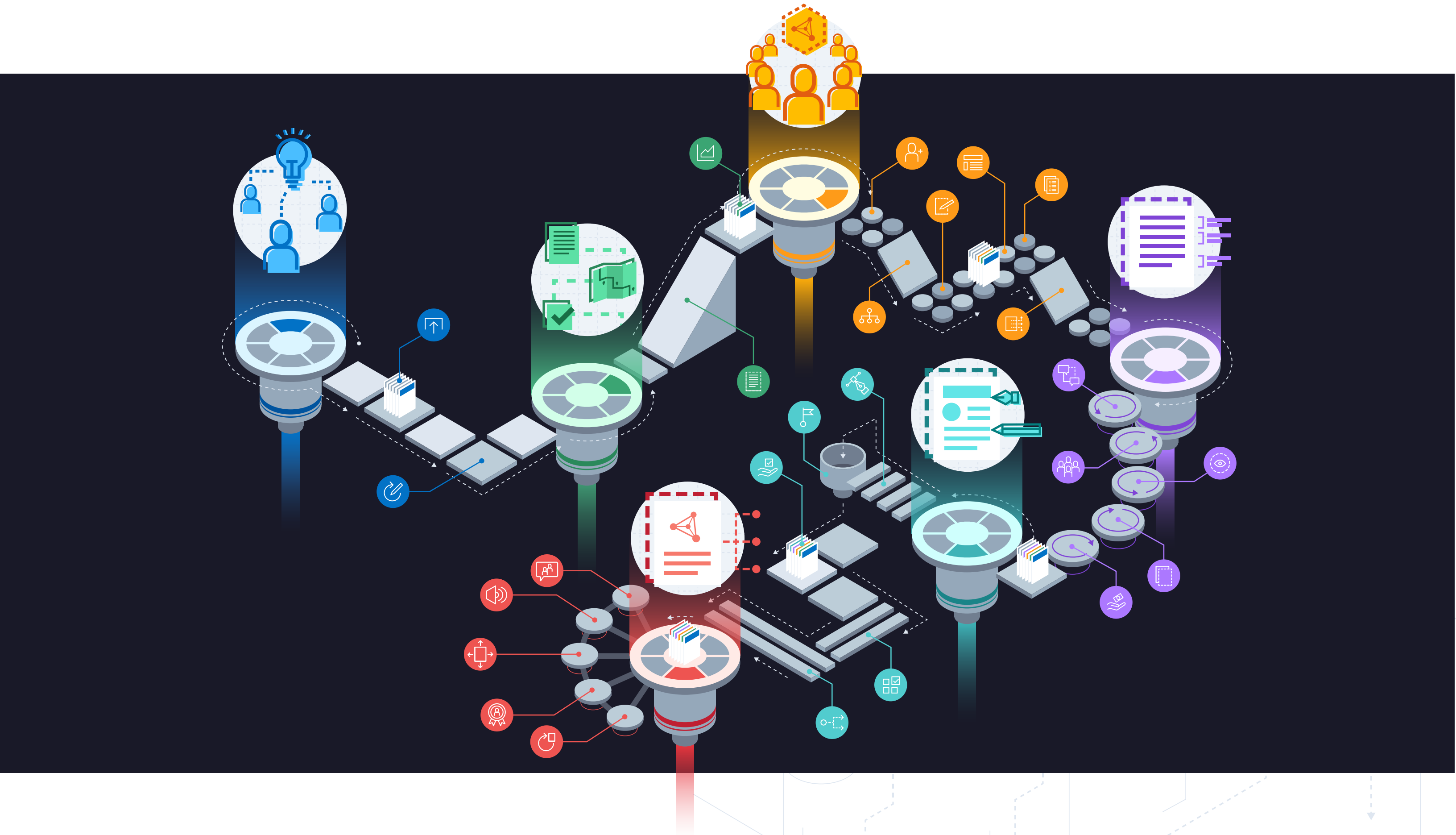
cloud security alliance®

Charter 2020

Quantum-Safe Security Working Group



© 2020 Cloud Security Alliance – All Rights Reserved. Valid at time of printing.

All rights reserved. You may download, store, display on your computer, view, print, and link to the "Quantum-Safe Security Working Group Charter" at https://cloudsecurityalliance.org/research/working-groups/quantum-safe-security/, subject to the following: (a) the Charter may be used solely for your personal, informational, non-commercial use; (b) the Charter may not be modified or altered in any way; (c) the Charter may not be redistributed; and (d) the trademark, copyright or other notices may not be removed. You may quote portions of the Charter as permitted by the Fair Use provisions of the United States Copyright Act, provided that you attribute the portions to the "Quantum-Safe Security Working Group Charter" (2020).

