

**STF 684 – QSCS - 101196442**

**Technical Description (Part B)**

(SMP STAND Standard)

**Version 6.0**

**19 August 2024**

# PROJECT FACT SHEET

**QSCS - STF 684 / [2024-06**]

|  |  |
| --- | --- |
| Reference Body | CYBER QSC / ISG QKD |
| EC/EFTA Funding | Manpower: 462 545 €  Travels: 30 900 €  Other Cost: 5 000€  **Total Budget : 498 445 €** |
| Project Duration | **36 months** |
| |  |  |  |  | | --- | --- | --- | --- | | **WP#** | **Task in BC** | **Task names** | **Amount** | | **WP1: Project management and coordination** | T0 | T1.1 Project set-up | 0€ | | T1 | T1.2 Project Management | 15 600€ | | **WP2: QSETS - Quantum Safe Enterprise Transport Security** | T2 | T2.1 New Work Item in TC CYBER QSC WG | 1 540€ | | T3 | T2.2 Initial draft reviewed | 21 560€ | | T4 | T2.3 Final draft reviewed | 53 900€ | | T5 | T2.4 Publication of standard | 10 780€ | | **WP3: AQSHKEX - Authenticated Quantum Safe Hybrid Key Exchange** | T6 | T3.1 New Work Item in TC CYBER QSC WG | 1 540€ | | T7 | T3.2 Initial draft reviewed | 5 390€ | | T8 | T3.3 Initial sketch of proof | 48 510€ | | T9 | T3.4 Public draft | 43 120€ | | T10 | T3.5 Conference submission | 10 780€ | | T11 | T3.6 Final draft | 21 560€ | | T12 | T3.7 Proof paper | 43 120€ | | T13 | T3.8 Reference implementation | 32 340€ | | T14 | T3.9 Standard publication | 10 780€ | | **WP4: PP - QKD Common Criteria Protection Profile – Key Processing Module** | T15 | T4.1 Create and approve New Work Item | 1 540€ | | T16 | T4.2 Review of protocols | 11 500€ | | T17 | T4.3 TOE boundary / interfaces | 11 500€ | | T18 | T4.4 Outline security modelling | 17 300€ | | T19 | T4.5 Early draft of PP | 22 500€ | | T20 | T4.6 Develop testing methods | 22 500€ | | T21 | T4.7 Refine PP | 33 085€ | | T22 | T4.8 Independent review | 16 500€ | | T23 | T4.9 Finalise PP, approval, and publication | 5 600€ | | |

# TECHNICAL DESCRIPTION (PART B)

|  |  |  |
| --- | --- | --- |
| **HISTORY OF CHANGES** | | |
| VERSION | PUBLICATION DATE | CHANGE |
| 1.0 | 01.03.2022 | Initial version (new MFF). |
| 2.0 | 01.06.2022 | Consolidation, formatting and layout changes. Tags added. |
| 3.0 | 27.05.2024 | Version submitted to Board for review |
| 4.0 | 04.06.2024 | Updated version addressing Board comments |
| 5.0 | 06.06.2024 | Final version for EISMEA Submission |
| 6.0 | 14.08.2024 | Comments addressed following ESR:   * Relevance:   + Updated 3.1 to clarify TC CYBER could consider upgrade to EN after publication of TS.   + Updated 1.3 to consider work in relation to JTC 22 roadmaps; also mentioning Liaison Statements between ISQ QKD and JTC 22 WG4, as well as TC CYBER and JTC 13. * Quality – Project Design and implementation   + Updated 2.7 mitigation to Risk No 1.   + Updated 4 Task descriptions to make clear conference will be European or international (MS12 mentions that ETSI conferences as examples if timing suitable), and example for independent reviewers for PP. * Quality – Project Team and Cooperation arrangements   + Update 2.5 about cooperation between TC CYBER and ISG QKD (1.1. already mentions that these groups work together to organise ETSI QSC Conference). |

## COVER PAGE

|  |  |
| --- | --- |
| **PROJECT** | |
| **Project name:** | Quantum Safe Cryptographic Solutions |
| **Project acronym:** | QSCS |
| **Project Duration (in months)** | 36 Months |
| **Coordinator contact:** | Jan Ellsberger, ETSI |

**TABLE OF CONTENTS**

[PROJECT FACT SHEET 2](#_Toc177653933)

[TECHNICAL DESCRIPTION (PART B) 3](#_Toc177653934)

[COVER PAGE 3](#_Toc177653935)

[PROJECT SUMMARY 5](#_Toc177653936)

[1. RELEVANCE 5](#_Toc177653937)

[1.1 Background and general objectives 5](#_Toc177653938)

[1.2 Needs analysis and specific objectives 6](#_Toc177653939)

[1.3 Complementarity with other actions and innovation 7](#_Toc177653940)

[2. QUALITY 8](#_Toc177653941)

[2.1 Concept and methodology 8](#_Toc177653942)

[2.2 Consortium set-up 8](#_Toc177653943)

[2.3 Project teams, staff and experts 9](#_Toc177653944)

[2.4 Consortium management and decision-making 11](#_Toc177653945)

[2.5 Project management, quality assurance and monitoring and evaluation strategy 11](#_Toc177653946)

[2.6 Cost effectiveness and financial management 13](#_Toc177653947)

[2.7 Risk management 13](#_Toc177653948)

[3. IMPACT 14](#_Toc177653949)

[3.1 Impact and ambition 14](#_Toc177653950)

[3.2 Communication, dissemination and visibility 15](#_Toc177653951)

[3.3 Sustainability and continuation 15](#_Toc177653952)

[4. WORKPLAN, WORK PACKAGES, ACTIVITIES, RESOURCES AND TIMING 17](#_Toc177653953)

[4.1 Work plan 17](#_Toc177653954)

[4.2 Work packages, activities, resources and timing 17](#_Toc177653955)

[Work Package 1 17](#_Toc177653956)

[Work Package 2 21](#_Toc177653957)

[Work Package 3 23](#_Toc177653958)

[Work Package 4 26](#_Toc177653959)

[Total Project costs 31](#_Toc177653960)

[4.3 Subcontracting 32](#_Toc177653961)

[Timetable 33](#_Toc177653962)

[5. OTHER 35](#_Toc177653963)

[5.1 Ethics 35](#_Toc177653964)

[5.2 Security 35](#_Toc177653965)

[6. DECLARATIONS 35](#_Toc177653966)

#@APP-FORM-SMPSTAND@#

#@PRJ-SUM-PS@# [This document is tagged. Do not delete the tags; they are needed for the processing.]

