska lösningar samt att man använder sig av specialiserad mjukvara för att skanna sina system.

Det är av stor vikt att denna förteckning är ordentligt specifik i algoritmer och protokoll, hur nycklar hanteras samt vilka parametrar som används.

Shors algoritm

På en vanlig dator är det lätt att multiplicera tal snabbt. Exempelvis är 89891*58271=5238038461. Den omvända beräkningen, att faktorisera ett tal, går däremot väldigt långsamt på en vanlig dator. Matematikern Peter Shor beskrev 1994 en algoritm för att faktorisera tal snabbt på en kvantdator. Flera av de mest använda asymmetriska krypteringsalgoritmerna bygger på att faktorisering går långsamt för att hålla krypterade meddelanden hemliga. Därför behöver de bytas ut mot kvantsäker kryptografi.

Krav på inventering av kryptografiska lösningar

Som tidigare beskrivet så ska verksamhetsutövare enligt cybersäkerhetslagen vidta proportionella tekniska, driftsrelaterade och organisatoriska säkerhetsåtgärder för att skydda nätverks- och informationssystem och systemens fysiska miljö mot incidenter. Åtgärderna ska utgå från ett allriskperspektiv och säkerställa en nivå på säkerheten som är lämplig i förhållande till risken. De ska åtminstone avse bland annat strategier och förfaranden för användning av kryptografi samt, vid behov, kryptering.

För att överhuvudtaget kunna ha strategier för användning av kryptografi och kryptering, och dessutom kunna utvärdera hur de används, så måste en verksamhet veta var och hur kryptering används just nu i organisationen. Att upprätta en kryptografisk mjukvaruförteckning är en utmärkt grund för att veta vad säkerheten är byggd på.

I strategin för användning av kryptografi bör det ingå en policy för hur den kryptografiska mjukvaruförteckningen hålls uppdaterad.

Ta stöd i informationsklassificeringen

Parallellt med att de kryptografiska tillgångarna inventeras så bör verksamhetens arbete med informationsklassificering anpassas för att stödja verksamhetsledningens strategiska val och senare till mer operativa val av kryptografiska metoder. En central fråga som behöver besvaras snabbt och rapporteras till verksamhetens ledning är:

Vilken information hanteras som är känslig mer än tio år framåt?

För den typen av information måste övergången till kvantsäker kryptografi ske så fort som möjligt och senast vara klar vid slutet av år 2030.

Grovers algoritm

Att hitta saker i en databas tar lång tid på en vanlig dator. Det kan göras något snabbare med en kvantdator med hjälp av en algoritm som matematikern Lov Grover kom på 1996. Med hjälp av den blir symmetrisk kryptologi något svagare med kvantdatorernas intåg. Men det räcker med att fördubbla nyckellängden för att lösa problemet. Allt längre nycklar behövs ändå gradvis, eftersom vanliga datorer också blir snabbare med tiden. Hotet mot symmetrisk kryptologi från Grovers algoritm är fundamentalt mindre än hotet mot asymmetrisk kryptologi från Shors algoritm och i det närmaste en distraktion i övergången till kvantsäker kryptografi.

Rekommenderade algoritmer och protokoll

Vilka algoritmer som ska användas är för de flesta organisationer en fråga som ligger i framtiden. Man bör först se till att det strategiska arbetet på ledningsnivån fungerar och att en ordentlig inventering av kryptografin i organisationen har gjorts. Först därefter är det av intresse att fundera på algoritmer. Detta avsnitt riktar sig främst till de som senare ska leverera mjukvara till it-system i verksamheter, inte för verksamheterna själva. Det kan också vara av intresse för myndigheter med föreskriftsrätt på området (såsom Försvarets radioanstalt, Försvarsmakten, Post- och telestyrelsen och Säkerhetspolisen).

De flesta verksamheter behöver inte direkt hantera vilka kryptografiska algoritmer som används eller hur de implementeras. Att överskatta en verksamhets kryptografiska kompetens är en reell risk i sig. För en mycket stor grupp användningsfall kommer uppgraderingen att ske osynligt, i och med att browsers och mobiltelefoner uppdateras och man kommer kunna anta att kommunikationen skyddas av lämpliga, kvantsäkra algoritmer. Man bör i första hand köpa mjukvara från leverantörer som har en gedigen förståelse för cybersäkerhet och ställa krav i upphandlingar.

