|  |  |  |
| --- | --- | --- |
| ITU logo | INTERNATIONAL TELECOMMUNICATION UNION**TELECOMMUNICATIONSTANDARDIZATION SECTOR**STUDY PERIOD 2017-2020 | TSAG-TD620R1 |
| **TSAG** |
| **Original: English** |
| **Question(s):** | N/A | Geneva, 23-27 September 2019 |
| **TD** |
| **Source:** | Chairman, Quantum Adhoc Sessions |
| **Title:** | Chairman’s proposal on a shared vision for adhoc sessions on Quantum |
| **Purpose:** | Information |
| **Contact:** | Arnaud TaddeiSymantec CorporationUnited States of America | Tel: +41 79 506 1129E-mail: Arnaud\_Taddei@symantec.com  |

|  |  |
| --- | --- |
| **Keywords:** | Shared Vision; Focus Group; Coordination; |
| **Abstract:** | This document regroups Chairman’s analysis and proposal of an initial shared vision to help the community attending the adhoc sessions on quantum reach a pragmatic consensus regarding both a potential Focus Group on ‘Quantum’ and the required Coordination.  |

Opening remarks:

~10 delegates were in last TSAG Dec 2018. UK, US, CA, CN, DE, etc.

Chairman to be netrual, facilitate conversation, help this group to listen to each other, understand each other.

Table 2: ETSI docs? are missing

# Disclaimer and Intention

Chairman’s intention is to initiate a live document toward a common shared vision for consensus or not, before engaging in any ToR drafting work.

This initial version is a very first draft and a simple ‘black ink’ of considerations of the Chairman, generated from a number of public declarations and private offline conversations, a number of observations and personal investigations over the course of a short year.

This is by no means, meant to be perfect or correct, is probably provocative too, but for the good intention to give the best possible atmosphere for this community to understand each other and reveal some hidden dependencies, constraints, on underestimated aspects.

# Introduction

In less than a year, from the situation left at last TSAG meeting in December 2018 to this TSAG meeting, the conditions regarding how to address in the most efficient way the nascent work on Quantum at the ITU has evolved in a number of ways:

|  |  |  |
| --- | --- | --- |
| Area | Status | Comments |
| Creation of Quantum Focus Group | No consensus  | Concerns regarding * Duplication with other SDOs and work started in SGs about QKD and QRNG
* Topics seen as still long term research, not ready for qualification for standardization
 |
| Coordination between ITU SGs | Proposed but not started |  |
| Coordination with other SDOs | No proposition | Identified SDOs: ETSI, ISO, IETF, IEEE |
| Workshops  | ITU Shanghai Workshop was delivered last June 2019SG17 organized a Quantum Mini Workshop in January 2019 |  |
| Standardization  | SG2 considers management aspectsSG5 considers environmental aspectsSG11 considers protocol aspectsSG13 engaged on QKDSG17 engaged on QKD and QRNGSG15 received contributions |  |
| TSAG Level | Hot Topic 15 declared |  |

In this TSAG meeting the initial situation at the beginning of the adhoc sessions on quantum can be summarized below

|  |  |  |
| --- | --- | --- |
| Proponents | Proposal | Comments |
| C97 contributors  | Create a FG on Quantum based on C97 | industry, Academia, operators, KT, SKT, NICT, IDQuantique.  |
| US, UK, Canada, France, Germany  | Concentrate on a JCA for sorting coordination issues |  |
| SG13 and SG17 Leaders  | Support a FG on Quantum TD579 with no duplication of work with current QKD and QRNG work  | Referred to ETSI ISG QKD |
| ISO/IEC JTC 1 | No duplication vs AG4 Quantum Computing (TD493) | Interesting coverage of Terminology and ICT aspects |
| IEC/ISO/ITU SPCG | No duplication vs AG4 (see above) and Security requirements, tests and evaluation methods for QKD (TD605) | Coordination issue on Security Requirements? |

# Chairman’s considerations

## General considerations

Based on opening plenary declarations and offline consultations:

