|  |  |  |
| --- | --- | --- |
|  | **Asamblea Mundial de Normalización de las Telecomunicaciones (AMNT-24)**Nueva Delhi, 15-24 de octubre de 2024 |  |
|  |
|  |  |
| SESIÓN PLENARIA | Addéndum 42 alDocumento 37-S |
|  | 22 de septiembre de 2024 |
|  | Original: inglés |
|  |
| Administraciones miembro de la Telecomunidad Asia-Pacífico |
| PROYECTO DE NUEVA RESOLUCIÓN [APT-PQC] – Promoción de la implementación de la criptografía poscuántica y migración a esta tecnología. |
|  |
|  |

|  |  |
| --- | --- |
| **Resumen:** | El presente documento contiene la propuesta de nueva Resolución de la AMNT sobre la promoción de la implantación de la criptografía poscuántica y la migración a esta tecnología. |
| **Contacto:** | Sr. Masanori KondoSecretario GeneralTelecomunidad Asia-Pacífico | Correo-e: aptwtsa@apt.int |

Introducción

Los algoritmos criptográficos son la base fundamental de las redes para crear confianza y seguridad en la utilización de las TIC.

Una vez que se disponga de ordenadores cuánticos con capacidad criptográfica relevante, la mayoría de los algoritmos de clave pública existentes y sus protocolos asociados serán vulnerables a ataques elaborados desde estos ordenadores. La amenaza cuántica proviene de los ordenadores cuánticos, los cuales, con su excepcional potencia computacional, tienen la capacidad de superar a los algoritmos criptográficos ampliamente utilizados, incluidos RSA y ECC (Elliptic Curve Cryptography). En la actualidad se está desarrollando un conjunto de algoritmos criptográficos, denominados algoritmos de criptografía poscuántica (PQC), que se consideran seguros desde un punto de vista cuántico o de resistencia cuántica, lo que significa que se espera que sigan siendo seguros incluso en presencia de ordenadores cuánticos con capacidad criptográfica relevante.

En la Resolución se reconoce la definición de PQC de la CE 17, que se refiere a los algoritmos clásicos de resistencia cuántica.

En la actualidad, la infraestructura de redes de comunicaciones de confianza se basa en algoritmos criptográficos tradicionales como Diffie-Hellman y RSA, que son vulnerables a las amenazas cuánticas. Por consiguiente, la transición de las redes TIC a una infraestructura fiable de resistencia cuántica es crucial antes de la llegada de los ordenadores cuánticos.

Aunque con la PQC se aprovecha la infraestructura existente y se ofrece una solución de seguridad cuántica costoeficaz y bien establecida, las organizaciones necesitarán mucho tiempo y recursos para migrar completamente a esta tecnología.

En vista de ello, es inminente la necesidad de que las CE del UIT-T tomen la iniciativa en la labor de normalización con miras a promover la implementación de la criptografía poscuántica y la migración a esta tecnología en las redes de telecomunicaciones/TIC.

Por otra parte, la CE 17 del UIT-T acordó el "uso de la criptografía poscuántica" como un nuevo tema para el próximo periodo de estudios (2025-2028) en su proceso de preparación de la AMNT‑24.

Propuesta

Sobre la base de lo expuesto anteriormente, las Administraciones Miembros de la APT proponen a la AMNT‑24 que estudie la posibilidad de establecer una nueva Resolución de la AMNT sobre la promoción de la implementación de la criptografía poscuántica y la migración a esta tecnología.

ADD APT/37A42/1

PROYECTO DE NUEVA RESOLUCIÓN [APT-PQC] (Nueva delhi, 2024)

Promoción de la implementación de la criptografía poscuántica
y migración a esta tecnología

*(Nueva Delhi, 2024)*

La Asamblea Mundial de Normalización de las Telecomunicaciones (Nueva Delhi, 2024),

recordando

*a)* la Resolución 130 (Rev. Bucarest, 2022) de la Conferencia de Plenipotenciarios sobre el fortalecimiento del papel de la UIT en la creación de confianza y seguridad en la utilización de las tecnologías de la información y la comunicación;

*b)* la Resolución 50 (Rev. Ginebra, 2022) de la AMNT sobre ciberseguridad;

*c)* la Resolución 57/239 de la Asamblea General de las Naciones Unidas sobre la creación de una cultura mundial de la ciberseguridad;

*d)* la Resolución 78/287 de la Asamblea General de las Naciones Unidas sobre el Año Internacional de la Ciencia y la Tecnología Cuánticas (2025),

considerando

*a)* la importancia de los algoritmos criptográficos para la creación de confianza y seguridad en el uso de las tecnologías de la información y la comunicación (TIC);