Kryptografiska algoritmer — Post Quantum Cryptography (PQC)

De kvantsäkra kryptografiska algoritmerna måste vara standardiserade i öppna transparenta processer och redan användas i stor skala internationellt av företag och myndigheter. Idag uppfylls det endast av fem standarder antagna av det amerikanska National Institute of Standards and Technology (NIST).

PQC-algoritmer i protokoll

De PQC-algoritmer som rekommenderats ovan ska användas inom ramen för protokoll som till exempel TLS. Det är alltså inte tänkt att man själv implementerar algoritmerna i mjukvara, utan att man använder bibliotek med implementerade protokoll. I dessa bibliotek finns ofta val av olika PQC-algoritmer och parametrar, det är via det valet som man specificerar vilken PQC-algoritm som används.

Det är inte bara själva PQC-algoritmerna som ska vara standardiserade och valda enligt beskrivningen ovan, utan också hur de används i protokoll behöver vara standardiserat på ett internationellt accepterat vis. Huvudsakligen ska detta ske genom att använda standarder antagna av the Internet Engineering Task Force (IETF), men för vissa användarfall så har the European Telecommunications Standards Institute (ETSI) och mobilstandardiseringsorganet 3GPP protokollstandarder som är att föredra. Utifrån vilken sektor man verkar i och regelverk som ska följas så förväntas det inte vara svårt att hitta lämpliga protokoll från år 2026.

Hybridisering är en teknik för att kombinera en av de nuvarande kryptografiska algoritmerna, som inte är kvantsäker, med en av de nya kvantsäkra algoritmerna, på ett sådant sätt att säkerheten hos hybriden är lika hög som hos den av de ingående algoritmerna som har den högsta säkerheten.

NCSC, liksom EU:s färdplan för övergången till kvantsäker kryptografi[9], rekommenderar användning av standardiserade och testade hybridlösningar, när det är genomförbart och lämpligt. Precis som för PQC-algoritmerna ovan ska sådana hybridlösningar vara implementerade i protokoll som i sin tur är standardiserade och testade.

Rekommenderade kvantsäkra kryptografiska algoritmer

Funktion	Typ	Rekommenderad	Inte längre rekommenderad
Nyckelutbyte/ Nyckelenkapsulering	Asymmetrisk	ML-KEM(1)	ECDH(2) RSA(3)
Digital signatur - tillståndslös	Asymmetrisk	ML-DSA(4) SLH-DSA(5)	ECDSA EdDSA RSA(6)
Digital signatur - tillståndsfull	Asymmetrisk	LMS XMSS(7)	

(1) FIPS 203. Module-Lattice-Based Key-Encapsulation Mechanism Standard. National Institute of Standards and Technology (NIST). https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.203.pdf

(2) NIST SP 800-56A. Recommendation for Pair-Wise Key-Establishment Schemes Using Discrete Logarithm Cryptography (NIST) https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-56Ar3.pdf

(3) NIST SP 800-56B. Recommendation for Pair-Wise Key Establishment Using Integer Factorization Cryptography (NIST) https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-56Br2.pdf

(4) FIPS 204. Module-Lattice-Based Digital Signature Standard. National Institute of Standards and Technology (NIST). https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.204.pdf

(5) FIPS 205. Stateless Hash-Based Digital Signature Standard. National Institute of Standards and Technology (NIST). https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.205.pdf

(6) FIPS 186-5. Digital Signature Standard (DSS). (NIST) https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.186-5.pdf

(7) NIST SP 800-208. Recommendation for Stateful Hash-Based Signature Schemes. National Institute of Standards and Technology (NIST). https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-208.pdf

Transport Layer Security

TLS är ett protokoll för att säkra kommunikationen på datornätverk som Internet. Det är standardiserat av IETF och bygger på protokoll från slutet av 90-talet. En del av TLS handlar om kryptologi och de bitarna uppdateras regelbundet, exempelvis för att kvantsäkras under de senaste åren.