Table of Contents

Working Group Executive Overview

The Cloud Security Alliance (CSA) Quantum-Safe Security Working Group (QSSWG) was created to address evolving quantum information sciences technologies and some of the related critical threats to existing infrastructures. Quantum computers will soon (likely within the next 5-10 years) mature to a point where many traditional, trusted, forms of cryptography will be severely weakened or completely broken. Quantum computers will soon be capable of halving the effective protection of hash-functions and symmetric ciphers like AES, although using key sizes of 256-bits and longer should be sufficient for the foreseeable future. Unfortunately, the majority of traditional asymmetric algorithms (i.e. private/public key encryption, key exchange, and digital signatures) will be completely broken and soon can no longer be relied upon. Much of the world is in a race to develop reliable quantum-safe technologies, involving both quantum-resistant cryptography and the use of the same quantum technologies to counter the quantum computer threat. We will likely have new recommended quantum-resistant ciphers and digital signature schemes to start implementing within the next few years, if not sooner. Security will also be improved with quantum random number generators and quantum key distribution.

1. The QSSWG is focusing on two current technologies which most CSA members will need to address over the next few years, namely:
2. Quantum resistant cryptography (also known as post-quantum cryptography or PQC)
3. Quantum key distribution (or QKD)

Both technologies have a place in the secure networks of the future. The working group is focused on long-term data protection in this world of rising cryptanalysis capabilities. The goal of the working group is to support the quantum-safe cryptography community in development and deployment of a framework to protect data whether in movement or at rest.

Working Group Responsibilities

The focus of the Quantum-Safe Security Working Group is on cryptographic methods that will remain safe after the widespread availability of the quantum computer. This working group will be a forum for corporations, organizations, and individuals who are interested in the topic of quantum-safe security. The goal in forming this working group is to educate, increase awareness, and spark discussions on projects and issues regarding securing communications for which current encryption methods will not be safe anymore when, in the near future, quantum computers are available. The working group will also be open to welcoming external/outside collaborations with like-minded 3rd parties for joint development of research artefacts and standards.

Working Group Mission

The mission of the Quantum-Safe Security Working Group is to stimulate the understanding, adoption, use, and widespread application of quantum-safe cryptography to commercial institutions, policy makers, and all relevant government bodies. This mission includes, but is not limited to, the following:

- Provide objective information, education, and advice relating to these issues
- Provide thought leadership for the field of quantum-safe encryption and key management
- Become a trusted advisor to policy makers, analysts, consultants, industry leaders, and internal security or risk officers on issues relating to securing data in the long term
- Bridge the gap between mathematicians and physicists, and bring quantum cryptography solutions into a traditional security framework.
- Provide adequate resources to help build/develop standards as is necessary in this space.

Working Group Scope and Objectives

The scope of the Quantum-Safe Security Working Group will include the following topics:

- Educational programs
  - Training sessions and webinars
- Policy issues
  - Influence policy maker decisions through participation in relevant activities
    - Global view
    - Individual country view as selected by the members
  - Ensure adherence to existing policies
- Advocacy
  - Presentation at conferences
  - Represent the view of the working group at panel sessions
- Marketing
  - Highlighting the more secure aspects of quantum-safe cryptography
- Innovation sharing
  - Create an atmosphere within the group to foster innovation
  - Allow for ideas to be shared with all members of the group
- Standards and certification
  - Contributing to relevant standardization efforts
  - Help formalize certification models for quantum-safe solutions and algorithms
  - Contribute to educational models as required in this space.

Working Group Membership

The Quantum-Safe Security Working Group is run by appointing at least two co-chairs who will provide guidance and direction. Membership into the working group is open to any CSA member individual or organization who is interested in quantum-safe security topics.

Each chaired entity will have a principal attendee and one alternate to be designated by each principal.

Other individuals may be invited to attend meetings by the principals or alternates as deemed necessary to provide inputs to topics under discussion.

Sub-Work Groups

Ad hoc sub-work groups comprised of subject matter experts may be formed to plan or execute any related outreach, awareness, or research opportunities. Such sub-working groups shall report directly to the QSSWG.

The Quantum-Safe Security Working Group may also choose to allow resource sharing between cloud communities and other CSA working groups to assist in the timely completion of projects, programs, and other activities needed to support/enable Quantum-Safe Security's defined body of work.

