EUROPA-
KOMMISSIONEN

Bruxelles, den 11.4.2024
C(2024) 2393 final

KOMMISSIONENS HENSTILLING

af 11.4.2024

om en koordineret gennemførelseskøreplan for overgangen til kvantesikker kryptografi

KOMMISSIONENS HENSTILLING

af 11.4.2024

om en koordineret gennemførelseskøreplan for overgangen til kvantesikker kryptografi

EUROPA-KOMMISSIONEN HAR —

under henvisning til traktaten om Den Europæiske Unions funktionsmåde, særlig artikel 292,

under henvisning til Europa-Parlamentets og Rådets direktiv (EU) 2022/2555 af 14. december 2022 om foranstaltninger til sikring af et højt fælles cybersikkerhedsniveau i hele Unionen, om ændring af forordning (EU) nr. 910/2014 og direktiv (EU) 2018/1972 og om ophævelse af direktiv (EU) 2016/1148[1] (NIS 2-direktivet), og

ud fra følgende betragtninger:

(1) Databeskyttelse og sikring af følsom kommunikation er afgørende for samfundet, økonomien, sikkerheden og velstanden i Unionen. Cybersikkerhed er af strategisk betydning i indsatsen for at gøre "Europa klar til den digitale tidsalder"[2] og er et centralt mål for politikprogrammet for det digitale årti[3].

(2) Både strategien for EU's sikkerhedsunion[4] og EU's strategi for cybersikkerhed[5] fremhæver kryptering som en central teknologi til at opnå modstandsdygtighed og teknologisk suverænitet og til at opbygge operationel kapacitet til forebyggelse af cyberangreb. Kryptering er afgørende i den digitale verden for at sikre digitale systemer og transaktioner, beskytte en række grundlæggende rettigheder og sikre forsvarskapaciteter. En række lande og private enheder deltager i kapløbet om udvikling af kvantedatabehandlingskapacitet og nye potentielle fordele, hvilket udgør en trussel mod de nuværende kryptografiske standarder. Disse standarder spiller en central rolle med hensyn til at sikre datafortrolighed og -integritet, beskytte følsom kommunikation og understøtte væsentlige elementer i netværkssikkerheden.

(3) Den fremtidige potentielle udvikling af kvantecomputere, der er i stand til at bryde de nuværende krypteringsformer, gør det nødvendigt for Europa at søge stærkere sikkerhedsforanstaltninger, der kan sikre beskyttelsen af følsom kommunikation og den langsigtede integritet af fortrolige oplysninger, dvs. ved hurtigst muligt at overgå til kvantesikker kryptografi. Denne nye type kryptografi vil fjerne de kendte sårbarheder i nutidens asymmetriske kryptografi og øge robustheden over for truslen fra ondsindet brug af kvantecomputere.

(4) Kommissionen har finansieret forskning i og udvikling af kvantesikker kryptografi i over ti år i erkendelse af den potentielle trussel, som kvantedatabehandling udgør for nutidens kryptografi med offentlig nøgle.

---

1 EUT L 333 af 27.12.2022, s. 80.
2 COM(2020) 67 final.
3 Europa-Parlamentets og Rådets afgørelse (EU) 2022/2481 af 14. december 2022 om etablering af politikprogrammet for det digitale årti 2030 (EUT L 323 af 19.12.2022, s. 4).
4 COM(2020) 605 final.
5 JOIN(2020) 18 final.

(5) Medlemsstaterne bør overveje hurtigst muligt at migrere deres nuværende digitale infrastrukturer og tjenester for offentlige myndigheder og andre kritiske infrastrukturer til kvantesikker kryptografi, hvilket indebærer et grundlæggende skift i kryptografiske algoritmer, protokoller og systemer. Som fremhævet i Kommissionens nylige hvidbog "How to master Europe's digital infrastructure needs?" (foreligger pt. ikke på dansk), kræver dette en koordineret indsats med inddragelse af statslige organer, standardiseringsorganer, interessenter fra industrien, forskere og fagfolk inden for cybersikkerhed.

(6) Med denne henstilling opfordrer Kommissionen medlemsstaterne til at udvikle en omfattende strategi for indførelse af kvantesikker kryptografi for at sikre en koordineret og synkroniseret overgang blandt de forskellige medlemsstater og deres offentlige sektorer. Strategien bør fastlægge klare mål, milepæle og tidsfrister og til sidst føre til fastlæggelsen af en fælles gennemførelseskøreplan for kvantesikker kryptografi. Dette bør føre til, at der i hele Unionen indføres kvantesikker kryptografi i de offentlige myndigheders eksisterende systemer og kritiske infrastrukturer via hybride ordninger, der kan kombinere kvantesikker kryptografi med eksisterende kryptografiske tilgange eller med kvantenøglefordeling ("Quantum Key Distribution").