9 NIC CG (2025). A Coordinated Implementation Roadmap for the Transition to Post-Quantum Cryptography, Part 1, June 2025. https://digital-strategy.ec.europa.eu/en/policies/nis-cooperation-group

Forum som arbetar med kryptografi

För att samordna och harmonisera användandet av kvantsäker kryptografi krävs även att myndigheter och företag deltar i forum för att bygga upp samhällets kompetens tillsammans. Det sker redan i flera forum. Här kan företag hitta myndigheter i sina sektorer som arbetar för att utveckla cybersäkerhetsarbetet och kvantsäker kryptografi.

Eftersom lösningar för kvantsäker kryptografi håller på att standardiseras handlar hälften av de omnämnda forumen om standardisering. Inom standardisering sker ett arbete för att driva området tekniskt framåt och det är därför utmärkt att delta för att informera sig, men också för att påverka hur tekniken utformas och hur den sen används i samhället. Cybersäkerhetslagen genomför EU:s NIS 2-direktiv[10] som uppmuntrar användandet av standarder för åtgärder som kryptografi och kryptering.

Samarbetet mellan tillsynsmyndigheter

Vilka myndigheter som har tillsynsansvar framgår av cybersäkerhetsförordningen (2025:1507). Tillsynen är sorterad enligt respektive sektor och från 1 juli 2026 är Försvarets radioanstalt genom NCSC gemensam kontaktpunkt för tillsynsmyndigheterna enligt Artikel 8.3 i NIS 2-direktivet och ska leda ett samarbetsforum där tillsynsmyndigheterna ingår som ska underlätta samordning och åstadkomma en effektiv och likvärdig tillsyn.. Eftersom en hel del verksamheter under cybersäkerhetslagen även fortsatt förväntas kunna vara under tillsyn av flera myndigheter på en gång, är det av stor vikt att kryptografin harmoniseras.

Samarbetet mellan föreskrivande myndigheter

Cybersäkerhetsförordningen anger att Post- och telestyrelsen (PTS) och (från 1 juli 2026) Försvarets radioanstalt (FRA) har rätt att meddela föreskrifter kopplat till cybersäkerhetslagen.

Samarbetsgruppen för nät- och informationssäkerhet i EU (NIS CG)

Samarbetsgruppen för nät- och informationssäkerhet i EU (NIS CG) upprättades i och med NIS-direktivets införande. Från 1 juli 2026 representerar FRA genom NCSC i NIS CG. Det finns ett antal undergrupper för specifika tekniska frågor. Den som berör kvantsäker kryptologi kallas NIS CG WS PQC och FRA bistår med expertis från svensk sida i gruppen.

Huvuduppgiften för NIS CG WS PQC är att skriva en färdplan för hur hela EU ska gå över till kvantsäker kryptologi och att därmed bistå medlemsstaterna i utarbetandet av deras nationella färdplaner som utgår från kommissionens rekommendation om en samordnad färdplan för genomförandet av övergången till postkvantkryptografi[11]. Starkt knutet till det är frågor relaterade till hur kryptografi används inom 5G/6G, i vilket PTS deltar, samt hur det sen i praktiken ska certifieras, i vilket Försvarets materielverk (FMV) deltar. Alla dessa myndigheter sitter också i NCSC:s standardiseringsgrupp.

10 Europaparlamentets och rådets direktiv (EU) 2022/2555 av den 14 december 2022 om åtgärder för en hög gemensam cybersäkerhet i hela unionen

11 Kommissionens rekommendation av den 11.4.2024 om en samordnad färdplan för genomförandet av övergången till postkvantkryptografi. https://digital-strategy.ec.europa.eu/sv/library/recommendation-coordinated-implementation-roadmap-transition-post-quantum-cryptography

Cybernodens kompetensgemenskap

Cybernoden är Sveriges nationella kompetensgemenskap inom cybersäkerhetsforskning och innovation. De har ca. 300 medlemmar, varav deltagande myndigheter för närvarande är Myndigheten för digital förvaltning (DIGG), FMV, FRA, Integritetsskyddsmyndigheten (IMY), Myndigheten för civilt försvar (MCF), Myndigheten för totalförsvarsanalys (MTFA), Pensionsmyndigheten, Riksbanken, Statens fastighetsverk, Strålsäkerhetsmyndigheten, Totalförsvarets forskningsinstitut (FOI), Universitets- och högskolerådet (UHR), Vetenskapsrådet, Vinnova samt 12 högskolor och universitet, sex regioner och fyra kommuner.