## PROJECT SUMMARY

|  |
| --- |
| This project defines specifications for constructing interoperable post-quantum cryptographic solutions that leverage both provable security based on computational assumptions of algorithmic solutions and composable security properties of Quantum Key Distribution (QKD) protocols.  (QSETS) A quantum-safe (QS) profile for ETS (Enterprise Transport Security), which is described in ETSI TS 103 523-3. The specification includes use of a static Diffie-Hellman key, and thought needs to go into how this can be made QS. The standard will specify the solution to this. A QS version of ETS is needed for enterprises who need to perform passive decryption of TLS sessions for reasons including:   * Application health monitoring and troubleshooting * Intrusion detection * Detection of malware activity * Detection of advanced DDOS attacks * Compliance audits   (AQSHKEX) A new TS in ETSI TC CYBER QSC to produce an authenticated hybrid key establishment method, including requirements for QKD. The existing TS on performing hybrid key exchange is being revised to use the latest FIPS ML-KEMs as a normative reference and to add mechanisms for static keys (secure against chosen ciphertext attacks). It also allows for the use of PSK QKD keys as part of the hybridization. The existing TS does not provide authentication, nor does it consider the information theoretical property of this mixing of QKD keys. The work will include development, testing and measurement of open-source software in ETSI's forge.  (PP) A Group Specification (GS) that is a Common Criteria Protection Profile – Key Processing Module for the certification of modules that can together provide secret random keys shared between nodes of a QKD network, including when not directly connected by a single QKD link. Such modules process QKD keys established separately by pairs of QKD modules. The PP addresses a critical element of trusted-node QKD networks, for which the security model has not yet been formalised in a certification framework. |

#§PRJ-SUM-PS§# #@REL-EVA-RE@# #@PRJ-OBJ-PO@#

## 1. RELEVANCE

### 1.1 Background and general objectives

|  |
| --- |
| The scope of this project directly addresses objectives 1, 2 and 3 of Topic 1, Standards for quantum-safe connectivity. The first two work items will develop standards suitable for use between EU member states, and more globally, directly addressing the recommendations of the EC Recommendation on Post-Quantum Cryptography [1] for member states to adopt harmonized implementations across member states. Applications that use standardized protocols to communicate can adopt standards being developed in other de facto standards organizations like the IETF. These solutions are highly specific to the application protocols. Many applications will require similar capability from a more generic construction. There is also a concrete need to provide an additional layer of authentication to QKD-established keys, e.g. end-to-end authentication within client applications based upon independent trust relationships. The industry, and the EC recommendations, suggest the use of hybrid for migration to quantum resistant technologies. ETSI TC CYBER QSC has demonstrated its ability to produce standards [2] that are supported by the necessary security proofs [3] that warrant wide-scale acceptance and deployment. These standards would be suitable for EU policy and regulations for adoption of quantum-resistant technology.  The Secure Connectivity Programme indicates the use of the combination of conventional solutions, post-quantum cryptography and possibly QKD in hybrid approaches for EU classified information. However, suitable standards for optimally combining conventional and post-quantum methods with QKD are needed and the standard on Authenticated Quantum Safe Hybrid Key Exchange proposes to address this.  Technologies for European quantum communication infrastructure are a policy priority under the 2024 Annual Union Work Programme (AUWP) for European standardisation. ETSI ISG QKD has an existing Group Specification that is a Protection Profile for QKD modules that use a prepare and measure QKD protocol [4]. Constructing a QKD network from pairs of QKD modules typically involves either securely forwarding keys through a series of trusted nodes connected by QKD links, or using another agreement protocol to produce secret random keys shared between nodes that are not directly connected by a QKD link. The European Quantum Communication Infrastructure (EuroQCI) aims to create an EU-wide quantum-safe network in which all parts of the network have been certified. A variety of network architectures are being adopted in different member states. It would be beneficial to standardise a PP for the certification of modules performing this core functionality and for this to be consistent with a range of QKD network architectures, including those being specified in ITU-T and ETSI. The proposed PP can contribute to ensuring the security of a class of quantum technology products used in planned deployments of pan-EU quantum-safe infrastructure, in line with one of the high-level objectives for standardization of quantum technologies in the AUWP 2024.  Further, ETSI & Institute for Quantum Computing has an established conference [4] dedicated to the dissemination of advancements in Quantum Safe Cryptography, Quantum Key Distribution and Quantum Computing. The TC CYBER QSC and ISG QKD play critical roles in this conference. This ensure that in addition to the direct reach of ETSI standards this work will be disseminated to a wider audience.  [1] <https://digital-strategy.ec.europa.eu/en/news/commission-publishes-recommendation-post-quantum-cryptography>  [2] <https://www.etsi.org/deliver/etsi_ts/103700_103799/103744/01.01.01_60/ts_103744v010101p.pdf>  [3] <https://eprint.iacr.org/2023/972.pdf>  [4] ETSI GS QKD 016 V2.1.1 (2024-01) Quantum Key Distribution (QKD);Common Criteria Protection Profile - Pair of Prepare and Measure Quantum Key Distribution Modules <https://www.etsi.org/deliver/etsi_gs/QKD/001_099/016/02.01.01_60/gs_QKD016v020101p.pdf>  [4] <https://www.etsi.org/events/2284-10th-etsi-iqc-quantum-safe-cryptography-event> |

