|  |  |  |
| --- | --- | --- |
|  | World Telecommunication Standardization Assembly (WTSA-24)New Delhi, 15–24 October 2024 |  |
|  |
|  |  |
| PLENARY MEETING | Addendum 42 toDocument 37-E |
|  | 22 September 2024 |
|  | Original: English |
|  |
| Asia-Pacific Telecommunity Member Administrations |
| draft NEW RESOLUTION [APT-PQC] - PROMOTING IMPLEMENTATION OF AND MIGRATION TO POST-QUANTUM CRYPTOGRAPHY |
|  |
|  |

|  |  |
| --- | --- |
| **Abstract:** | This document contains the proposal for a new WTSA Resolution on promoting the implementation of and migration to post-quantum cryptography. |
| **Contact:** | Mr. Masanori Kondo Secretary GeneralAsia-Pacific Telecommunity | E-mail: aptwtsa@apt.int  |

Introduction

Cryptographic algorithms are key foundation to networks for building confidence and security in the use of ICTs.

Once access to cryptographically relevant quantum computers becomes available, most existing public-key algorithms and their associated protocols will be vulnerable to quantum computer-based attacks. The quantum threat comes from quantum computers, with their exceptional computational power, which have the potential to break widely used cryptographic algorithms, including RSA and ECC (Elliptic Curve Cryptography). A set of cryptographic algorithms are being developed, referred to as Post-Quantum Cryptography (PQC) that are believed to be “quantum-safe” or “quantum-resistant”, meaning that they are expected to remain safe even in the presence of cryptographically relevant quantum computers.

The resolution recognizes that SG17 definition of PQC which refers to quantum resistant classical algorithms.

Currently, the trust infrastructure of communication networks is based on traditional cryptographic algorithms such as Diffie-Hellman and RSA, which are vulnerable to quantum threats. Therefore, the transition of ICT networks to a quantum-resistant trust infrastructure becomes crucial before the advent of quantum computers.

While PQC leverages existing infrastructure and offers a cost-effective and well-established quantum-safe solution, it will take significant time and resources for organisations to fully migrate to PQC.

In view of this, there is impending requirement for ITU-T SGs to actively take up standardization work for promoting implementation of and migration to post-quantum cryptography in telecommunication/ICT networks.

In addition, ITU-T SG17 agreed on “use of post quantum cryptography” as an emerging topic for the next study period (2025-2028) in its WTSA-24 preparation process.

Proposal

Based on the background above, APT Member Administrations propose WTSA-24 to consider establishment of new WTSA Resolution on promoting the implementation of and migration to post‑quantum cryptography.

ADD APT/37A42/1

DRAFT NEW RESOLUTION [APT-PQC] (New Delhi, 2024)

Promoting implementation of and migration to Post-Quantum Cryptography

(New Delhi, 2024)

The World Telecommunication Standardization Assembly (New Delhi, 2024)

recalling

*a)* Resolution 130 (Rev. Bucharest, 2022) of the Plenipotentiary Conference, on strengthening the role of ITU in building confidence and security in the use of information and communication technologies;

*b)* Resolution 50 (Rev. Geneva, 2022) of this assembly, on cybersecurity;

*c)* United Nations General Assembly (UNGA) Resolution 57/239, on the creation of a global culture of cybersecurity;

*d)* UNGA Resolution 78/287, on the International Year of Quantum Science and Technology, 2025,

considering

*a)* the importance of cryptographic algorithms for building confidence and ensuring security in the use of information and communication technologies (ICTs);

*b)* the advent of cryptographically-relevant quantum computing technology will compromise many of the current cryptographic algorithms, especially public-key cryptography, which is widely used to protect digital information;

*c)* cryptographic algorithms on which telecommunication/ICT infrastructures depend are used worldwide in components of many different communications, processing, and storage systems;

*d)* once access to cryptographically-relevant quantum computers becomes available, most existing public-key algorithms and their associated protocols will be vulnerable to quantum computer-based attacks;

*e*) PQC algorithms can be used in existing infrastructure and leverage system expertise to implement a quantum safe solution;

*f*) typical applications of PQC may include all sectors such as IMT-2020/IMT-2030, and DLT;

*g*) the necessity for international collaboration and information sharing to address threats to security from cryptographically relevant quantum computers;

*h)* ITU’s role focuses on the implementation of PQC and its migration to build security and confidence in the use of Telecommunication/ICT infrastructure, not standardizing PQC algorithms or protocols;

*i)* PQC can help develop trust infrastructure that are secure against both quantum and classical computers, and can interoperate with existing communications protocols and networks;

*j*) migrating the existing classical cryptographic systems to PQC based systems that can resist quantum computing attacks is a long-term and costly project. At present, there are already many vertical industries in the world exploring the application of and migration to PQC, and it is necessary for the telecommunication/ICT industry to prepare for this tendency right now;

*k*) the PQC migration process is extremely complex and will take many years to complete it as it requires replacing cryptographic algorithms, updating cryptographic protocols, schemes, components, infrastructure, etc., into quantum-safe cryptographic technologies;

