ISG QSC
Terms of Reference

From: **Founding members of an ISG on Quantum-Safe Cryptography (QSC)**

To: **ETSI Director General**

Subject: **Terms of Reference of the Industry Specification Group on Quantum-Safe Cryptography**

1 References

TWP clause 3	Operation of Industry Specification Groups
TWP clause 3.2	Creation and Termination of an Industry Specification Group
TWP Annex D 3	Requirements for an Industry Specification Group

2 Rationale

The white paper [Quantum Safe Cryptography V1.0.0 (2014-10)] lists several well-known families of cryptographic primitives believed to be quantum safe, gives some example applications and use-cases, and emphasises the need to migrate real-world systems to quantum safe security in ways that are sensible and realistic for industry from both the technical and economic viewpoints.

The ETSI Quantum Safe Cryptography (QSC) ISG aims to make an assessment and recommendations on the various proposals from industry and academia for quantum safe cryptography for real-world deployment and to standardize their relevant parts when needed. In addition to considering the security properties of these proposals in isolation, it is also important to understand their practical properties (efficiency, functionality, agility); which real-world applications each might be well suited to (Internet protocols, constrained environments, cloud, big data, SCADA, etc.); and to make pragmatic comparisons between currently deployed solutions and the proposed quantum safe alternatives.

ETSI has a proven track-record for its development and standardization of security algorithms for the mobile industry, which draws both on in-house expertise (ETSI SC SAGE) and its partners in industry and academia. ETSI has been the home of an ISG on QKD standardization since 2008. QSC is an issue of global impact and requires urgent development, especially given the recent progress in the development of a quantum computer and the lack of adequate means to fulfill current corporate, government and institutional policy requirements for the forward security of long-lasting data.

The creation of an ETSI ISG is essential to taking forward QSC work as it will enable experts who are not ETSI members to provide input. Such input is vital to ensuring that the specifications are as good as possible and have global reach.

The ETSI ISG is used for highly specific technical work, requiring a very particular set of experts, especially in the fields of mathematics and cryptography. This is an important reason that the ISG mechanism is the appropriate tool of choice for QSC. In addition, expertise from non-ETSI members will also be required.

3 Terms of Reference for ETSI ISG Quantum-Safe Cryptography [TWP D.3, Part Aa)]

In the following clauses, deviations from the applicable ETSI TWP as agreed by the members of ISG QSC, including deviations to the ETSI TWP made in the ISG Membership/Participant Agreements, are stipulated.

3.1 Scope

The QSC ISG will aim to make recommendations on core cryptographic primitives and develop ETSI Group Specifications (GSs) for quantum-safe ICT applications highlighted by industry. It will also aim to offer practical advice and guidance to industry on real-world deployment issues, such as transition timescales, generic requirements from operators or vendors, assessment of threats and risks, etc.

The activities of the QSC ISG will be performed in close co-operation with relevant standards activities within and outside ETSI, including QKD ISG and TC CYBER. It is not the intention of the ISG to work on items already covered by the QKD ISG.

The work of the QSC ISG will include:

- Identification of proposals from industry and academia for quantum safe cryptographic primitives, and the development of a framework for quantum safe algorithms.
- High-level characterization of these primitives in term of computational complexity, security assumptions against classical and quantum threats, efficiency and agility.
- Assessment of the suitability of the cryptographic primitives with respect to the quantum safe requirements and applications.
- Threat and risk assessment for real-world use cases.
- Providing evidence of the need for new standards and technological guidance, along with a development roadmap, including performance standards and verification techniques for quantum safe algorithms.
- Dissemination of guidance and standards documents, and later maintenance of the standardised algorithms under the custodianship of the ETSI SC Security Algorithms Group of Experts (SAGE).
- Defining criteria for, and assessment of, the suitability of cryptographic primitives.

3.2 Membership

According to Clause 3.4. of the ETSI Technical Working Procedures (TWP), membership in ISG QSC is restricted to ETSI Full/Associate Members and applicants for Full/Associate membership, who have signed the ISG QSC Membership Agreement.

Observers and non-members of ETSI may not become members of the ISG but may participate in the ISG according to the rules as described in the ISG QSC Participant Agreement. Participation of non-members of ETSI is subject to acceptance of the ISG QSC Participant Agreement, and payment of a per-meeting participation fee as described in the ISG QSC Participant Agreement.

3.3 Budget

Budget for operation is fixed on an annual basis by the Members, based on the costs the members anticipate to incur.

