ETSI Releases World First Protection Profile for Quantum Key Distribution

SOPHIA ANTIPOLIS., FRANCE, April 27, 2023 /EINPresswire.com/ -- * First Protection Profile for the security evaluation of quantum key distribution (QKD) modules
* Anticipates the need for quantum safe cryptography
* Will help manufacturers to evaluate QKD under a security certification process
* Using widely recognized security certification scheme of the Common Criteria for Information Technology Security Evaluation

ETSI has just released a Protection Profile (PP) for the security evaluation of quantum key distribution (QKD) modules, ETSI GS QKD 016. This Protection Profile is a first and anticipates the need for quantum safe cryptography. The ETSI specification will help manufacturers to submit pairs of QKD modules for evaluation under a security certification process. Such modules can be used by telecom operators and enterprises in securing their networks with the knowledge that certified products have been subjected to the scrutiny of a formal security evaluation process. The Protection Profile specifies high-level requirements for the physical implementation of prepare and measure QKD protocols through to the output of final secret keys.

Quantum Key Distribution is a quantum-safe security technique to generate shared random secret keys by using the quantum properties of optical signals. Attempts to measure these signals in transit are detectable, and a QKD protocol can take these into account to ensure - in a quantifiable manner - that only secure keys are delivered.

"The development of large-scale quantum computers threatens most of the public-key cryptography in use today. For some use cases, quantum key distribution could provide an addition to post-quantum cryptography to mitigate this threat. In order to develop trustworthy QKD devices, appropriate security requirements and evaluation criteria are crucial in BSI's view.

This Protection Profile for quantum key distribution modules is the first of its kind and an important first step in this direction. That is why BSI has supported its development and would like to thank the ETSI Industry Specification Group Quantum Key Distribution for the fruitful collaboration," states Dr. Günther Welsch, BSI (German Federal Office for Information Security), Head of Division "Information Assurance Technology and IT Management".

“We are delighted to publish this initial Protection Profile as an important step to help certify QKD modules under the widely recognized security certification scheme of the Common Criteria for Information Technology Security Evaluation,” says Martin Ward, Chair of the ETSI ISG QKD.

The ETSI Quantum Key Distribution Industry Specification Group brings together experts from various companies and organizations with interests in QKD certification. These include potential customers for applications and system manufacturers, along with security experts from organizations involved in certification schemes and academia.

About ETSI

ETSI provides members with an open and inclusive environment to support the development, ratification and testing of globally applicable standards for ICT systems and services across all sectors of industry and society. We are a non-profit body, with more than 900 member organizations worldwide, drawn from over 60 countries and five continents. The members comprise a diversified pool of large and small private companies, research entities, academia, government, and public organizations. ETSI is officially recognized by the EU as a European Standardization Organization (ESO).

For more information, please visit us at https://www.etsi.org/

Claire Boyer
ETSI
+33 6 87 60 84 40
claire.boyer@etsi.org