(7) Med henblik på en effektiv overgang til kvantesikker kryptografi bør den koordinerede gennemførelseskøreplan for kvantesikker kryptografi indeholde en liste over foranstaltninger, som medlemsstaterne skal træffe, herunder overvejelser om algoritmer til kvantesikker kryptografi, med en klar tidsplan for de forskellige faser og milepæle, der skal nås, under hensyntagen til deres indbyrdes afhængighed samt de interessenter, der skal inddrages.

(8) For at sikre en harmoniseret gennemførelse af kvantesikker kryptografi i hele Unionen er det vigtigt at udvikle fælles europæiske standarder og udvikle en ramme for identifikation og udvælgelse af algoritmer til kvantesikker kryptografi, der skal anvendes i digitale netværk og tjenester i hele Unionen. Med aktiv deltagelse af EU-finansierede forskere støtter Unionen allerede udviklingen og afprøvningen af mulige algoritmer til kvantesikker kryptografi med henblik på standarder i internationale udvælgelsesprocesser til kvantesikker kryptografi. I denne henstilling fra Kommissionen opfordres medlemsstaterne til på EU-plan at arbejde tæt sammen med Unionens cybersikkerhedseksperter, NIS-samarbejdsgruppen og Den Europæiske Unions Agentur for Cybersikkerhed (ENISA) om evaluering og udvælgelse af passende algoritmer til kvantesikker kryptografi og deres vedtagelse som EU-standarder med henblik på en harmoniseret indførelse i hele Unionen.

(9) Medlemsstaterne og Unionen bør fortsat samarbejde aktivt med deres internationale strategiske partnere om udviklingen af internationale standarder inden for kvantesikker kryptografi med henblik på at sikre kommunikationssystemernes interoperabilitet i fremtiden.

(10) Når medlemsstaterne er nået til enighed herom, bør den koordinerede gennemførelseskøreplan for kvantesikker kryptografi tjene som skabelon for fastlæggelsen af de nationale planer for overgangen til kvantesikker kryptografi eller, hvor der allerede findes nationale planer, tilpasning af disse planer efter den fælles koordinerede gennemførelseskøreplan for kvantesikker kryptografi.

(11) For at sikre, at der gøres fremskridt med hensyn til målene i denne henstilling, agter Kommissionen at overvåge de foranstaltninger, der træffes som reaktion på henstillingen, nøje. Medlemsstaterne opfordres derfor til på Kommissionens anmodning at forelægge Kommissionen alle relevante oplysninger, som de med

rimelighed kan forventes at fremlægge, for at sikre en sådan overvågning. På grundlag af de således indhentede oplysninger og alle andre tilgængelige oplysninger vil Kommissionen vurdere virkningerne af denne henstilling og afgøre, om der er behov for yderligere foranstaltninger, herunder forslag til bindende EU-retsakter.

(12) Denne henstilling om kvantesikker kryptografi bygger på de politiske mål, der er fastsat i EU's strategi for cybersikkerhed, om at forbedre sikkerheden og modstandsdygtigheden fra første til sidste led i Unionens digitale infrastrukturer og tjenester for offentlige myndigheder og andre kritiske infrastrukturer; henstillingen bidrager ligeledes til at opfylde målene med det digitale indre marked og den fælles meddelelse om en europæisk økonomisk sikkerhedsstrategi 10919/23[6]; henstillingen tager også højde for risiciene for den fysiske sikkerhed og cybersikkerhed i forbindelse med kritisk infrastruktur samt de risici, der er konstateret i forbindelse med den nyligt gennemførte risikovurdering af kvanteteknologier[7]. Den overholder de grundlæggende rettigheder og de principper, som navnlig anerkendes i EU's charter om grundlæggende rettigheder (artikel 7, 8 og 11) og den europæiske menneskerettighedskonvention (artikel 8 og 10), som indebærer positive forpligtelser for regeringerne til at minimere risikoen for ulovlig adgang til og kontrol med oplysninger, hvilket gør det nødvendigt at beskytte og fremme kryptografiske teknologier —

VEDTAGET DENNE HENSTILLING:

1. ANVENDELSESOMRÅDE OG MÅL

Formålet med denne henstilling er at fremme overgangen til kvantesikker kryptografi med henblik på beskyttelse af offentlige myndigheders digitale infrastrukturer og tjenester og andre kritiske infrastrukturer i Unionen ved at sætte medlemsstaterne i stand til at:

(1) fastlægge en "koordineret gennemførelseskøreplan for kvantesikker kryptografi" med henblik på at synkronisere medlemsstaternes indsats for at udforme og gennemføre nationale overgangsplaner og samtidig sikre interoperabiliteten på tværs af grænserne

(2) støtte evalueringen og udvælgelsen af relevante EU-algoritmer til kvantesikker kryptografi med hjælp fra cybersikkerhedseksperter og fremme yderligere indførelse af disse algoritmer som EU-standarder, der bør gennemføres i hele Unionen som led i den koordinerede gennemførelseskøreplan for kvantesikker kryptografi

(3) træffe passende og forholdsmæssige foranstaltninger til at forberede denne overgang.