### 1.2 Needs analysis and specific objectives

|  |
| --- |
| While there exist standards for hybridizing keys with pre-shared keys, there are no detailed standards that are optimised for hybridizing QKD keys with keys from other post-quantum methods. For applications to obtain the maximum benefit from the diversity offered by such hybridization and remain certifiable, an appropriate specification is required. With the Secure Connectivity Programme requiring attention to the combination of cryptographic techniques, including possibly QKD, the lack of an appropriate standard is problematic for both QKD vendors and application developers. This project will resolve this with the approval of a new TS for an appropriate method being the main measure of achievement.  The current absence of certified QKD network products is limiting the growth of the market for QKD products. Considerable investments have been made into developing QKD technology and establishing competition in the market. The development of PPs are steps towards the certification of products under the EUCC for a complete quantum-safe network. Achievement will be represented by publication by ETSI of a Group Specification developed by ISG QKD that is a Protection Profile for a key processing module that can work with other such modules to agree secret random keys across a trusted node QKD network, including between nodes that are not directly connected by a single QKD link. Currently no Protection Profile is available for such modules, which are security critical in a trusted node QKD network. It is anticipated that that the deliverable can be applicable to QKD networks adopting a variety of different network architectures.  QSETS Quantum Safe Enterprise Transport Security   * New Work Item: a new work item will be written, garner 3 additional supporters from the TC CYBER QSC WG, and be approved.  This will include the identification of a rapporteur. * Initial draft: An initial draft based on the general scope of the NWI will be created. * Final draft: An updated late-stage draft version. * Standard: ETSI TC CYBER will approve the TS for final publication. * NCSC   Associated with this is likely 4 ETSI meetings.  AQSHKEX Authenticated Quantum Safe Hybrid Key Exchange   * New Work Item: a new work item will be written, garner 3 additional supporters from the TC CYBER QSC WG, and be approved. This will include the identification of a rapporteur. * Initial draft: An initial draft based on the general scope of the NWI will be created. * Design & Proof Sketch: an early draft base on collaboration between the TC CYBER QSC WG and QKD ISG and a sketch of a security proof will be developed. * Public draft: a late-stage draft version of the standard approved for public review and comment period. * Conference submission: Present this public draft at a suitable European or international conference for generating awareness and traction for input. * Final draft: An updated late-stage draft version with written explanations on how received comments are addressed. * Proof paper: A published paper of the security proofs of the claims made in the standard. * Reference implementation: A reference implementation of the standard that includes test vectors to be included in the standard. * Standard: ETSI TC CYBER will approve the TS for final publication. * IETF will likely also standardized hybrid key establishment techniques, but these will be specific to their use in Internet protocols. Having an ETSI standard focused on primitives and technologies recommended for EU member states will reduce the overall costs of EU-centric standardized solutions for generic application development.   Associated with this is likely 7 ETSI meetings.  PP - QKD Common Criterial Protection Profile – Key Processing Module   * New Work Item: a new work item proposal will be written, garner 3 additional supporters from the ISG QKD Members, and be approved. This will include the identification of a rapporteur. * A review of protocols used for key agreement will be performed. * Discussions to decide a TOE Definition, including the TOE boundary and interfaces to accommodate a range of network architectures. A contribution outlining the TOE Definition, but not necessarily in formal CC language, to be accepted by ETSI ISG QKD. * Contributions and discussions in ETSI ISG QKD meetings to find a security model that can accommodate a range of network architectures and implementations. A contribution outlining the security problem definition and the intended security modelling of the PP, but not necessarily in formal CC language, to be accepted by ETSI ISG QKD. * Early draft of the NWI created based on the agreed TOE definition and security modelling. * Develop testing methods for non-standard aspects of the TOE. * Refine PP through discussions with ETSI ISG QKD. * Independent review by CC experts outside of ETSI ISG QKD. * Finalise PP and approval by ETSI ISG QKD of the GS for final publication.   Associated with this is likely 2 ETSI meetings. |

#§PRJ-OBJ-PO§# #@COM-PLE-CP@#

### 1.3 Complementarity with other actions and innovation

|  |
| --- |
| The U.S. Commerce Department will publish new Federal Information Processing Standards (FIPS) for post quantum cryptography (PQC), current draft FIPS 203 [1], FIPS 204[2] and FIPS 205 [3]. ISO will revise ISO/IEC 18033-2, Encryption algorithms — Part 2: Asymmetric ciphers to contain the BSI-recommended FrodoKEM. These standards will address the core cryptographic standards to be adopted by other standards developing organizations (SDO) and application developers. There is still a lot of innovation on how to use these standards with existing standardized algorithms and quantum key distribution (QKD) to achieve higher level needs of systems, such as key establishment and authenticated key establishment. The IETF will naturally take the lead when it comes to updating their protocols to post-quantum cryptography. There are a number of other applications and communication environments that will require quantum resistant key establishment and authenticated key establishment. Any such construction suitable for adoption must be accompanied with evidence of correctness, a proof of security based on widely accepted principals and assumptions. Further, these constructions must be both generic for application development and efficient, which are often in conflict with each other, and requires expertise to get right within the confines of provability.  Numerous projects from SECOQC through OpenQKD in the EU and those in China, Japan, Korea etc., have studied the construction of trusted-node QKD networks from a technical perspective. Standardisation work on QKD networks is progressing within ITU-T on a specific functional architecture, as well as related security requirements. These all offer important background for consideration in this work, which aims to deliver a PP suitable for direct use in product certifications. Within EuroQCI many EU member states are constructing national networks at the moment and networks are being constructed in several other countries. In the absence of a Technical Community on QKD it is particularly important to bring vendors together across borders within an SDO to make progress towards consensus on PPs for QKD network products. ISO/IEC 23738 and existing ETSI GS QKD 016, as well as other specifications have started to address QKD modules, although there remains a need to develop other background documents to support certification of QKD modules. This call excludes such work and focusses on complimentary developments towards certification of other aspects of quantum-safe networks. Markets are expected to remain restricted generally until the lack of certified products in all necessary security-critical parts of such networks can be overcome.  The draft CEN/CENELEC JTC 22 Working Group 4 Technical Report on “Gaps in QKD System and QKD Network Security Assurance” includes a section on “Gaps: QKD Network Security Assurance”. The draft is at an early stage but Work Package 4 addresses a gap that is central to this topic. Hybrid approaches including PQC and QKD as in Work Package 4 are identified as a use case in the “Standardization Roadmap on Quantum Technologies” from the former CEN-CENELEC Focus Group on Quantum Technologies (FGQT). ISG QKD will continue to send Liaison Statements to update this working group.  TC CYBER will send Liaison Statements to CEN/CENELEC JTC 13 to keep them apprised of work in this area to help ensure it is aligned with their standardization efforts and avoid duplication.  [1] <https://csrc.nist.gov/pubs/fips/203/ipd>  [2] <https://csrc.nist.gov/pubs/fips/204/ipd>  [3] <https://csrc.nist.gov/pubs/fips/205/ipd> |