*b)* que la llegada de la tecnología de computación cuántica con capacidad criptográfica relevante pondrá en peligro muchos de los algoritmos criptográficos actuales, especialmente los de criptografía de clave pública, que se utilizan ampliamente para proteger la información digital;

*c)* que los algoritmos criptográficos de los que dependen las infraestructuras de telecomunicaciones/TIC se utilizan en todo el mundo en componentes de muchos sistemas diferentes de comunicaciones, procesamiento y almacenamiento de datos;

*d)* que una vez que se disponga de acceso a ordenadores cuánticos con capacidad criptográfica relevante, la mayoría de los algoritmos de clave pública existentes y sus protocolos asociados serán vulnerables a los ataques desde ordenadores cuánticos;

*e)* que los algoritmos de PQC pueden utilizarse en la infraestructura existente y aprovechar la experiencia del sistema para implementar una solución cuántica segura;

*f)* que las aplicaciones típicas de PQC pueden incluir todos los sectores, como las IMT‑2020/IMT‑2030 y DLT;

*g)* la necesidad de colaboración internacional e intercambio de información para hacer frente a las amenazas a la seguridad provenientes de ordenadores cuánticos con capacidad criptográfica relevante;

*h)* que la función de la UIT se centra en la implementación de la PQC y en la migración a esta tecnología para crear seguridad y confianza en la utilización de la infraestructura de telecomunicaciones/TIC, no en la normalización de algoritmos o protocolos de PQC;

*i)* que la PQC puede ayudar a desarrollar infraestructuras de confianza seguras frente a computadores cuánticos o tradicionales, y puede interoperar con los protocolos y las redes de comunicación existentes;

*j)* que el paso de los sistemas criptográficos clásicos existentes a unos sistemas basados en PQC que puedan resistir los ataques de la computación cuántica es un proyecto costoso y a largo plazo. En la actualidad, ya hay muchos sectores verticales en el mundo que están estudiando la aplicación de la PQC y la migración a esta tecnología, y es necesario que el sector de las telecomunicaciones/TIC comience a prepararse inmediatamente ante esta tendencia;

*k)* el proceso de migración a la PQC es extremadamente complejo y llevará muchos años completarlo, ya que requiere la sustitución de algoritmos criptográficos, la actualización de protocolos, esquemas, componentes, infraestructuras, etc., criptográficos por tecnologías criptográficas de seguridad cuántica;

*l)* en la migración a la PQC puede incluirse el diseño y desarrollo de mecanismos para actualizar de manera flexible los sistemas criptográficos y la actualización constante de los sistemas de información de aplicaciones criptográficas con miras a facilitar la implementación de futuros algoritmos de PQC;

*m)* la evaluación de la seguridad de los algoritmos de PQC es un trabajo continuo del Instituto Nacional de Normas y Tecnología (NIST),

considerando además

*a)* que la Recomendación UIT-T X.1811 proporciona directrices de seguridad para la aplicación de algoritmos de seguridad cuántica en los sistemas IMT-2020, que TR.qs-dlt proporciona directrices para que el sistema de DLT de seguridad cuántica proteja esta tecnología de libro mayor y que al mismo tiempo la CE 17 del UIT-T está preparando dos informes técnicos, uno de ellos de orientación sobre el uso de la criptografía avanzada basada en PQC (*Guidance on use of advanced cryptography based on PQC*);

*b)* que el JTC ISO/CEI 1/SC 27/GT 2 y el Instituto Europeo de Normas de Telecomunicación (ETSI) están trabajando en la normalización de la criptografía poscuántica (PQC) y en el intercambio de información sobre esta tecnología;

*c)* que el National Cybersecurity Center of Excellence (NCCoE) del NIST está iniciando el desarrollo de prácticas para facilitar la migración del conjunto actual de algoritmos criptográficos de clave pública a algoritmos de sustitución resistentes a ataques informáticos cuánticos,

observando

*a)* que el UIT-T debería desempeñar un papel rector en la elaboración de normas para crear confianza y garantizar la seguridad en la utilización de las TIC;

*b)* que se está llevando a cabo un proceso iniciado por el NIST para solicitar, evaluar y normalizar uno o más algoritmos criptográficos de clave pública de resistencia cuántica;

*c)* que el NIST ha publicado normas para tres algoritmos PQC;

*d)* que el IETF cuenta con un grupo de trabajo sobre el uso de protocolos poscuánticos (pquip) para intentar superar problemas de ingeniería y transición en materia de PQC aprovechando la experiencia relevante relacionada con el trabajo en el IETF y en la implementación activa de PQC en protocolos IETF, incluidos IPSec, TLS y OpenPGP;

*e)* que el JTC ISO/CEI 1/ SC 27/GT 2, *Cryptography and Security Mechanisms* (Mecanismos de criptografía y seguridad), está trabajando en la normalización de los algoritmos de PQC seleccionados por el NIST;

