COMISIA
EUROPEANĂ

Bruxelles, 11.4.2024
C(2024) 2393 final

RECOMANDAREA COMISIEI

din 11.4.2024

privind o foaie de parcurs coordonată pentru punerea în aplicare a tranziției către criptografia postcuantică

RECOMANDAREA COMISIEI

din 11.4.2024

privind o foaie de parcurs coordonată pentru punerea în aplicare a tranziției către criptografia postcuantică

COMISIA EUROPEANĂ,

având în vedere Tratatul privind funcționarea Uniunii Europene, în special articolul 292,

având în vedere Directiva (UE) 2022/2555 a Parlamentului European și a Consiliului din 14 decembrie 2022 privind măsuri pentru un nivel comun ridicat de securitate cibernetică în Uniune, de modificare a Regulamentului (UE) nr. 910/2014 și a Directivei (UE) 2018/1972 și de abrogare a Directivei (UE) 2016/1148[1] (Directiva NIS 2),

întrucât:

(1) Protejarea datelor și securizarea comunicațiilor sensibile sunt de o importanță determinantă pentru societatea, economia, securitatea și prosperitatea Uniunii. Securitatea cibernetică este de importanță strategică în construirea unei Europe pregătite pentru era digitală[2] și face parte din obiectivele-cheie ale programului de politică privind deceniul digital[3].

(2) Atât Strategia UE privind uniunea securității[4], cât și Strategia de securitate cibernetică a UE[5] pun accentul pe criptare ca tehnologie-cheie pentru dobândirea rezilienței și a suveranității tehnologice și pentru consolidarea capacității operaționale de prevenire a atacurilor cibernetice. De fapt, criptarea este esențială pentru lumea digitală, care permite securizarea sistemelor și a tranzacțiilor digitale, protejarea unei serii întregi de drepturi fundamentale, precum și asigurarea capabilităților de apărare. Mai multe țări și entități private s-au angajat într-o veritabilă cursă pentru dezvoltarea de capacități de calcul cuantic și pentru deblocarea de noi oportunități care pot oferi diverse avantaje, fapt ce reprezintă o amenințare la adresa standardelor criptografice actuale. Aceste standarde joacă un rol esențial în asigurarea confidențialității și a integrității datelor, în protejarea comunicațiilor sensibile și în sprijinirea elementelor esențiale ale securității rețelelor.

(3) Având în vedere faptul că, în viitor, este posibil să apară calculatoare cuantice capabile să descifreze criptarea actuală, Europa trebuie să obțină garanții mai puternice, de natură să asigure protecția comunicațiilor sensibile și integritatea pe termen lung a informațiilor confidențiale, mai precis prin trecerea la criptografia postcuantică cât mai curând posibil. Acest nou tip de criptografie va elimina vulnerabilitățile cunoscute ale

[1] JO L 333, 27.12.2022, p. 80.
[2] COM(2020) 67 final.
[3] Decizia (UE) 2022/2481 a Parlamentului European și a Consiliului din 14 decembrie 2022 de instituire a programului de politică pentru 2030 privind deceniul digital (JO L 323, 19.12.2022, p. 4).
[4] COM(2020) 605 final.
[5] JOIN(2020) 18 final.

criptografiei asimetrice actuale și va spori robustețea împotriva amenințărilor reprezentate de utilizarea rău-intenționată a calculatoarelor cuantice.

(4) Comisia finanțează de peste zece ani activități de cercetare și dezvoltare din domeniul criptografiei postcuantice, recunoscând amenințarea potențială pe care informatica cuantică o reprezintă pentru criptografia cu cheie publică folosită în prezent.

(5) Statele membre ar trebui să aibă în vedere cât mai curând posibil migrarea către criptografia postcuantică a actualelor infrastructuri și servicii digitale destinate administrațiilor publice și altor infrastructuri critice, determinând o schimbare fundamentală la nivel de algoritmi, protocoale și sisteme criptografice. După cum s-a subliniat în recenta Carte albă a Comisiei intitulată „Cum se pot gestiona nevoile Europei în materie de infrastructură digitală?”, este necesar ca, în acest scop, agențiile guvernamentale, organismele de standardizare, părțile interesate din industrie, cercetătorii și profesioniștii din domeniul securității cibernetice să își unească forțele.

(6) Prezenta recomandare a Comisiei încurajează statele membre să elaboreze o strategie cuprinzătoare pentru adoptarea criptografiei postcuantice, în vederea asigurării unei tranziții coordonate și sincronizate între diferitele state membre și sectoarele lor publice. Strategia ar trebui să definească obiective, obiective intermediare și termene clare care să permită întocmirea unei foi de parcurs comune pentru punerea în aplicare a criptografiei postcuantice. Finalitatea ar trebui să fie implementarea, în întreaga Uniune, a tehnologiilor criptografice postcuantice în sistemele existente ale administrației publice și în infrastructurile critice actuale, prin intermediul unor sisteme hibride care să poată combina criptografia postcuantică cu abordările criptografice existente sau cu distribuția cuantică a cheilor.