#§COM-PLE-CP§# #§REL-EVA-RE§# #@QUA-LIT-QL@# #@CON-MET-CM@#

## 2. QUALITY

### 2.1 Concept and methodology

|  |
| --- |
| ETSI’s standards-making process is based on **consensus** – agreement between our members – and on openness. Our members:   * define what to standardize, and we have a particular focus on quantum-safe cryptography, * have a history and practice of obtaining the necessary resources to produce standards in a timely fashion, * and have a well-defined process from new work item to the approval of the final drafts.   The standards we produce truly respond to the **needs of the ICT industry**, as represented by our members. They are freely available to Industry, Academia and Government.  Where necessary, for cryptographic standards, ETSI members produce the necessary formal security proofs and publish them in external venues to provide additional transparency and evidence of the standards done at ETSI.  The Common Criteria is an international security certification scheme for IT products and the basis of the EUCC. Certification of QKD network products apart from QKD modules has largely not been considered in SDOs at the time of writing. The methodology is to first analyse the protocols in use, then to reach agreement upon the TOE boundary, interfaces and security modelling before attempting to write the formal CC text in an efficient manner. Independent experts will be brought in at a late stage of the development of the PP to ensure that fresh eyes provide a detailed review before publication. |

#§CON-MET-CM§# #@CON-SOR-CS@#

### 2.2 Consortium set-up

|  |
| --- |
| Not Applicable for ETSI |

### 2.3 Project teams, staff and experts

|  |  |  |
| --- | --- | --- |
| Name and function | Organisation | Role/tasks/professional profile and expertise |
| Léa Belloulou  Head of Funded Activities | ETSI | Head of ETSI funded Projects planning and control   * Management of the project costs and funding * Responsible for the Reporting to ETSI Management and EC/EFTA. * Management of audit processes on Funded projects * Management of contractual aspects * Monitoring of the administrative and financial tasks of the projects * Validation of milestones, payments |
| Kim Nordström for TC CYBER QSC  Carmine Rizzo for ISG QKD  Technical Officers | ETSI | ETSI Technical officer for the Technical Committees TC CYBER QSC and ISG QKD   * Act as prime ETSI Secretariat contact for the standardization activity. * Supervise the operation of the standardization activity under the relevant Directives, monitor progress of work programme. * Advise the group on the application of the relevant directives, drafting rules, and common best practice. * Ensure that deliverables are fit for purpose, and in line with the relevant directives, drafting rules and quality recommendations, and accompany them through the drafting and publication phases. * Act as secretary where appropriate, provide official reports of the group's meetings, highlighting actions and decisions. * Ensure that decisions, actions, approval of new work items and deliverables are properly recorded and communicated within the Secretariat. * Monitor activities of other relevant groups, both inside and outside of ETSI and advise of relevant activities as required. * Take appropriate actions to develop and maintain personal expertise in the relevant technical areas, and associated regulatory and market affairs. |
| Matthew Campagna  TC CYBER QSC Chair  Martin Ward ISG QKD Chair | ETSI | TC CYBER WG Chair and ISG Chair  The primary duties of a Chair:   * Ensure an efficient working of the TB/ISG and its Working Groups (in conjunction with the Vice-Chair(s), Working Group (WG) Chair(s) and Vice-Chair(s)). * Ensure the TB/ISGs’ activities adhere to ETSI Directives and its rules, policies and procedures. * Ensure that the Work Programme is kept up to date. * Maintain strict impartiality and act in the interest of ETSI and its members. * Ensure that the ETSI Guidelines for Antitrust Compliance are strictly observed. * Remind the members of the TB/ISG of their statutory obligations to submit IPR disclosures. * Endeavour to reach consensus on all issues, including the approval of draft ETSI deliverables.   Report to the OCG, Board and the General Assembly on the activities of the TB/ISG upon request. |

|  |
| --- |
| **Outside resources (subcontracting, seconded staff, etc)** |
| According to ETSI Technical Working Procedure on the selection of the service providers, ETSI will issue a call for expertise to get the necessary skills and resources as described below. A project manager will be appointed from one of the Service Providers and will be responsible for coordinating the execution of the tasks assigned to the individual Service Providers, according to the project requirements and following the technical direction given by ETSI TC CYBER QSC WG and ETSI ISG QKD.  The project Manager will possess project management experience, report-writing skills, experience of consensus building, presentations skills, experience of working in an international environment, and in liaising with other international organisations.  It is possible experts may span more than one of these roles.  The optimum number of experts will depend upon the responses received to the call for experts. For Work Package 4 a minimum of 2 experts will be require to allow for the independent review. If experts with different specialisms respond to the call it is anticipated that 3 or 4 experts could be selected.  Cryptographic Researcher (1) – Ph.D. in Mathematics, Computer Science or equivalent, 5+ years experience in the development of security proofs for cryptographic constructions.  Software Developer (1) – B.S. in Mathematics, Computer Science, with 5+ years in developing cryptographic implementations.  Rapporteuer (2) – B.A. or B.S. in technical field. 5+ years experience defining standards, ideally cryptographic standards.  QKD Researcher / Developer – Ph.D. in Physics, Engineering, Mathematics, Computer Science or equivalent, 5+ years experience in the development of QKD, or QKD network solutions or key management systems.  Common Criteria Practitioner – Certified Common Criteria Evaluator or 5+ years’ experience including multiple projects involving Protection Profiles.  C:\Users\kozubal\AppData\Local\Microsoft\Windows\INetCache\Content.MSO\CCC5FF89.tmp  Using the ETSI-defined call for expertise and contractor selection process outlined above, the selected experts will begin the project with the preparatory meeting at the end of the second month of the project (M2). |