* Whilst there are different expressed views, there is no sense of red lines being crossed
* Whilst there is a need for coordination, Chairman considers only coordination won’t be sufficient
* Whilst there is a new proposal for a Focus Group, Chairman considers
	+ The proposition needs to be more focused
	+ The proposition would benefit from highlighting the outcomes towards standardization
* At this stage there is little potential overlap with other SDOs
* At this stage it is considered there is room for a potential consensus

## Specific considerations

Debates and offline conversations are showing a number of mis-understood aspects by various delegations that need significant clarification:

The most notable surprise is the assumption by all the parties that: QKD is being standardized in SG13 and SG17, therefore it is de-facto excluded from the scope of the proposed Focus Group. This general assumption will cause a significant set of issues and needs to be better analyzed.

Another surprise is that some parties consider that Quantum Computing is not specific to ICT and should be excluded in block from ITU activities. This seems extreme and should be re-qualified.

The lack of caution regarding timing aspects is a surprise too. We cannot ignore that WTSA-20 will happen at the end of 2020 and that any entity will not be immune from potential changes.

Another point that is never discussed is the maturity level of this new field and including about the experts themselves. Underestimating this aspect is removing a significant aspect of the root-cause analysis of why we are in a situation that we seem to deny.

# Complications

Based on the above Chairman proposes to look at specific complications in more details.

## State of QKD standardization in ITU-T

Whilst the topic of Quantum arrived to the ITU-T and is under significant development we should observe the following:

* QRNG is in a good situation and has consented its first work item. We do not expect any specific issues in this area which is well purposed for standardization
* QKD development however is showing a significant number of issues that should by any means NOT be denied

Some of the QKD work is indeed engaged in SG13 and SG17 with the following observations by Chairman:

On the down side

* Whilst both SGs have now a plan for collaboration, the collaboration didn’t formally start. In the meantime the community is painfully going through the 4 steps of any team: form (they just did), storm (they are in this phase), norm and perform;
* Y.3800 was consented in a rush in last SG13 meeting (7 revs; ETSI Huawei editor proposal was not taken into consideration.), and the last call and AAP process are showing a significant number of issues. [NICT: Y.3800 was progressed and consented as scheduled.] Wehighlight here 2 relevant issues for this work:
	+ some are due to fundamental lack of perspective on use cases, design and architecture which could be addressed by a Focus Group.
	+ A ‘no rush’ approach would have helped a “forming group”. Now, in addition we need to heal some of the situation, which could be addressed by a Coordination model (JCA)
* At SG17 last meeting, experts realized that they had a disagreement on what the letter K in QKD means. This is an absolute RED FLAG and requires strong coordination of all the current QKD standardization work in the ITU-T and other SDOs. [Canada: Do you imply Y.3800 shouldn’t be approved?] This calls to another question, the next surprises to us: what is the codified terminology that this community relies on for QKD? This is the other element that could be addressed by a Focus Group.

[SG17 Chairman: terminology is fundamental to standardization. Do SG13 and SG17 need to wait 2-yrs for a FG deliverable?]

[AT: inspired by FG-DLT term deliverable. This one term might not need to wait, but other bigger area might be for FG]

[NICT: SG13 is developing definition of ‘key’]

[Huawei: ETSI ontology is published] [Canada: proven we need a JCA for consideration]

On the up side

* The mini workshop organized by SG17 was very good and showed a number of key elements (use case considerations, specific design aspects, etc.) that could nurture a Focus Group
* Seeing delegates from ISO, ETSI participating now regularly to the work is encouraging
* Seeing delegates from Operators whom we usually don’t see in ITU-T like Telefonica is encouraging
* Understanding the reasons why some operators are interested by QKD revealed an interesting gap. Indeed some operators would consider that set-top box could become QKD devices peering the Access Network. This is giving a very different use case vs the current one and shows a huge gap that could be fulfilled by a Focus Group.