(7) Pentru o tranziție eficace către criptografia postcuantică, foaia de parcurs pentru punerea în aplicare coordonată a criptografiei postcuantice ar trebui să prezinte lista acțiunilor care trebuie întreprinse de statele membre, inclusiv luarea în considerare a algoritmilor de criptografie postcuantică, și să prevadă un calendar clar pentru diferitele etape și obiective intermediare care trebuie parcurse și atinse și ținând seama de interdependențele acestora, precum și de părțile interesate care trebuie să fie implicate.

(8) Pentru o punere în aplicare armonizată a criptografiei postcuantice în întreaga Uniune, este esențial să se elaboreze standarde europene comune și să se elaboreze un cadru pentru identificarea și selectarea algoritmilor de criptografie postcuantică care urmează să fie introduși în rețelele și serviciile digitale din întreaga Uniune. Prin participarea activă a cercetătorilor cărora le acordă finanțare, Uniunea sprijină deja dezvoltarea și testarea de algoritmi de criptografie postcuantică „candidați” la statutul de standarde în cadrul proceselor internaționale de selecție a criptografiei postcuantice. Prezenta recomandare a Comisiei încurajează statele membre să colaboreze îndeaproape la nivelul UE cu experții Uniunii în materie de securitate cibernetică, cu Grupul de cooperare NIS și cu Agenția Uniunii Europene pentru Securitate Cibernetică (ENISA) în ceea ce privește evaluarea și selectarea algoritmilor de criptografie postcuantică adecvați și adoptarea acestora ca standarde ale UE în vederea punerii în aplicare armonizate în întreaga Uniune.

(9) Statele membre și Uniunea ar trebui să continue cooperarea activă cu partenerii strategici internaționali în ceea ce privește elaborarea de standarde internaționale în domeniul criptografiei postcuantice, pentru a asigura interoperabilitatea comunicațiilor în viitor.

(10) După ce va fi aprobată de statele membre, foaia de parcurs pentru punerea în aplicare coordonată a criptografiei postcuantice ar trebui să servească drept model pentru elaborarea planurilor naționale de tranziție către criptografia postcuantică sau, în cazul în care există deja planuri naționale, pentru alinierea acestora la foaia de parcurs comună pentru punerea în aplicare coordonată a criptografiei postcuantice.

(11) Pentru a se asigura că se avansează în direcția îndeplinirii obiectivelor prezentei recomandări, Comisia intenționează să monitorizeze îndeaproape măsurile întreprinse ca răspuns la prezenta recomandare. De aceea, pentru a asigura această monitorizare, statele membre sunt încurajate să transmită Comisiei, la cererea acesteia, toate informațiile relevante despre care se poate preconiza în mod rezonabil că vor trebui să le comunice. Pe baza informațiilor astfel obținute și a tuturor celorlalte informații disponibile, Comisia va evalua efectele prezentei recomandări și va stabili dacă sunt necesare măsuri suplimentare, inclusiv propunerea de acte legislative ale Uniunii cu caracter obligatoriu.

(12) Prezenta recomandare privind criptografia postcuantică se bazează pe obiectivele de politică stabilite în Strategia de securitate cibernetică a UE, și anume îmbunătățirea securității și a rezilienței de la un capăt la altul a infrastructurilor și digitale ale Uniunii și a serviciilor destinate administrațiilor publice, precum și a altor infrastructuri critice; aceasta urmărește îndeplinirea obiectivelor pieței unice digitale și ale Comunicării comune privind „Strategia europeană pentru securitate economică” 10919/23[6] și examinează riscurile pentru securitatea fizică și cibernetică a infrastructurilor critice, precum și riscurile identificate în cadrul evaluării riscurilor pentru tehnologiile cuantice[7], efectuată recent. Recomandarea respectă drepturile fundamentale și se conformează principiilor recunoscute în special în Carta drepturilor fundamentale a UE (articolele 7, 11 și 8) și în Convenția europeană a drepturilor omului (articolele 8 și 10), care presupun, din partea guvernelor, obligații pozitive de a reduce la minimum riscul de acces la informații și de control ilegal asupra acestora, ceea ce necesită protejarea și promovarea tehnologiilor criptografice,

ADOPTĂ PREZENTA RECOMANDARE:

1. SFERA DE APLICARE ȘI OBIECTIVELE

Prezenta recomandare are drept scop promovarea tranziției către criptografia postcuantică pentru protecția infrastructurilor și a serviciilor digitale destinate administrațiilor publice și a altor infrastructuri critice din Uniune, permițând statelor membre:

(1) să stabilească o „foaie de parcurs pentru punerea în aplicare coordonată a criptografiei postcuantice”, cu scopul de a sincroniza eforturile întreprinse de statele membre pentru a elabora și a pune în aplicare planuri naționale de tranziție, concomitent cu asigurarea interoperabilității transfrontaliere;

(2) să sprijine evaluarea și selectarea algoritmilor de criptografie postcuantică relevanți ai UE cu ajutorul experților în securitate cibernetică și să continue adoptarea algoritmilor de acest tip cu titlu de standarde ale Uniunii care ar trebui să fie puse în aplicare în întreaga Uniune în cadrul foii de parcurs pentru punerea în aplicare coordonată a criptografiei postcuantice;

(3) să ia măsuri adecvate și proporționale pentru a se pregăti în vederea acestei tranziții.