### 2.4 Consortium management and decision-making

|  |
| --- |
| Not applicable for ETSI |

#§CON-SOR-CS§# #@PRJ-MGT-PM@#

### 2.5 Project management, quality assurance and monitoring and evaluation strategy

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| The chairs of TC CYBER QSC and ISG QKD follow the ETSI Chair’s Guide [1], to ensure an efficient working of the TB/ISG and its Working Groups (in conjunction with the Vice-Chair(s), Working Group (WG) Chair(s) and Vice-Chair(s)). They will ensure the TB/ISGs’ activities adhere to ETSI Directives and its rules, policies and procedures, and ensure that the Work Programme is kept up to date. They will maintain strict impartiality and act in the interest of ETSI and its members and ensure that the ETSI Guidelines for Antitrust Compliance are strictly observed.  The Working Group chairs, using ETSI’s consensus practices, are responsible for identifying Rapporteur’s that are suitable for completing new work items according to the Work Programme. Further, chairs are responsible for ensuring that Rapporteur’s follow the ETSI Rapporteur’s Guide [2].  [1] <https://portal.etsi.org/Portals/0/Chairs_Guide.pdf>  [2] <https://portal.etsi.org/Portals/0/TBpages/edithelp/Docs/Guides/ETSI_Rapporteurs_guide.pdf>  The overall progress of the work will be the responsibility of the Project Leader. Progress within each Work Package will also be monitored by the Chair and Technical Officer of TC CYBER QSC or ISG QKD, depending on the Work Package.  For Work Packages 2 and 3 TC CYBER and WG QSC will operate its usual procedures for the development and approval of ETSI Technical Specifications. The Rapporteur will be responsible for progressing the development of the work and seeking consensus on the content of the deliverable. For Work Package 3 a late-stage draft will be released as a public draft for comments and awareness will be generated through a European or international conference submission announcing the publication of this draft. The security proof will be published in an external venue for further external scrutiny.  For Work Package 4 ISG QKD will operate its usual procedures for the development and approval of an ETSI Group Specification. The Rapporteur will be responsible for progressing the development of the work and seeking consensus on the content of the deliverable. Plenary meetings will be held twice per year with remote access and monthly meetings will be held online. Ad Hoc / Rapporteur Group meetings can be used where further discussions are required and these can be dedicated to Work Package 4 activities to improve efficiency. Some milestones involve preliminary work being contributed to and approved by ISG QKD and such contributions may be the responsibility of other experts assigned to the related task(s). All technical decisions will be subject to review by ISG QKD. Leadership by the Rapporteur in ensuring that high quality drafts are submitted to ISG QKD will help the work to proceed efficiently. Ultimately the appropriateness and correctness of the PP for products for use in QKD networks will depend upon review by members of the ISG, with additional quality monitoring by the by Chair and Technical Officer. T4.8 has been included to ensure that the final PP formally conforms to the Common Criteria through an independent review.  WG QSC and ISG QKD will exchange Liaison Statements to inform each other of progress in relevant activities. ETSI Members are able to join work in both groups and will be encouraged to do so to promote cooperation. Where appropriate, the Chairs will arrange for ETSI Members and ISG QKD Participants to be able to meet (including online) to discuss together. A particular need is anticipated towards the start of the activities under Work Package 3, when the requirements for Authenticated Quantum Safe Hybrid Key Exchange are being considered.  All ETSI deliverables will be subject to the usual checks in terms of quality and conformance to ETSI drafting rules by ETSI’s editHelp service. For Work Package 4 review by editHelp before approval will be requested so that any editorial issues etc. are resolved before final reviews are performed to ensure they do not impact conformance to the Common Criteria.   |  |  |  |  |  |  | | --- | --- | --- | --- | --- | --- | | *Criteria* | *Definitely* | *Satisfactorily* | *Somewhat* | *Not at all* | *Not applicable* | | *Deliverable matches the expected requirements* |  |  |  |  |  | | *Objectives are clear and in line with the planned activities?* |  |  |  |  |  | | *Issues at project level are properly treated?* |  |  |  |  |  | | *Author responds to readers’ needs?* |  |  |  |  |  | | *Technical approaches used are appropriate?* |  |  |  |  |  | | *Content is well organised?* |  |  |  |  |  | | *Issues raised are relevant?* |  |  |  |  |  | | *Contents contribute to the state of the art?* |  |  |  |  |  | | *Conclusions (if any) are valid?* |  |  |  |  |  | | *Deliverable is complete (no major parts missing)?* |  |  |  |  |  | | *Deliverable is formally correct.* |  |  |  |  |  | |

#§PRJ-MGT-PM§# #@FIN-MGT-FM@#

### 2.6 Cost effectiveness and financial management

|  |
| --- |
| ETSI Secretariat doesn’t have technical experts as staff thus all the EC/EFTA funded projects are subcontracted.  For reasons linked to French social Regulations and to avoid a risk of subordinate relationship that could trigger negative consequences for ETSI, on advice of its lawyers, ETSI has abandoned the principle of a daily rate to contract its experts and ETSI works now under the principle of service contracts. The contractor is bound by delivering the agreed service for the price determined. It is the responsibility of the service provider to make available the necessary experts to deliver the expected service. The company contracted may allocate different experts of different seniority and expertise level, having each a different daily rate.  Each subcontractor is allocated to specific tasks with an expected level of contribution. The financial resources allocated to the subcontractor are calculated on this principle.  At the start of the project, ETSI develops a baseline cost plan. It is calculated with the cost of the tasks and the scheduled progress of task at each milestone cut-off date. This baseline cost plan provides the costs at each milestone cut-off date.  The milestone payment schedule for each subcontractor is then calculated considering the baseline cost plan and the expected level of contribution. The milestone payment schedule is contractual.  The subcontractors’ payments are submitted to the validation of the project milestones. The TC and ETSI proceed to the validation of the milestone.  As the number of person days and the maximum daily rates are requested in the part 0 Introduction, of the EISMEA Call for Proposals, and taking into account the needed expertise, the maximum daily rate is assumed to be 1,300 EUR with an average daily rate ~847 EUR and is based on the market price.  The estimated effort for all work packages amount to approximatively 546 days of work spread out over a period of 36 months.  Travels are strongly reduced, as teleconferences will be the most common tool for organising technical meetings. Travels are accounted to allow for face-to-face participation in the ETSI Technical Committee and for coordination.  ETSI Secretariat ensures that neither the project as a whole nor any part of it have benefited from any other EU Grant thus avoiding any trouble with double funding. |