*f)* que el grupo de trabajo *Quantum-Safe Cryptography* (Criptografía de seguridad cuántica) del ETSI ha publicado un informe técnico en el que se definen estrategias de migración y recomendaciones para sistemas de seguridad cuántica;

*g)* que la Comisión de Estudio 17 del UIT-T es la Comisión de Estudio rectora sobre seguridad dentro del UIT-T que se encarga tanto de coordinar las actividades de seguridad dentro del UIT-T y con otros organismos de normalización y foros, como de desarrollar marcos para mejorar la colaboración,

reconociendo

*a)* que la definición de la PQC de la CE 17 se refiere a los algoritmos clásicos de resistencia cuántica;

*b)* que el desarrollo de un marco para evaluar y comprender los despliegues de sistemas criptográficos existentes es esencial para que las organizaciones planifiquen la migración del conjunto actual de algoritmos criptográficos de clave pública a los algoritmos de PQC resistentes a ataques informáticos cuánticos;

*c)* que tres flujos de trabajo paralelos son importantes en la migración a la PQC: el de los algoritmos (normalización de algoritmos de PQC), los protocolos (habilitación de la PQC para protocolos de seguridad) y los sistemas (integración de la PQC en sistemas y procesos),

resuelve

1 que se sigan elaborando las Recomendaciones necesarias para promover la implantación de la PQC y la migración a esta tecnología dentro de las redes de telecomunicaciones/TIC;

2 que se elaboren nuevas Recomendaciones para promover la necesidad de construir una infraestructura fiable basada en PQC y planes de acción para la migración a esta tecnología, los cuales se utilizarán en la infraestructura de telecomunicaciones/TIC una vez que las organizaciones más adecuadas para realizar esa labor hayan desarrollado los algoritmos, protocolos y normas necesarios;

3 que se elabore un marco para ayudar a las organizaciones a evaluar sus actuales implantaciones de sistemas criptográficos y a planificar la migración a la PQC,

encarga a la Comisión de Estudio 17 como Comisión de Estudio Rectora sobre seguridad y a otras Comisiones de Estudio pertinentes del Sector de Normalización de las Telecomunicaciones de la UIT

1 evaluar las Recomendaciones presentes, las que se revisen y las nuevas relativas a la implementación de la PQC y la migración a esta tecnología;

2 seguir elaborando Recomendaciones y otras publicaciones del UIT-T sobre directrices y prácticas idóneas, que ayudarán a las organizaciones a prepararse para la implantación de la PQC y la migración a esta tecnología;

3 colaborar con las partes interesadas del sector para recabar ideas y prácticas idóneas con miras a promover la implantación de la PQC y la migración a esta tecnología en las redes de telecomunicaciones/TIC;

4 colaborar con otras Comisiones de Estudio del UIT-T y otras organizaciones para la aplicación de la presente Resolución;

5 alentar a divulgar los avances pertinentes relacionados con la implementación de la PQC y la migración a esta tecnología en las redes de telecomunicaciones/TIC;

6 formular recomendaciones al Grupo Asesor de Normalización de las Telecomunicaciones sobre la manera de hacer frente a las cuestiones ajenas al mandato de las Comisiones de Estudio,

encarga al Grupo Asesor de Normalización de las Telecomunicaciones

impulsar un esfuerzo concertado entre las Comisiones de Estudio pertinentes para acelerar la labor de normalización a fin de promover la implementación de la PQC y la migración esta tecnología en las redes de telecomunicaciones/TIC,

encarga al Director de la Oficina de Normalización de las Telecomunicaciones

1 prestar la asistencia necesaria para establecer planes de acción que promuevan la implantación de la PQC y la migración a esta tecnología en la infraestructura de telecomunicaciones/TIC y alentar la participación y las contribuciones de los Estados Miembros, los Miembros de Sector, los Asociados y las Instituciones Académicas;

2 organizar uno o más talleres para reunir recomendaciones y aportaciones sobre este asunto de un gran número de interesados;

3 prestar apoyo al Director de la Oficina de Desarrollo de las Telecomunicaciones (BDT) para que ayude a los Estados Miembros a promover la implantación de la PQC y la migración a esta tecnología en la infraestructura de telecomunicaciones/TIC,

invita a los Estados Miembros, Miembros de Sector, Asociados e Instituciones Académicas

1 a presentar contribuciones para la elaboración de Recomendaciones y otras publicaciones del UIT-T sobre directrices y prácticas idóneas para promover la implantación de la PQC y la migración a esta tecnología en la infraestructura de telecomunicaciones/TIC;

2 a facilitar talleres educativos y sesiones de formación para promover la implementación de la PQC y la migración a esta tecnología en las redes de telecomunicaciones/TIC.

\_\_\_\_\_\_\_\_\_\_\_\_\_\_