|  |  |  |
| --- | --- | --- |
| Title: ITU logo | INTERNATIONAL TELECOMMUNICATION UNION**TELECOMMUNICATION STANDARDIZATION SECTOR**STUDY PERIOD 2022-2024 | TSAG-TD585 |
| TSAG |
| **Original: English** |
| **Question(s):** | N/A | Geneva, 29 July - 2 August 2024 |
| **TD(Ref.:** [JCA-QKDN-LS4](http://handle.itu.int/11.1002/ls/sp17-jca-qkdn-oLS-00004.docx)**)** |
| **Source:** | JCA-QKDN |
| **Title:** | LS/i on feedback on discussions related to work on quantum-resistance in ITU-T [from JCA-QKDN] |
| **LIAISON STATEMENT** |
| **For action to:** | - |
| **For information to:** | TSAG |
| **Approval:** | JCA-QKDN meeting, Singapore |
| **Deadline:** | - |
| **Contact:** | Junsen LaiCAICT, China | E-mail: laijunsen@caict.ac.cn  |
| **Contact:** | Mark McFaddenDSIT, United Kingdom | E-mail: mark@internetpolicyadvisors.com  |
| **Contact:** | Hao QinNUS, Singapore | E-mail: hao.qin@nus.edu.sg  |
| **Contact:** | Gillian MakamaraTSB; Secretary JCA-QKDN  | E-mail: gillian.makamara@itu.int  |

A new liaison statement has been received from JCA-QKDN.

This liaison statement follows and the original file can be downloaded from the ITU ftp server at <http://handle.itu.int/11.1002/ls/sp17-jca-qkdn-oLS-00004.docx>.

|  |  |  |
| --- | --- | --- |
|  | INTERNATIONAL TELECOMMUNICATION UNION**TELECOMMUNICATIONSTANDARDIZATION SECTOR**STUDY PERIOD 2022-2024 | **JCA-QKDN-LS4** |
| **JCA-QKDN** |
| **Original: English** |
|  |  | Singapore, 17 May 2024 |
| **Ref.:** [**JCA-QKDN-064**](https://extranet.itu.int/sites/itu-t/jca/qkdn/meetingdocs/JCA-QKDN-064.docx) |
| **Source:** | JCA-QKDN |
| **Title:** | LS on feedback on discussions related to work on quantum-resistance in ITU-T |
| **LIAISON STATEMENT** |
| **For action to:** | - |
| **For information to:** | TSAG |
| **Approval:** | JCA-QKDN meeting (Singapore, 17 May 2024) |
| **Deadline:** | - |
| **Contact:** | Junsen LaiCAICT, China | E-mail: laijunsen@caict.ac.cn  |
| **Contact:** | Mark McFaddenDSIT, United Kingdom | E-mail: mark@internetpolicyadvisors.com  |
| **Contact:** | Hao QinNUS, Singapore | E-mail: hao.qin@nus.edu.sg  |
| **Contact:** | Gillian MakamaraTSB; Secretary JCA-QKDN  | E-mail: gillian.makamara@itu.int  |

|  |  |
| --- | --- |
| **Abstract:** | This liaison statement provides feedback to TSAG on discussions related to work on quantum-resistance in ITU-T. |

At the TSAG meeting in Geneva, 22-26 January 2024, JCA-QKDN was tasked with reviewing proposals to revise its Terms of Reference (ToR).

Following this guidance, the JCA-QKDN discussed this extensively in the meeting held in Singapore on 17 May 2024.

The discussions were immensely valuable, resulting in a consensus to keep the JCA-QKDN ToR unchanged. Additionally, the following points were agreed upon as feedback to TSAG on the topic of quantum resistance work in ITU-T:

– JCA-QKDN recognizes that the development of quantum-resistant cryptography algorithms is actively underway in other standards organizations that have the remit to study the topic and have specialised expertise required for this area. Collaboration with and engagement in these organizations is strongly encouraged.

– The transition of existing telecommunications protocols to incorporate quantum-resistant technology remains a topic of crucial importance to the ITU-T. In this regard, JCA-QKDN highlights that the ITU-T is already considering how to adapt certain Recommendations e.g., ITU-T X.509 for a post-quantum environment. In the case of ITU-T X.509, this work is done in collaboration with ISO/IEC JTC 1 and is supported by the annual ITU-T X.509 Day (convened every 9 May since 2022) which facilitate open discussions on transition strategies for ITU-T X.509. JCA-QKDN also highlights the following work related to quantum resistance:

* ITU-T Study Group 11: Published Technical Report QSTR-USSD “*Low resource requirement, quantum resistant, encryption of USSD messages for use in financial services*”
* ITU-T Study Group 13: Published Y Supp. 79 “*ITU-T Y.3800 series – Quantum key distribution networks – Role in end-to-end cryptographic services with non-quantum cryptography*” and is developing new Recommendations: [Y.QKD-IPSec-fr](https://www.itu.int/ITU-T/workprog/wp_item.aspx?isn=19390), [Y.QKDN-nq-qos-rf](https://www.itu.int/ITU-T/workprog/wp_item.aspx?isn=19145), [Y.QKDN-nq-rf](https://www.itu.int/ITU-T/workprog/wp_item.aspx?isn=19180) and [Y.QKD-TLS](https://www.itu.int/ITU-T/workprog/wp_item.aspx?isn=19159).
* ITU-T Study Group 17: Published ITU-T X.1811 “*Security guidelines for applying quantum-safe algorithms in IMT-2020 systems*” and is developing Technical Reports [TR.ac-pqc](https://www.itu.int/ITU-T/workprog/wp_item.aspx?isn=19311) and [TR.hyb\_qsafe](https://www.itu.int/ITU-T/workprog/wp_item.aspx?isn=18763). Additionally, SG17 is considering studies on the use of post-quantum cryptography in the next study period.

– In this study period, mechanisms for introducing new work items related to the adaptation of existing protocols and standards for quantum resistance is deemed sufficient. Specifically, the gap analysis used in Study Groups 11, 13 and 17 have been found to be effective in coordinating efforts in this emerging area. Therefore, it is suggested that no changes or new considerations for addressing quantum-resistance are introduced to the ITU-T study groups for the remainder of the current study period.

– Looking forward to the next Study Period, the transition to quantum-resistance may be a possible area for discussion when considering Resolutions at the upcoming WTSA.

JCA-QKDN thanks TSAG for the opportunity to discuss this issue in detail and looks forward to reporting on the topic at the upcoming TSAG meeting in Geneva, 29 July - 2 August 2024.

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