#§FIN-MGT-FM§# #@RSK-MGT-RM@#

### 2.7 Risk management

|  |  |  |  |
| --- | --- | --- | --- |
| Risk No | Description | Work package No | Proposed risk-mitigation measures |
| **1** | **Insufficient responses to calls for experts. (Low risk)** | **1** | **Additional calls for experts can be held after consideration of how work can be redistributed. Liaison Statements to CEN/CENELEC JTC 22 WG4 and/or JTC 13 could be used if additional calls require wider visibility.** |
| **2** | **Many late-stage changes proposed for PP give rise to unnecessary work in redrafting formal CC content. (Medium risk)** | **4** | **Discuss and agree the TOE description, security modelling, and outline before commencing formal CC drafting.** |
| **3** | **Developing a formal security proof of hybrid key establishment and authentication may not be feasible in the timeframe (Medium risk)** | **3** | **Replace the publication of a formal security proof with an Appendix that has less formal security consideration. Accept a little more risk in the output.** |
| **4** | **New post quantum schemes are broken. (Low risk)** | **2, 4** | **Abandon WP 2, and work on WP2 using QKD in WP 3.** |
| **5** | **Failure to meet milestone deadlines (Medium/High risk)** | **All** | **The project’s tried and tested management methodology and its transparency will naturally flag potential progress-threats very early before they become a problem. This will enable us to respond quickly, via effort re-allocation or re-prioritisation, to any changes or deviations that may affect the plan.** |

#§RSK-MGT-RM§# #§QUA-LIT-QL§# #@IMP-ACT-IA@#

## 3. IMPACT

### 3.1 Impact and ambition

|  |
| --- |
| QSETS will provide middlebox vendors with quantum-safe mechanisms for performing passive decryption of TLS sessions in environments where both the client and server, and by inference the data being exchanged over the TLS session, are under the control of the same entity. TLS encryption is often stipulated by internal or external security policies, but access to the unencrypted packet data is necessary to ensure these policies are met. Enterprises that require the use of Middlebox technology want to know these solutions are using secure and vetted mechanisms that are standardized. This change would allow middlebox technology to remain security against a potential future quantum adversary.  AQSKHEX will provide the necessary security proof to support a new standard for performing authenticated quantum-safe key exchanges. It will do so with consideration of how to also include a quantum key distributed (QKD) key. This standard will be utilized by application developers to develop interoperable standardized key establishment that are quantum resistant. To assist in this development, a reference implementation will allow integrators to develop interoperable implementations. This supports the EC recommendation for interoperable migration to post-quantum cryptography across EU member states.  Having an EU-standard that incorporates algorithms and technologies specifically recommended for use in EU member states allow for the development of new products and services for the EEA. Ideally, these standards will allow European manufacturers innovate new products and services target for the EU based on the proven security of standardized techniques. Some examples are EV charging, vehicle-to-infrastructure communication, IoT applications, DWDM link encryption solutions.  TC Cyber has converted Technical Specifications into European standards (EN) in the past. Technical Specifications developed under this work plan could be considered for conversion into ENs in the future.  QKD vendors, key management system vendors, and application vendors can use the standard for hybridizing QKD keys in their products. The availability of standardized protocols for such hybridization will increase confidence in products offering key hybridization, as well as removing a significant barrier to their certification.  Vendors of systems to manage keys within trusted-node QKD networks can develop products that conform to the new PP, making it easier for them to present products for certification. The construction of QKD networks consisting of products that have all been certified requires a full stack of certified devices to be available. One of the priorities EuroQCI has identified is certification across complete quantum safe networks and the new PP can help towards addressing one aspect of this.  Large investments within the EU have been directed towards establishing a range of SMEs producing QKD products. These include companies attempting to sell QKD modules, those trying to sell key management products, and those specialising in products to provide control and management functionality within QKD networks. In Asia some countries have already pushed ahead to create certification schemes for local QKD products. A robust EU certification scheme can help build trust in products certified under it, but the fact that there are currently no products certified within the EU is a substantial barrier to the development of its SMEs.  Certification of new technologies is difficult and expensive, presenting a particular challenge for new SMEs. The availability of PPs can help to bring forward the date at which such companies can be able to present products for certification. The ambition includes helping SMEs to achieve this within a timeframe in which they can sustain themselves through the sale of products that are not certified. In the longer-term such companies could form the basis of a wider European industry for quantum technologies.  This call excludes the quantum layer for which work in both ISO/IEC and ETSI is available as an initial starting for point towards the certification of QKD modules. The PP to be developed can help support the certification of security-critical key processing products that are common in trusted node QKD networks. |

#§IMP-ACT-IA§# #@COM-DIS-VIS-CDV@#

### 3.2 Communication, dissemination and visibility

|  |
| --- |
| **Communication, dissemination and visibility of funding**  *Describe the communication and dissemination activities which are planned in order to promote the activities/results and maximise the impact (to whom, which format, how many, etc.). Clarify how you will reach the target groups, relevant stakeholders, policymakers and the general public and explain the choice of the dissemination channels.*  *Describe how the visibility of EU funding will be ensured.* |
| ETSI publications are freely available for download so there is no barrier for adoption by vendors, including SMEs, and any potential customer of such vendors can access the standards to understand the implication of conformity statements by vendors. The activities will also be promoted in international meetings, for example ETSI / IQC Quantum Safe Cryptography Conferences and ETSI Security Conferences, as well as in general ETSI communications.  WP3 also includes a conference submission and proof paper. |