*l*) the migration to PQC may include the design and development of mechanisms to flexibly update cryptographic systems and the iterative updating of cryptographic application information systems in order to make implementation of future PQC algorithms easier;

*m*) the security assessment of the PQC algorithms is continuous work by NIST (National Institute of Standards and Technology),

considering further

*a*) Recommendation ITU-T X.1811 provides security guidelines for applying quantum‑safe algorithms in IMT-2020 systems, TR.qs-dlt provides guidelines for Quantum-Safe DLT System to secure DLT, while two Technical Reports including “Guidance on use of advanced cryptography based on PQC” are under development of ITU-T SG17;

*b*) ISO/IEC JTC 1/SC 27/WG 2 and European Telecommunications Standards Institute (ETSI) are working on standardizing post quantum cryptography (PQC) and exchanging information on PQC;

*c*) NIST National Cybersecurity Center of Excellence (NCCoE) is initiating the development of practices to ease the migration from the current set of public-key cryptographic algorithms to replacement algorithms that are resistant to quantum computer-based attacks,

noting

*a)* that the ITU‑T should play a leading role in the development of standards for building confidence and ensuring security in the use of ICTs;

*b)* that a process initiated by NIST is under way to solicit, evaluate, and standardize one or more quantum-resistant public-key cryptographic algorithms;

*c)* that the NIST has released standards for three PQC algorithms;

*d)* that IETF has a Working Group on Post-Quantum Use In Protocols (pquip) to address PQC engineering and transition issues and experience relevant to work in the IETF and actively implementing PQC in IETF protocols including IPSec, TLS, and OpenPGP;

*e)* that ISO/IEC JTC 1/SC 27/WG 2, *Cryptography and Security Mechanisms*, is working on standardization for PQC algorithms selected by NIST;

*f*) that ETSI Quantum-Safe Cryptography (QSC) working group has released a Technical Report defining migration strategies and recommendations for quantum-safe schemes;

*g)* that ITU-T Study Group 17 is the lead study group on security within ITU‑T, assigned with the task of coordinating security activities within ITU‑T and with other standards-development organizations and forums, and developing frameworks to improve collaboration,

recognizing

*a)* that SG17 definition of PQC refers to quantum resistant classical algorithms;

*b)* that the development of a framework to assess and understand existing cryptographic system deployments is essential for organisations to plan their migration from the current set of public-key cryptographic algorithms to PQC algorithms that are resistant to quantum computer‑based attacks;

*c)* that three parallel workstreams are important in the PQC migration for algorithms (standardization of PQC algorithms), protocols (making the security protocols PQC-enabled), and systems (integration of PQC into systems and processes),

resolves

1 to continue to develop the necessary Recommendations to promote PQC implementation and migration within telecommunication/ICT network;

2 to develop new Recommendations to promote the need to build trusted infrastructure based on PQC and action plans for migration to PQC to be used in telecommunication/ICT infrastructure once the necessary algorithms, protocols, and standards have been developed by the organisations most suited to do that work;

3 to develop a framework to assist organisations in assessing their existing cryptographic systems deployments and planning for migration to PQC,

instructs Study Group 17 as the lead study group on security and other relevant study groups of the ITU Telecommunication Standardization Sector

1 to evaluate existing, evolving and new Recommendations with respect to implementation of and migrating to PQC;

2 to continue to develop Recommendations and other ITU-T publications on guidelines and best practices, which will help organizations to prepare for implementation of and migration to PQC;

3 to engage with industry stakeholders to gather insights and best practices for promoting PQC implementation and migration within telecommunication/ICT network;

4 to collaborate with other ITU-T study groups and other organizations for implementation of this resolution;

5 to encourage to share advancements of relevant developments that concerns PQC implementation and the migration and migration within telecommunication/ICT network to PQC;

6 to make recommendations to the Telecommunication Standardization Advisory Group on how to address the topics that are outside the mandate of the study groups,

instructs the Telecommunication Standardization Advisory Group

to drive a concerted effort across relevant study groups to accelerate standardization work for promoting implementation of and the migration and migration within telecommunication/ICT network to PQC,

instructs the Director of the Telecommunication Standardization Bureau

1 to provide the necessary assistance to establish action plans for promoting implementation of and the migration of telecommunication/ICT infrastructure to PQC and to encourage participation and contributions from Member States, Sector members, Associates, and Academia;

2 to organize workshop(s) to collect recommendations and inputs on this topic from a wide range of stakeholders;

3 to support the Director of the Telecommunication Development Bureau (BDT) in assisting Member States in promoting implementation of and migration of telecommunication/ICT infrastructure to PQC,

invites Member States, Sector Members, Associates and Academia

1 to submit contributions for developing Recommendations, other ITU-T publications on guidelines and best practices for promoting implementation of and migration of telecommunication/ICT infrastructure to PQC;

2 to facilitate educational workshops and training sessions to promote implementation of and the migration and migration within telecommunication/ICT network to PQC.