Chairman is now considering the following:

* At this stage what is under development for standardization at SG13 and SG17 is a SMALL subset of the whole QKD area
* The current level of maturity of the experts is significantly below other fields and this is normal. Yet a comparison of what SG15 developed on just their architecture part through G.800, G.805 and the forthcoming G.807 creates a benchmark on which we would aim to. Yet it will take years for this community to reach. No surprise here but we should recognize this important question: Did we put the cart before the horses and shouldn’t we have considered a Focus Group earlier?
* Being inspired by the FG DLT structure, in order to remedy our current situation a Focus Group including QKD could offer significant deliverables on:
	+ Terminology and Ontology
	+ Use Cases
	+ Architectures and Design
* And they are all linked together

[Editorial note: Describing the fine grain finesses of all the links between the topics is actually starting the Focus Group work and is beyond the time allocations of this ad hoc but a ‘rapid thinking’ approach will list:

* Use cases: which are the various use cases we need to consider? Do they have a business value qualified today or under consideration? Do we have functional requirements?
* Design aspects: [NICT: Y.3800 already considered design aspects and architecture.]
	+ Stability of the architecture:
		- How to make the system Highly Reliable knowing that today it seems physics allows a bi-way QKD but not an N-way. How to ‘clusterise’ the nodes and if not, what is the mitigation? Note: QKD is intrinsically limited to a point-to-point link between 2 parties. There are no ways to do QKD with more than 2 parties. However, optical switching is possible if we want to address several parties
		- Any study on the scalability effect to move from the use case of 2 data centers or relays of chained nodes like in the example of the Beijing-Shanghai line, vs the case of multi-millions of QKD devices, say in a potential use case of set-top boxes?
	+ Flexibility of the architecture:
		- What are the system architecture patterns that are candidates? Ground based? Air based? Space based? Hybrid? For which use cases Data Centers? Set-top Boxes? Backhauls? Peering?
		- Are they independent or can we find a unification model?
		- If not independent how to measure their flexibility to understand their limits?
	+ Manageability of the architecture:
		- How management-friendly/unfriendly are the various architecture patterns?
		- What is the cost of supporting a discrete number of QKD devices vs millions or dozen of millions
	+ Migratability of the architecture:
		- What happens to the photons that in a device Version n when moving to a device Version n+1 or a competing device? Do we introduce a loss in the SLA? Which is the security risk? Which is the management cost and risk? Which is the customer impact?
	+ There are other criteria such as security itself, integratability, sustainability, testability, certifiability, etc.
	+ See Architecture Adivsory Board proposition in RG-SS [C99](https://www.itu.int/md/T17-TSAG-C-0099/en)
* All of the above + QKD itself is going to generate significant requirements for Terminology
	+ And this is why the 3 aspects of use case, architecture/design and terminology are linked

]

[China: people thought FG scope not clear enough. But our proposed FG is pre-standardization study, to help identify what should be standardized by SGs. We agreed in last TSAG FG will not duplicate work items already ongoing in SGs.]

[Huawei: recognizing SG13 architecture ongoing, but nothing in stone. Principles should be in FG] [UK: Y.3800 is framework, not architecture. SG13 ongoing work item on Y.qkd-architecture started in June 2019.]

[China: protocol work to be done in SG11.]

[SG13 Chair: Y.3800 framework = overview.]

## Are there use cases for Quantum Computing for the ICT

Assuming that the strength of Quantum Computing is the possibility to offer true parallelism capabilities vs conceptual parallelism offered by traditional computer architectures, the ICT is not short of NP Complete problems to resolve:

* The traveling salesman problem is a traditional issue in networking and traffic
* The density of computation generated by data analytics in general and with the augmentation with AI/ML is asking the question IF Quantum Computing could help here to resolve issues such as AI/ML for Zero Touch, for 5G, for IoT, etc. and for the security itself of the previous topics

In addition we still need to analyze the impact of quantum computing to networks (positive and negative)

So rejecting upfront Quantum Computing for ICT should at minimum require a proper qualification in a Use Case format in a Focus Group.

Here we note that

* the Focus Group could significantly benefit the work of the ISO AG4 and probably the AG4 could benefit from perhaps wider/more diverse ICT expertise
* the coupling between the Focus Group and a coordination group like a potentially attached JCA starts to feel being essential

## A natural path for QIN [AT: QIN is a scalable version of QKD]

QIN is more about connectivity between devices operating with quantum signal.