#§COM-DIS-VIS-CDV§# #@SUS-CON-SC@#

### 3.3 Sustainability and continuation

|  |
| --- |
| **Sustainability, long-term impact and continuation**  *Describe the follow-up of the project after the EU funding ends. How will the project impact be ensured and sustained?*  *What will need to be done? Which parts of the project should be continued or maintained? How will this be achieved? Which resources will be necessary to continue the project? How will the results be used?*  *Are there any possible synergies/complementarities with other (EU funded) activities that can build on the project results?* |
| ETSI TC CYBER QSC and ETSI ISG QKD are both groups that have been active in their technical areas for some years and intend to continue their work. The need to deploy quantum-safe cryptography is becoming increasingly well understood.  The EC recently published a Commission Recommendation on a Coordinated Implementation Roadmap for the transition to Post-Quantum Cryptography. This document describes that for a harmonized implementation of Post-Quantum Cryptography across the Union it is essential to develop common European standards and develop a framework for identifying and selecting Post-Quantum Cryptography algorithms to be deployed in the digital networks and services across the Union. This is expected to be a driver for continued standards development on interoperable post-quantum cryptographic solutions.  Directive (EU) 2022/2555 (repealing the NIS2 Directive, which first introduced some of the requirements) requires each Member State to adopt a national cybersecurity strategy, including policies in relation to the certification of ICT products. It also empowers the Commission to require categories of essential and important entities to use certain certified ICT products or obtain a certificate under a European cybersecurity certification scheme. This Directive and the creation of the EUCC by ENISA after a request from the Commission following the Cybersecurity Act, and subsequent focus on planning for EUCC certification within EuroQCI are driving customers to ask vendors for certified security products. This is particularly challenging for SMEs developing products based on new technology such as QKD, and a range of additional standards will be important to support the certification of both QKD modules and products for other parts of complete quantum-safe networks.  Horizon Europe and EuroQCI include projects considering the security of quantum safe systems, including post-quantum cryptographic solutions and QKD. It is hoped that results can feed into future standardisation activities. |

#§SUS-CON-SC§#

#@WRK-PLA-WP@#

## 4. WORKPLAN, WORK PACKAGES, ACTIVITIES, RESOURCES AND TIMING

### 4.1 Work plan

|  |
| --- |
| **Work plan**  *Provide a brief description of the overall structure of the work plan (list of work packages or graphical presentation (Pert chart or similar)).* |
| The work plan includes one administrative work package, two work packages that will be developed in ETSI TC CYBER QSC (\*) and one in ETSI ISG QKD (†).  Work Package 1: Project management and coordination  Work Package 2 (\*): QSETS – Quantum Safe Enterprise Transport Security  Work Package 3 (\*): AQSHKEX - Authenticated Quantum Safe Hybrid Key Exchange  Work Package 4 (†): PP - QKD Common Criterial Protection Profile – Key Processing Module |

### 4.2 Work packages, activities, resources and timing

|  |
| --- |
| **WORK PACKAGES** |

#### Work Package 1

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Work Package 1: Project management and coordination** | | | | | | | | | | | | | | | |
| **Duration:** | | | M1 - M36 | | **Lead Beneficiary:** | | | | ETSI | | | | | | |
| **Objectives** | | | | | | | | | | | | | | | |
| * Ensure efficient and effective management of the project, including planning, contractual, monitoring, reporting and audit functions etc. | | | | | | | | | | | | | | | |
| **Activities and division of work (WP description)** | | | | | | | | | | | | | | | |
| Task No  (continuous numbering linked to WP) | Task Name | | | | | Description | | | | | Participants | | | | In-kind Contributions and Subcontracting  (Yes/No and which) |
| Name | | Role  (COO, BEN, AE, AP, OTHER) | |
| T1.1 | Project Setup | | | | | ETSI Secretariat will arrange a call for experts. For Work Packages 1 to 3 ETSI TC CYBER QSC Chair will review the potentials candidates and select those to best meet the workplan, including the assignment of the project leader. For Work Package 4 ETSI ISG QKD Chair will review the potentials candidates and select those to best meet the workplan.  ETSI Secretariat will make arrangements for project members (service contracts, etc…) The ETSI TC Chair will check that the objectives of all WPs are clearly recognised by the participants | | | | | ETSI,  TC WG & ISG Chairs | | COO | | In-kind |
| T1.2 | Project Management | | | | | * The overall management of the project will be under the responsibility of the Project Leader. He will ensure effective coordination among the different Tasks, working in close collaboration with the different Task Leaders and supervising them if needed, but also with ETSI TC CYBER QSC WG and ETSI ISG QKD representatives.   The overall project management consists in:   * Planning, organisation and preparation of meetings * Interacting with TC CYBER QSC WG * Interacting with ISG QKD * On-going reporting * Participation at TC CYBER QSC meetings * Delivery of progress reports | | | | | ETSI | | COO | | Yes, subcontracting |
| **Milestones and deliverables (outputs/outcomes)** | | | | | | | | | | | | | | | |
| Milestone No  (continuous numbering not linked to WP) | | Milestone Name | | Work Package No | | | Lead Beneficiary | Description | | | | Due Date  (month number) | | Means of Verification | |
| MS1 | | Project Team established | | 1 | | | ETSI | STF members selected and hired by ETSI. | | | | 2 | | Contracts signed by ETSI and all STF members. | |
| MS2 | | First Intermediate results have been delivered | | 1 | | | ETSI | First term Progress Report with the achieved results approved by TC CYBER QSC and sent to EISMEA | | | | 12 | | Report by ETSI Staff to EISMEA | |
| MS3 | | Second Intermediate results have been delivered | | 1 | | | ETSI | Second term Progress Report with the achieved results approved by TC CYBER QSC and sent to EISMEA | | | | 24 | | Report by ETSI Staff to EISMEA | |
| MS4 | | Final results have been delivered | | 1 | | | ETIS | Final Report with the achieved results approved by TC CYBER QSC and sent to EISMEA | | | | 36 | | Report by ETSI Staff to EISMEA | |
| Deliverable No  (continuous numbering linked to WP) | | Deliverable Name | | Work Package No | | | Lead Beneficiary | Type | | Dissemination Level | | Due Date  (month number) | | Description  (including format and language) | |
| D1.1 | | 1st Annual Report | | 1 | | | ETSI | R *—* Document,report | | SEN *—* Sensitive | | 12 | | * The activities performed until month 12, the coordination work of the activities and the production of the expected deliverables anticipated in the work-plan. * The latest drafts of the deliverables are available according to the time plan. * Overview of ad-hoc meetings if necessary. * The plan for the future activities to complete the deliverables and further expected (coordination) meetings. * Quality intermediate report. * Standard EISMEA reporting   English | |
| D1.2 | | 2nd Annual Report | | 1 | | | ETSI | *[*R *—* Document,report | | SEN *—* Sensitive | | 24 | | * The activities performed until month 24, the coordination work of the activities and the production of the expected deliverables anticipated in the work-plan. * The latest drafts of the deliverables are available according to the time plan. * Overview of ad-hoc meetings if necessary. * The plan for the future activities to complete the deliverables and further expected (coordination) meetings. * Quality intermediate report. * Standard EISMEA reporting   English | |

|  |
| --- |
| **Estimated budget — Resources** |
| See TOTAL PROJECT COSTS table below. |