3.4 Duties and Rights of Members

Members and participants have the duty to constructively cooperate on the development of ISG Group Specifications within the scope of the ISG as described in clause 3.1.

Members have the right to cast their vote on the approval of a Group Specification when necessary, and in other instances when decisions by the members are required. Members have the right to appeal directly to the ETSI Board to challenge a Chairman's decision and shall inform the ISG Chairman and the ETSI Director-General beforehand.

3.5 Preparation of Group Specifications

Group specifications are prepared within the ISG or within specific working groups. Working groups are chaired by working group chairs, who are appointed according to the rules of operation of the ISG. All draft specifications must be approved by the ISG members using the decision making process detailed in the rules of operation of the ISG. If a specification is prepared in a working group and fails to be approved by the members, it is referred back to the working group.

3.6 Participant fee

The Participant shall pay to ETSI a per-meeting attendance fee amounting to €700 (excluding taxes) per delegate per physical meeting.

3.7 Detailed deviations from the ETSI Technical Working Procedures (TWP)

In the following, deviations from the applicable ETSI TWP as agreed by the Members of ISG QSC, are stipulated. All other sections, which are not subject to deviation are negligible.

Section 3.7 is included in these Terms of Reference only for information and reflects the agreement of Founding Members and Participants as the prevailing document in respect of changes to the TWP is the ISG QSC Membership Agreement.

3.7.1 Participation in the work of the Industry Specification Group (extension of TWP 3.4)

Observers or non-members of ETSI must sign the ISG QSC Participant Agreement in order to be authorized to participate. The Participant Agreement will be terminated if the participant has not participated in at least 2 physical meetings of the ISG QSC in a 12 months period. A revocation notice under article 9.1 (c) of the ISG Participant Agreement is sent to the participant in this case. The ISG Chairman will periodically review the participation record of authorized Participants.

In addition, access to meeting documents, mailing lists etc. will be removed from authorized Participants if they fail to participate in, or register and pay participation fees for two successive physical meetings. Such access will be restored upon registration for a subsequent physical meeting of the ISG QSC.

3.7.2 Convening an ISG meeting (TWP 3.5)

3.7.2.1 Invitation to an Industry Specification Group meeting (TWP 1.5.1)

The invitation to an Industry Specification Group meeting and the necessary logistical information shall be disseminated by the hosting organization at least 30 days before the meeting to all on the Industry Specification Group membership list (see clause 1.5.5).

The first meeting of a new Industry Specification Group will be announced in a Collective Letter, with at least 30 days' notice, by the ETSI Secretariat.

3.7.2.2 Agenda for an Industry Specification Group meeting (TWP 1.5.2)

The draft agenda shall be disseminated by the responsible Chairman to all on the Industry Specification Group membership list at least 30 days before a meeting. The draft agenda shall include details of draft ETSI deliverables for approval and officials for appointment. Any other subject matters where voting may be required shall also be included and indicated in the draft agenda.

The draft agenda for the first meeting of a new Industry Specification Group will be announced in a Collective Letter, with at least 30 days' notice, by the ETSI Secretariat.

3.7.2.3 Documentation for an Industry Specification Group meeting (TWP 1.5.3)

Documents shall be numbered as shown in the following example:

ETSI/TB(nn)x

This numbering system has four logical elements:

1) **ETSI:** to indicate that it is an ETSI document;
2) **/TB:** the name of the Technical Body or Working Group;
3) **(nn):** to indicate the year, e.g. (15);
4) **x:** to indicate any additional information concerning the unique number of the document or its status, etc.

The fourth item (x) can be used in any way that an individual Industry Specification Group sees fit.

3.7.2.4 Registration for an Industry Specification Group meeting (TWP 1.5.4)

Every Attendee shall register on arrival at each meeting. Each Attendee who represents an ISG QSC member or ISG QSC participant shall declare the precise name of that member. An Attendee may only represent one ISG QSC member or one ISG QSC Participant.

3.7.2.5 Maintaining an Industry Specification Group membership list (TWP 1.5.5)

The QSC Industry Specification Group shall maintain a membership list within an email exploder list established specifically for that purpose. Any individual may join this email exploder list if he/she is a representative of an ETSI member that has signed the "QSC Industry Specification Group agreement" and has an ETSI server user account, and those who join this email exploder list will be considered as being on the Industry Specification Group membership list. Failure to reconfirm the intention to remain on the email exploder list at regular intervals (lists are normally reviewed every six months) will result in removal from this email exploder list and thus from the Industry Specification Group membership list.

The ISG QSC membership list shall be used for the dissemination of information and for decision making within the ISG QSC.