The core of the problem is how to make QKD scalable so that it can support more use cases and therefore how to make QKD evolve into a QIN.

This will make new elements appear in the architecture such as quantum relays and quantum repeater technologies as they will not only answer the scalability issues but as well some use cases support issues (networks, new applications, co-fibre transmission issues and the merger with the new elements).

In order to have a good development of standards into SGs and across SDOs it is essential to understand what is coming so that the standardization can avoid too limited recommendations, highlights abstraction layers and can create a solid foundation.

Chairman considers that both Terminology, Use Case and Architecture/Design are three key elements that a Focus Group could carry to the benefit of standardization.

This will answer a real critical problem in the development of the work as it will offer the required flexibility to prepare and pave the way for the next generation technology in this area.

[Editor’s note: Expecting support from the experts here but now I can make the exact link between the pieces]

## And a natural inclusion of sensors and metrology aspects

With QKD scaling to QIN and now including step by step all the components like Quantum Computers, we can now naturally include metrology aspects.

The nature of Quantum networks will create a new challenge to measure networks themselves due to the nature of physics. It is now much more natural to introduce metrology aspects because you probably can’t do measurements with traditional methods.

Of course performing measurements requires specific topology positions with very likely best practices or even possible/impossible positions in the architecture.

Again now we see that beyond terminology and use case we may have to consider quite deep architecture and design aspects.

[Editor’s note: Expecting support from the experts here but now I can make the exact link between the pieces]

## Constraints

### Timing

Chairman considers we cannot ignore WTSA-20 because if there are any form of structure change it can potentially impact any existing entity, Study Groups and Focus Groups.

Chairman considers that if a FG existence is 1-2 years, we should conservatively make a 1 year-long FG with the possibility to ask an additional 1 year extension after WTSA-20 with the provision to amend its ToR to reflect any relevant implications from WTSA-20 decisions.

### Resources

Resources is always a critical risk and there are a few aspects here:

* We need to ensure we have a sufficiently good critical mass where the risk is probably limited given the positive observations in the SGs, in the ITU Workshop, in the other SDOs and the informal collaboration that started ‘bonnant malant’
* We need to ensure we have a more diverse set of experts and our biggest risk is in the lack of product, software, system, service architects
* We need to ensure we have a multi-stakeholder approach in terms of representativity of member states, sector and associate members, academia, etc.

### Regulations

A constraint that will turn in a requirement and that we completely ignored are the regulatory aspects. Today on QKD or QRNG there is probably no need for such considerations but for example on a topic like Quantum Communication, should it be considered for a Focus Group, it is technically impossible to dismiss the various aspects of Lawful Interception otherwise anything that will be produced as deliverables will be impossible to implement in the real life.

So the requirements implied by Lawful Intercepts must be discussed in terms of what interfaces must the Quantum Communication be compliant to and what do they need to exhibit technically.

This will be a difficult topic to address but we cannot ignore it. This is asking the upfront question on whether Quantum Communication is ready for standardization at all.

[China: QKDN distribute classic info. QIN quantum teleportation, quantum repeater network, will distribute quantum state. Quantum communication ‘blind quantum computing’. Europe is building quantum network in Netherland. Quantum metrology is linked with quantum network, entangled quantums will enable better measurement.]

[Huawei: Dynamic network will fit for both QKDN QIN. QKDN QIN architectures should be unified.]

[Canada: what’s difference if work is done in FG or in SG?]

[AT: SG too rigid, bound by texts, no brainstorming/whiteboard. In SG, cluster of people in Qs defending their positions. ]

# Proposition

The above analysis is leaving chairman with the following considerations that at this stage there is room for:

* No consensus
* A consensus to be found on a Focus Group with a limited crisp scope?
* A consensus to be found on a coordination mechanism and if a JCA, which specifics?
* If both are in consensus, in which combination model the FG and the JCA should work?

## Visualizing the proposition for a Focus Group

Chairman considers there is room for a Focus Group for one year with an amendable ToR for a second extended year.