---

6 https://data.consilium.europa.eu/doc/document/ST-10919-2023-INIT/ro/pdf

7 JOIN(2023) 20 final

2. FOAIA DE PARCURS COORDONATĂ PENTRU PUNEREA ÎN APLICARE A TRANZIȚIEI CĂTRE CRIPTOGRAFIA POSTCUANTICĂ

(4) Prezenta recomandare încurajează statele membre să își coordoneze acțiunile la nivelul Uniunii prin intermediul unui forum al statelor membre dedicat acestei tranziții. În acest scop, Comisia recomandă statelor membre să profite de structurile existente la nivelul Uniunii în domeniul securității cibernetice și să înființeze un subgrup al Grupului de cooperare NIS. Din acest subgrup ar putea face parte reprezentanți ai agențiilor naționale de securitate și experți în securitate cibernetică, în special din cadrul autorităților naționale de securitate cibernetică și al ENISA. Subgrupul poate invita să participe la lucrările sale reprezentanți ai părților interesate relevante, de exemplu, reprezentanți ai organismelor consultative ale organizațiilor publice, ai industriei, furnizori de servicii și operatori, cu scopul de a strânge contribuții și de a face schimb de informații cu privire la tranziția infrastructurilor și a serviciilor digitale destinate administrațiilor publice și a altor infrastructuri critice către criptografia postcuantică în diferite sectoare, de a coordona eforturile depuse la nivel național și de a elabora foaia de parcurs coordonată pentru punerea în aplicare a criptografiei postcuantice, în conformitate cu normele în materie de concurență ale Uniunii și cu legislația în materie de protecție a datelor a Uniunii.

(5) Acest subgrup pentru criptografia postcuantică ar trebui să ia în considerare măsuri adecvate, eficace și proporționale pentru definirea și coordonarea elaborării foii de parcurs coordonate pentru punerea în aplicare a criptografiei postcuantice. Subgrupul pentru criptografia postcuantică este încurajat să poarte discuții cu alte organisme relevante, cum ar fi Europol, NATO sau altele, pentru a evita suprapunerea eforturilor și a asigura o abordare coerentă a provocărilor emergente.

(6) În acest scop, la scurt timp după publicarea prezentei recomandări, statele membre sunt invitate să instituie acest subgrup pentru criptografia postcuantică în temeiul Deciziei de punere în aplicare (UE) 2017/179 a Comisiei și să numească reprezentanți experți care să lucreze în strânsă cooperare cu Comisia și să aibă sarcina de a defini și de a elabora foaia de parcurs pentru punerea în aplicare coordonată a criptografiei postcuantice.

(7) Foaia de parcurs pentru punerea în aplicare coordonată a criptografiei postcuantice ar trebui să fie disponibilă la doi ani de la publicarea prezentei recomandări, care va fi urmată de elaborarea și adaptarea în continuare a planurilor de tranziție a criptografiei postcuantice ale fiecărui stat membru în parte, în conformitate cu principiile stabilite în Foaia de parcurs pentru punerea în aplicare coordonată a criptografiei postcuantice.

3. ACȚIUNI LA NIVELUL UNIUNII

(8) Activitatea generală va fi monitorizată și evaluată periodic de către Comisie, în cooperare cu reprezentanții experților din statele membre.

(9) În acest scop, Comisia poate solicita reprezentanților statelor membre să prezinte toate informațiile pertinente, în legătură cu care se poate preconiza în mod rezonabil că vor trebui să le comunice, pentru a asigura monitorizarea progreselor înregistrate în elaborarea acestei foi de parcurs pentru punerea în aplicare coordonată a criptografiei postcuantice și monitorizarea eficacității acestor măsuri.

(10) Pe baza acestor informații și a tuturor celorlalte informații disponibile, Comisia va evalua măsurile concepute și funcționarea rețelei de reprezentanți ai statelor membre

și va stabili dacă sunt necesare acțiuni suplimentare, inclusiv propuneri de acte obligatorii de drept al Uniunii.

4. REVIZUIRE

(11) Statele membre ar trebui să coopereze cu Comisia pentru a evalua efectele prezentei recomandări în termen de maximum trei ani de la publicarea acesteia, cu scopul de a stabili căile adecvate de urmat. Această evaluare ar trebui să țină seama de rezultatul activității subgrupului pentru criptografia postcuantică al experților naționali.

Adoptată la Bruxelles, 11.4.2024

Pentru Comisie,
Thierry BRETON
Membru al Comisiei

COPIE LEGALIZATĂ
Pentru Secretarul General

Martine DEPREZ
Director
Procesul decizional și colegialitatea
COMISIA EUROPEANA