Cybernoden har 12 temagrupper, varav en är fokuserad på kryptologi.

Sektorsvisa samarbetsforum

Samhället kan delas upp i sektorer som har olika behov av kvantsäker kryptografi. Det är dock viktigt att inte överdriva skillnaderna, e-post behöver skickas mellan verksamheter i olika sektorer. Men det finns specifika problemställningar, regelverk, traditioner och unika problem med legacy-system som gör samarbete inom sektorerna värdefullt.

Det är viktigt att samarbetsformer för övergången till kvantsäker kryptografi inom sektorerna kommer i gång så snart som möjligt. Ett exempel inom området hälso- och sjukvård är projektet ”Framtidens ekosystem för kvantsäkra hälsodata”, vilket koordineras av RISE med finansiering från Vinnova[12].

Standardiseringsgruppen på NCSC

NCSC har en grupp för standardiseringsfrågor inom cybersäkerhet med särskilt fokus på elektronisk kommunikation. Gruppen leds av PTS och är öppen för NCSC:s samverkansmyndigheter. I arbetet med att ta fram vägledningen för övergången till kvantsäker kryptografi i EU[13] så utgör standardiseringsgruppen på NCSC basen för samverkan mellan dessa myndigheter.

Standardisering i SIS, CEN/CENELEC och ISO

Det Svenska institutet för standarder (SIS) har kommittén TK 318 Informationssäkerhet, cybersäkerhet och integritetsskydd. I den pågår ett aktivt samarbete mellan 59 företag och organisationer i att vidareutveckla standarder inom både hur ledningssystem för informationssäkerhet sätts upp och hur riskhanteringsåtgärder som kryptografi tillämpas.

Myndigheterna som deltar är Arbetsmiljöverket, Ekobrottsmyndigheten, FMV, FRA, Försvarsmakten, MCF, DIGG, PTS, Skolverket, Styrelsen för Ackreditering & Teknisk Kontroll (SWEDAC), Trafikverket, Transportstyrelsen samt en region och två högskolor. Företag som deltar sträcker sig från små specialiserade konsultbolag med några få anställda till globala svenska bolag med miljardomsättning.

Kommittén SIS TK 318 har en arbetsgrupp AG 21 Kryptografi som leds av FRA. I den är utvecklingen av standarder för kvantsäker kryptografi central.

SIS koordinerar det svenska arbetet i den europeiska standardiseringsorganisationen CEN/CENELEC, där framför allt ett stort arbete sker med harmoniserade standarder beställda av EU. Det finns inga beställningar på harmoniserade standarder av kvantsäker

12 Framtidens ekosystem för kvantsäkra hälsodata. www.ri.se/sv/kvantteknologi/projekt/framtidens-ekosystem-for-kvantsakra-halsodata Läst den 2 februari 2026

13 NIS CG (2025). A Coordinated Implementation Roadmap for the Transition to Post-Quantum Cryptography, Part 1, June 2025. https://digital-strategy.ec.europa.eu/en/policies/nis-cooperation-group

kryptografi från unionen för tillfället och med tanke på kommissionens program för 2024–2029 så kan ingen sådan förväntas inom närtid. Det finns dock en stor mängd lagda beställningar på harmoniserade standarder, inom exempelvis AI, där cybersäkerhet är relevant och kryptografi kommer in i periferin.

Den mesta standardisering av kvantsäker kryptografi sker direkt på internationell nivå i ISO, vilket också koordineras av SIS utgående från den tekniska expertisen i arbetsgruppen TK 318 / AG 21.

Standardisering i ETSI/3GPP

European Telecommunications Standards Institute (ETSI) är ett europeiskt standardiseringsorgan inom telekommunikation. ETSI är medlem i 3GPP, som standardiserar 5G/6G. ETSI är drivande i att ta fram europeiska standarder inom cybersäkerhet och var tidiga med hur kvantsäker kryptografi ska användas. ETSI ordnar uppskattade konferenser för europeisk samverkan inom cybersäkerhet. Svenska myndigheter som deltar är DIGG, FRA, MCF, Polisen, PTS, Säkerhetspolisen och Trafikverket. Näringslivet finns representerat via exempelvis Advenica, Ericsson, Husqvarna, Scania, Sectra och Telia.