3.7.3 Decision making (TWP 1.7 and TWP 3.7)

3.7.3.1 Principles of decision making (TWP 1.7.1)

An Industry Specification Group shall endeavour to reach Consensus on all issues, including the approval of draft Group Specifications. If Consensus cannot be achieved, the Chairman can decide to take a vote which may be performed by a secret ballot.

A vote may be conducted during an Industry Specification Group meeting or by correspondence.

Where voting is used, vote results shall be evaluated by the Chairman on the basis of one ISG Member, one vote. ISG Participants do not have the right to vote.

Decisions concerning

(i) the ISG Budget under Article 3.1(b) of the ISG QSC Agreement,
(ii) Additional Costs under Article 3.1(c) of the ISG QSC Agreement, and
(iii) the allocation of costs among members of the ISG QSC under Article 3.2 of the ISG QSC Agreement, require unanimous support of the ISG QSC Members. For all other decisions, except for the appointment of officials of the ISG QSC, a proposal shall be deemed to be approved if 71 % of the votes cast are in favour. Abstentions or failure to submit a vote shall not be included in determining the number of votes cast.

For interpreting the result of an election for an official of the Industry Specification Group, a simple majority of the votes cast shall be used (*see 3.7.3.1.3 below).*

3.7.3.1.1 Voting during an Industry Specification Group meeting (TWP 1.7.1.1)

The following procedures apply for voting during an ISG QSC meeting:

- before voting, a clear definition of the issues shall be provided by the chairman;
- voting members shall only be entitled to one vote per member;
- if a voting member has more than one representative present, only one representative may vote;
- if manual voting procedures are used, each voting member may only cast the vote once;
- if electronic voting procedures are used, votes may be changed prior to the closure of the vote;
- ISG QSC members are only eligible for voting (voting members), if they have been present during at least two out of the previous 3 meetings;
- Founding Members of the ISG as identified in the ISG Agreement shall be eligible to vote during and up to the end of the first three meetings following the creation of the ISG. Thereafter they are subject to the above participation requirements as for all other members;
- voting by proxy is not permitted;
- there are no quorum requirements;
- the result including percentages of the vote shall be recorded in the meeting report.

3.7.3.1.2 Voting by correspondence (TWP 1.7.1.2)

The following procedures apply for voting by correspondence:

- before voting, a clear definition of the issues shall be provided by the Chairman and disseminated to all on the ISG QSC membership list;
- the voting period shall be defined by the ISG QSC Chairman and communicated to all on the ISG QSC membership list;
- ISG QSC members are only eligible for voting (voting members), if they have been present during at least two out of the previous 3 meetings;
- Founding Members of the ISG as identified in the ISG Agreement shall be eligible to vote during and up to the end of the first three meetings following the creation of the ISG. Thereafter they are subject to the above participation requirements as for all other members;
- voting members shall only be entitled to one vote per member;
- if electronic voting procedures are used votes may be changed prior to the closure of the vote;
- there are no quorum requirements;
- at the end of the voting period the Chairman shall count the votes as described in clause TWP 1.7.1.2;
- the result of the vote should be disseminated to everybody on the ISG membership list within 15 days.

3.7.3.1.3 Voting for the election of an Industry Specification Group official (TWP 1.7.1.3)

For the purpose of electing any Industry Specification Group official the procedures given in clauses 3.7.3.1, 3.7.3.1.1 and 3.7.3.1.2 shall apply.

In the case where there is more than one candidate, a secret ballot shall be used. For interpreting the result of an election for an Industry Specification Group official the following procedure shall apply:
the candidate obtaining the highest number of votes in the ballot is elected.

The ISG QSC Chairman shall be responsible for the voting process and shall ensure that confidentiality is maintained.

If the vote is conducted during an ISG QSC meeting only the final result shall be recorded in the meeting report.

If the vote is conducted by correspondence only the final result of the vote shall be disseminated.

3.7.3.2 Appealing against a Chairman's decision (TWP 1.7.2)

Any member of ISG QSC who is against the Chairman's ruling on a vote may submit its case to the Board for decision. In such cases the member shall also inform the ISG QSC Chairman and the ETSI Director General beforehand.

When the ISG QSC Chairman has made a ruling, his decision shall be taken as the basis for future operations, unless overturned by the Board.

4 ETSI field of interest [TWP D.3, Part Ab)]

The creation of an ETSI ISG is essential to taking forward QSC work as it will enable experts who are not ETSI members to provide input. Such input is vital to ensuring that the specifications are as good as possible and have global reach.