2. EN KOORDINERET GENNEMFØRELSESKØREPLAN MED HENBLIK PÅ OVERGANGEN TIL KVANTESIKKER KRYPTOGRAFI

(4) I denne henstilling opfordres medlemsstaterne til at koordinere deres indsats på EU-plan gennem et særligt forum for medlemsstaterne. Med henblik herpå anbefaler Kommissionen, at medlemsstaterne udnytter de eksisterende strukturer på EU-plan på cybersikkerhedsområdet og opretter en undergruppe under NIS-samarbejdsgruppen. En sådan undergruppe kan omfatte repræsentanter for nationale sikkerhedsagenturer og cybersikkerhedseksperter, navnlig fra nationale cybersikkerhedsmyndigheder og ENISA. Undergruppen kan indbyde repræsentanter

6 https://data.consilium.europa.eu/doc/document/ST-10919-2023-INIT/da/pdf.
7 JOIN(2023) 20 final.

for relevante interessenter til at deltage i sit arbejde, f.eks. rådgivende organer i offentlige organisationer, erhvervslivet, tjenesteudbydere og operatører, med henblik på at indsamle input og udveksle oplysninger om overgangen til kvantesikker kryptografi inden for offentlige myndigheders digitale infrastrukturer og tjenester og andre kritiske infrastrukturer i forskellige sektorer, koordinere deres indsats på nationalt plan og udvikle den koordinerede gennemførelseskøreplan for kvantesikker kryptografi i overensstemmelse med Unionens konkurrenceregler og EU's databeskyttelseslovgivning.

(5) Denne undergruppe om kvantesikker kryptografi bør overveje passende, effektive og forholdsmæssige foranstaltninger til at definere og koordinere udviklingen af den koordinerede gennemførelseskøreplan for kvantesikker kryptografi. Undergruppen opfordres til at indlede drøftelser med andre relevante organer såsom Europol, NATO eller andre for at undgå dobbeltarbejde og sikre en sammenhængende tilgang til håndtering af nye udfordringer.

(6) Med henblik herpå opfordres medlemsstaterne til kort efter offentliggørelsen af denne henstilling at nedsætte en sådan undergruppe om kvantesikker kryptografi i henhold til Kommissionens gennemførelsesafgørelse (EU) 2017/179 og til at udpege ekspertrepræsentanter, der bør arbejde tæt sammen med Kommissionen, og hvis opgave det bør være at fastlægge og udvikle den koordinerede gennemførelseskøreplan for kvantesikker kryptografi.

(7) Den koordinerede gennemførelseskøreplan for kvantesikker kryptografi bør foreligge to år efter offentliggørelsen af denne henstilling; derefter bør de enkelte medlemsstater udvikle og yderligere tilpasse deres planer for overgangen til kvantesikker kryptografi i overensstemmelse med principperne i den koordinerede gennemførelseskøreplan for kvantesikker kryptografi.

3. FORANSTALTNINGER PÅ EU-PLAN

(8) Det samlede arbejde vil blive overvåget og vurderet regelmæssigt af Kommissionen i samarbejde med medlemsstaternes ekspertrepræsentanter.

(9) Med henblik herpå kan Kommissionen anmode medlemsstaternes repræsentanter om at forelægge alle relevante oplysninger, som de med rimelighed kan forventes at forelægge, for at sikre overvågningen af de fremskridt, der gøres med udarbejdelsen af den koordinerede gennemførelseskøreplan for kvantesikker kryptografi, og foranstaltningernes effektivitet.

(10) På grundlag af disse og alle andre tilgængelige oplysninger vil Kommissionen vurdere de planlagte foranstaltninger og samarbejdet i netværket af repræsentanter for medlemsstaterne og afgøre, om der er behov for yderligere foranstaltninger, herunder forslag til bindende EU-retsakter.

4. REVURDERING

(11) Medlemsstaterne bør samarbejde med Kommissionen om at vurdere virkningerne af denne henstilling senest tre år efter dens offentliggørelse med henblik på at fastlægge passende skridt fremover. Ved vurderingen bør der tages hensyn til resultatet af arbejdet i undergruppen om kvantesikker kryptografi med deltagelse af nationale eksperter.

Udfærdiget i Bruxelles, den 11.4.2024.

På Kommissionens vegne
Thierry BRETON
Medlem af Kommissionen

BEKRÆFTET KOPI
For generalsekretæren

Martine DEPREZ
Direktør
Beslutningstagning og kollegialitet
EUROPA-KOMMISSIONEN