Operations

Peer Review/ Advisory

The Working Group may seek CSA's help in reaching out to peers for review of this charter and other documented activities of the Quantum-Safe Security Working Group. Other CSA working groups will be the primary source for peers to help with our reviews. A number of other CSA working groups have members that are subject matter experts in cloud security which will help provide perspective in defining our activities.

Communications Methods

Conference calls will be performed online using an online teleconferencing service such as Zoom proposed by the CSA.

Infrastructure & Resource Requirements

The working group will be composed of CSA volunteers and will require typical project management, online workspace, and technical writing assistance.

Work Group Conference Calls and In-person Meetings

The Quantum-Safe Security Working Group will hold conference calls bimonthly or less if decided by the majority of voting members. Attendance by the Principal or Alternate is required. The Alternate must have full authority to act on behalf of the Principal if the Principal is absent. In-person meetings will be held whenever requested by the majority of the members, in a location to be announced prior to each meeting. Minutes of meetings will be posted after each meeting.

Decision-making Procedures

A. Definition of a majority

1. A majority shall consist of more than half of the members present and voting.
2. In computing a majority, members abstaining shall not be taken into account.
3. In case of a tie, a proposal or amendment shall be considered rejected.
4. For the purpose under this Charter, a "member present and voting" shall be a member voting "for" or "against" a proposal, including proxy representative.
5. Proxy where authority is delegated through a written statement or non-repudiated email should be declared and inspected for validity by the working group leadership before voting starts.

B. Minimum number of voting members

1. When the number of voting members is below ten (10), the vote will be postponed until the next meeting or teleconference call.
2. The minutes of the meeting will describe the voting request, and inform members that the vote will take place during the next meeting, at which time the vote will be registered, whatever the number of voting members.

C. Abstentions of more than fifty percent

When the number of abstentions exceeds half the number of votes cast (for votes, plus against votes, plus abstention votes), consideration of the matter under discussion shall be postponed to a later meeting, at which time abstentions shall not be taken into further account.

D. Voting procedures

1. The voting procedures are as follows:
   - By a show of hands as a general rule, unless a secret ballot has been requested; if at least two members, present and entitled to vote, so request before the beginning of the vote and if a secret ballot under b) has not been requested, or if the procedure under a) shows no clear majority
   - By a secret ballot, if at least five of the members present and entitled to vote so request before the beginning of the vote (online voting is applicable)
2. The Chair(s) shall, before commencing a vote, observe any request as to the manner in which the voting shall be conducted, and then shall formally announce the voting procedure to be applied and the issue to be submitted to the vote. The Chair(s) shall then declare the beginning of the vote and, when the vote has been taken, shall announce the results.
3. In the case of a secret ballot, the working group leadership shall at once take steps to ensure the secrecy of the vote.

© Copyright 2020, Cloud Security Alliance. All rights reserved.

Deliverables/ Activities

The first meeting of the working group will outline the deliverables for the duration of the working group. The list of deliverables will be discussed and accepted at regular QSS meetings, and can be later updated during future QSS meetings. Future changes in the list of deliverables must be approved by all co-chairs and the majority vote of attending members of the meeting. The deliverables should fall within the scope of the working group and may include the following items:

- Plan web seminar agenda for the working group
- Deliver a whitepaper describing the various elements, processes, tools, and capabilities of QKD for the general public.
- Provide a whitepaper detailing how CSA members can prepare themselves for the coming quantum computing threats.
- Deliver a whitepaper to enable relevant decision makers to opt for QKD to secure their network. Targeted decision makers can include CISO, Chief Risk Officers, CFOs and CEOs in targeted markets such as government, finance, healthcare, telecommunications, and cloud services.
- Organize web or live seminars on the working group activities and results.
- Lay the framework for a certification focused on Quantum-Safe Security in alliance with another certification organization.
- Add potential opportunities for collaboration with other Educational Initiatives and R&D Efforts.

Dissemination

- The working group will coordinate the dissemination of its results within the CSA community and to the other stakeholders (policy makers, research community, cloud providers, and customers) through the organization of the dedicated workshops on Quantum-Safe technologies, by speaking at conferences, and producing and distributing (e.g. at RSA or InfoSecurity) educational materials.
- The working group will also engage with potential interested parties who wish to contribute to the working group activities.

Duration

The working group will operate until 2022 for its chartered deliverables, and at that time consider charter renewal.