Standardisering i IETF

Det öppna internationella samarbetsforum med kanske störst inflytande på hur kryptografi används i verkligheten är the Internet Engineering Task Force (IETF). Detta gäller även kvantsäker kryptografi. IETF utvecklar bland annat TLS-protokollet som används för nästan all internettrafik. Standardiseringen drivs av individer som i praktiken representerar sina företag eller organisationer. För de med ett djupt tekniskt engagemang i kvantsäker kryptografi är IETF centralt och cybersäkerhetsmyndigheter från flera länder deltar.
På IETF-mötet våren 2025 så ordnade Ericsson och FRA en session för att främja internationell dialog mellan industri och myndigheter inom kvantsäker kryptografi.

Europeiska gruppen för cybersäkerhetscertifiering – subgrupp kryptografi

Försvarets materielverk (FMV) är Sveriges representant i den Eurpeiska gruppen för cybersäkerhetscertifiering (ECCG) som ska bistå med genomförande av EU:s cybersäkerhetsakt och det europeiska ramverket för cybersäkerhetscertifiering.

En undergrupp till ECCG behandlar frågor om kryptografi och ger genom ECCG ut den vägledande skriften ”Agreed cyrptographic mechanisms” (ACM)

NCSC:s rekommendationer

1. Inventera den kryptografi som finns inom organisationen.
2. Säkerställ att organisationens ledning har en strategisk förståelse för vad övergången till kvantsäker kryptografi innebär för organisationen.
3. Skapa en strategi och plan för övergången till kvantsäker kryptografi för er organisation, inklusive för den mest kritiska informationen, och vilka leverantörsberoenden som finns.
4. Följ tidslinjen för övergången till kvantsäker kryptografi med slutlig övergång senast 2035 och 2030 för särskilt känslig information.

Litteraturlista

AIVD 2024. The PQC Migration Handbook.

Biden, J. (2022). National Security Memorandum on Promoting United States Leadership in Quantum Computing While Mitigating Risks to Vulnerable Cryptographic Systems. (The White House, Washington, DC), National Security Memorandum 10.

Cybersäkerhetslag (2025:1506). Försvarsdepartementet.

Europaparlamentets och rådets direktiv (EU) 2016/1148 av den 6 juli 2016 om åtgärder för en hög gemensam nivå på säkerhet i nätverks- och informationssystem i hela unionen (EUT L 194, 19.7.2016, ss. 1-30)

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) (EUT L 333, 27.12.2022, ss. 80–152).

FIPS 186-5. Digital Signature Standard (DSS). (NIST)

FIPS 203. Module-Lattice-Based Key-Encapsulation Mechanism Standard. National Institute of Standards and Technology (NIST).

FIPS 204. Module-Lattice-Based Digital Signature Standard. National Institute of Standards and Technology (NIST).

FIPS 205. Stateless Hash-Based Digital Signature Standard. National Institute of Standards and Technology (NIST).

ICCS (2025). Announcement on Launching the Next-generation Commercial Cryptographic Algorithms Program (NGCC). Institute of Commercial Cryptography Standards, China.

Kinesiska kryptografilagen (2019).

Kommissionens rekommendation av den 11.4.2024 om en samordnad färdplan för genomförandet av övergången till postkvantkryptografi.

NIC CG (2025). A Coordinated Implementation Roadmap for the Transition to Post-Quantum Cryptography, Part 1, June 2025.

NIST SP 800-56A. Recommendation for Pair-Wise Key-Establishment Schemes Using Discrete Logarithm Cryptography (NIST)

NIST SP 800-56B. Recommendation for Pair-Wise Key Establishment Using Integer Factorization Cryptography (NIST)

NIST SP 800-208. Recommendation for Stateful Hash-Based Signature Schemes. National Institute of Standards and Technology (NIST).

UK NCSC (2025). Timelines for migration to post-quantum cryptography.

För mer information och kontakt
www.ncsc.se och ncsc@ncsc.se

Nationellt cybersäkerhetscenter NCSC

NATIONELLT
CYBERSÄKERHETSCENTER
En del av FRA