At this stage this Focus Group should have potentially 3 deliverable (area)s (may mean 3 working groups)

* Terminology
* Use Cases
* Architectures and Design

This decomposition is non definitive though Chairman will not recommend at this stage to have Regulations as a 4th deliverable area because 1) this is too early and probably irrelevant and 2) there are various timing and resource issues



[Tunisia Telecom: support FG, bring new experts from non members, other SDOs, strengthen collaboration with SDOs.]

[UK: This table is also useful for JCA. Other SDOs should be added in this table.]

[US: beyond the scope/assignment of this Ad Hoc. US sees fundamental needs for coordination. FG allow non-members, so does JCA. FG by an SDO is too early for technology development.] [FG is transition something could be standardized, toward a Rec. JCA cannot produce]

[CASquantum: global coordination for standardization, many countries, different subjects. Lack of experts. FG could focus on those mature area.]

[France: avoid duplication of SDOs, sees SG17 work items overlaps with SC27/WG3 security requirements and evaluation. Call for JCA. Technical reports will incorporated into Recs. Confusing to the market. Re new work, e.g., metrology is for ISO/IEC; regulation is out of FG scope.]

[ZTE: JCA only coordinate (SG13, SG17 only do QKDN). FG can research.]

[UK: last TSAG, SG2 welcome contributions but none to SG2. Phil volunteered to table JCA]

[US: agree with France quantum metrology outside ITU-T].

[Emirates: JCA only sends LS. FG will 3-4 meetings/yr. Support FG.]

[Canada: A.1 Section 2.2 is about JCA. JCA is needed for QKD. Not sure for qc, qin]

[Saudi: support FG. FG is the right cooperation tool with other SDOs.]

[Russia: support FG, bring in a consolidated platform for global standardization].

[China: qc and qmetro we will not study themselves, but implications for networks. JCA for existing work items. But JCA don’t produce deliverable. FG can attract all experts, fresh air. Future looking approach]

[Jordan: support FG than JCA.]

Updated Input





## [Huawei: last two lines redundant. Volunteer to enter ETSI work in this table][some are mature, products. Needs standards]Visualizing a Coordination JCA

[Editor’s note: Chairman has no experience in JCA and will ask the delegates for help to develop this part]

Offline discussions resulted that the main differences between a JCA and a Focus Group are

|  |  |
| --- | --- |
| JCA | FG |
| Cannot deliver output but work can be developed in attached entitiesJCA will agree and designate which entity carries the work | Can deliver output but it cannot be normative |
| Has only a chair/co-chair level | Can have sub groups |
| New comers can only developed documents in standardization structure but it can be recommendations, technical papers, etc. | New comers keep working in a Focus Group and do not need to subscribe to a specific SDO with no potentially intimidating regimentary mode |

JCA and FG can both accept any documents

A plan that was discussed to this specific situation is:

* JCA attached to TSAG
* JCA with 3 co-chairs
* Scope covering QKD, QIN, QIT, Metrology for ICT, Quantum Computing for ICT
* A meeting every 6-8 weeks
* Opened discussions, adhocs, to reach agreements from input documentation
* Distribution of the work in the right entity (ITU SG, ISO, etc.)
* Allows for New Work Items to be developed in entities
* Allows for Technical Papers, Technical reports to be developed in entities
* Entities can accept this work through incubation mechanisms and other mechanism to allow innovation

## Visualizing a potential hybrid model FG + JCA

[Editor’s note: This part will develop if and after the 2 above points are mature enough]

There is a model where we can have both FG and JCA

* FG scope QIN, QIT, Quantum Computer, Metrology
* JCA scope QKD

# Recommendations

## Consensus Reached

## Expressed Views

# Conclusions

[Editor’s note: The outcome of this document will be the consensus reached or not and it will trigger or not the drafting of the necessary ToR based on these agreements. We consider that if the consensus is reached, drafting the ToR should be nearly only editorial and whilst it will require care and attention should be a rather mechanical phase after this shared vision exercise is finished]

Chair conclusion:

Finished up to agenda item 6.

Recognizing need for coordination. But innovations are coming. 2 pieces JCA+FG. We have a lot for study.

AoB: US cannot hate you but dislike you.

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