ETSI with its strategic topic on quantum technologies appears to be right place for standardizing quantum technologies and related security issues for global outreach.

5 Why any overlapping or complementary elements (with reference to existing work or Terms of Reference of any existing Technical Committee or Project) is regarded as desirable [TWP D.3, Part Ac)]

There is no known overlapping with any ongoing work in ETSI.

6 Time plan [TWP D.3, Part Ad)]

The first 2 years ISG QSC meetings and conference-calls will be planned to produce Group Specifications. After 2 years, ISG QSC will make proposals on how to evolve:

- close the ISG,
- or transfer and continue the work in an existing Technical Body meaning that all ISG participants would be required to become ETSI Members and that the ISG QSC voting rule would be changed to the ETSI Directive TC weighted vote rule,
- or create a new Technical Body (new WG in a TC, new TC, new EP or new EPP)
- or continue in ISG QSC for an extended period with revised Terms of Reference, if necessary.

7 Chairmanship [TWP D.3, Part Ae)]

Colin Whorlow, CESG has accepted to stand as convenor for the first meetings. The Collective Letter announcing the first meeting will include a call for candidates for the Chairmanship. If it is not possible to appoint a permanent Chairman at the first meeting then the meeting shall appoint a convenor for the second meeting.

The duration of chairmanship is 2 years.

8 Resource requirements [TWP D.3, Part Af)]

No resource requirements, beyond the "basic administrative support" provided by the ETSI Secretariat to ISGs, have been identified. Further resource requirements may be identified from time to time by the ISG members, who will decide on the funding arrangements as required.

9 ETSI Secretariat resources [TWP D.3, Part Ag)]

9.1 “Basic administrative support” will be provided by the ETSI Secretariat, e.g.:

- info/meeting/document handling area on the ETSI Portal.
- document storage area on the ETSI DOCBOX server.
- e-mail lists provision

- entry of the Work Items into the Work Program Management (WPM) database (provided by ETSI Operations (OPS) Department of the ETSI Secretariat).processing/publication of ETSI Deliverables (providing they have respected the ETSI Drafting Rules).
- a support officer will be allocated to provide guidance and assistance to the ISG.

9.2 Support for meetings will be provided when the meeting is held at the ETSI Headquarters, e.g.:

- meeting rooms in ETSI premises.
- meeting support for invitations, badges, etc in ETSI premises.
- tea/coffee in ETSI premises.

Meetings held outside of the ETSI Headquarters shall be supported by the hosting member organization as in 9.2.

10 ISG membership agreement [TWP D.3, Part Ah)]

See separate ISG QSC Agreements (Member Agreement and Participant Agreement).

11 ETSI full and/or associate members having declared their willingness to provide resources [TWP D.3, Part Ba)]

The following members have indicated that they are willing to support the ISG (at least four required):

- Approach Infinity
- C3L (Cadzow Communications Consulting Ltd)
- CESG
- PIDS
- University of Waterloo

The following counsellors of ETSI have also expressed an interest in participating in the work of the ISG QSC:

- Joint Research Centers of the European Commission

The following non-members of ETSI have also expressed an interest in participating in the work of the ISG QSC:

- SK Telecom

12 Planned deliverables and their delivery dates shall be identified [TWP D.3, Part Bb)]

At the point of writing this proposal no specific deliverables have been planned.

13 Internal organization [TWP D.3, Part Bc)]

No internal organization or Working Groups have yet been identified. This will depend on the results of the initial work of the ISG.

14 Any committee/project-external ETSI resources required (i.e. outside those provided by the Industry Specification Group participants) shall be specified [TWP D.3, Part Bd)]

No additional resources such as experts or Special Task Forces have yet been identified. This will depend on the results of the initial work of the ISG QSC.

15 Maintenance arrangements for deliverables shall be specified [TWP D.3, Part Be)]

The maintenance of any deliverables will be assured by the ISG QSC. At the end of the work the ISG QSC shall define the follow-on responsibility for any required maintenance.

16 The relationship with ETSI Technical Organisation shall be specified (i.e. list the interfaces between the ISG and ETSI TBs) [TWP D.3, Part Bf)]

The ISG QSC intends to establish a liaison relationship with the following ETSI TBs and Partnership Project:

- ISG QKD
- TC CYBER
- TC ESI
- SC SAGE

Depending on the way in which the work progresses, the ISG QSC may establish a liaison relationship with the following organizations:

If required, the ISG QSC may decide to establish additional liaison relationships.