#### Work Package 2

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Work Package 2: QSETS - Quantum Safe Enterprise Transport Security** | | | | | | | | | | | | | | | |
| **Duration: 18 months** | | | M3 – M20 | | **Lead Beneficiary:** | | | | ETSI | | | | | | |
| **Objectives** | | | | | | | | | | | | | | | |
| * Produce a new ETSI Technical Specification for a quantum-safe (QS) profile for ETS (Enterprise Transport Security), which is described in ETSI TS 103 523-3. | | | | | | | | | | | | | | | |
| **Activities and division of work (WP description)** | | | | | | | | | | | | | | | |
| Task No  (continuous numbering linked to WP) | Task Name | | | | | Description | | | | | Participants | | | | In-kind Contributions and Subcontracting  (Yes/No and which) |
| Name | | Role  (COO, BEN, AE, AP, OTHER) | |
| T2.1 | New Work Item in TC CYBER QSC WG | | | | | Develop a new work item will be written. Support from 3 additional members of TC CYBER QSC WG will be signed on. | | | | | ETSI | | COO | | Yes, subcontracting |
| T2.2 | Initial draft reviewed | | | | | An initial draft based on the general scope of the NWI will be created and reviewed at an ETSI TC CYBER QSC WG meeting. | | | | | ETSI | | COO | | Yes, subcontracting |
| T2.3 | Final draft reviewed | | | | | An updated late-stage draft for final review will be submitted to a TC CYBER QSC WG meeting where it will be reviewed and accepted for standardization. | | | | | ETSI | | COO | | Yes, subcontracting |
| T2.4 | Publication of standard | | | | | ETSI TC CYBER will approve the TS for final publication. | | | | | ETSI | | COO | | Yes, subcontracting |
| **Milestones and deliverables (outputs/outcomes)** | | | | | | | | | | | | | | | |
| Milestone No  (continuous numbering not linked to WP) | | Milestone Name | | Work Package No | | | Lead Beneficiary | Description | | | | Due Date  (month number) | | Means of Verification | |
| MS5 | | NWI approved | | 2 | | | ETSI | A new work item with three supporters will be reviewed by ETSI TC CYBER QSC WG and accepted by the committee. | | | | 4 | | Visible in ETSI TC CYBER QSC WG portal as a new work item | |
| MS6 | | Initial draft | | 2 | | | ETSI | An initial draft based on the scope of the NWI will be developed and submitted to an ETSI TC CYBER QSC WG meeting and reviewed. | | | | 8 | | Visible in ETSI TC CYBER QSC WG portal under current work items. | |
| MS7 | | Final draft | | 2 | | | ETSI | A final draft of the specification after a few iterations of WG reviewed drafts submitted for approval. | | | | 17 | | Visible in ETSI TC CYBER QSC WG portal under current work items. | |
| MS8 | | Published Standard | | 2 | | | ETSI | The publication of the Technical Specification | | | | 20 | | Visible as a published ETSI TS | |
| Deliverable No  (continuous numbering linked to WP) | | Deliverable Name | | Work Package No | | | Lead Beneficiary | Type | | Dissemination Level | | Due Date  (month number) | | Description  (including format and language) | |
| D2.1 | | TS on QSETS | | 1 | | | ETSI | R *—* Document,report | | PU *—* Public | | 20 | | This will be a published TS in English according to existing ETSI specification practices and procedures. | |

|  |
| --- |
| **Estimated budget — Resources** |
| See TOTAL PROJECT COSTS table below. |

#### Work Package 3

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Work Package 3: AQSHKEX - Authenticated Quantum Safe Hybrid Key Exchange** | | | | | | | | | | | | | | | |
| **Duration: 24** | | | M3 - M26 | | **Lead Beneficiary:** | | | | ETSI | | | | | | |
| **Objectives** | | | | | | | | | | | | | | | |
| * Produce a new ETSI Technical Specification for an authenticated hybrid key establishment method, including requirements for QKD. * Produce and publish a paper that contains the necessary security proof. * Develop a reference implementation for the generation of test vectors and the facilitation the interoperability of implementations. | | | | | | | | | | | | | | | |
| **Activities and division of work (WP description)** | | | | | | | | | | | | | | | |
| Task No  (continuous numbering linked to WP) | Task Name | | | | | Description | | | | | Participants | | | | In-kind Contributions and Subcontracting  (Yes/No and which) |
| Name | | Role  (COO, BEN, AE, AP, OTHER) | |
| T3.1 | New Work Item in TC CYBER QSC WG | | | | | Develop a new work item will be written. Support from 3 additional members of TC CYBER QSC WG will be signed on. | | | | | ETSI | | COO | | Yes, subcontracting |
| T3.2 | Initial draft reviewed | | | | | An initial draft based on the general scope of the NWI will be created and reviewed at an ETSI TC CYBER QSC WG meeting. | | | | | ETSI | | COO | | Yes, subcontracting |
| T3.3 | Initial sketch of proof | | | | | An initial sketch of the security proof will be developed and presented at a TC CYBER QSC WG meeting | | | | | ETSI | | COO | | Yes, subcontracting |
| T3.4 | Public draft | | | | | A late-stage draft will be reviewed by the TC CYBER QSC WG and approved for release as a public draft for comments | | | | | ETSI | | COO | | Yes, subcontracting |
| T3.5 | Conference submission | | | | | A European or international conference submission announcing the publication of this draft to generate awareness and alert the community to comment. | | | | | ETSI | | COO | | Yes, subcontracting |
| T3.6 | Final draft | | | | | A final draft for TC CYBER WSC WG review will be voted for standardization. | | | | | ETSI | | COO | | Yes, subcontracting |
| T3.7 | Proof paper | | | | | The security proof will be finalized and published in an external venue. | | | | | ETSI | | COO | | Yes, subcontracting |
| T3.8 | Reference implementation | | | | | A reference implementation for the generation of test vectors will be published to ETSI Forge | | | | | ETSI | | COO | | Yes, subcontracting |
| T3.9 | Standard publication | | | | | The approved specification will be made public as a TS | | | | | ETSI | | COO | | Yes, subcontracting |
| **Milestones and deliverables (outputs/outcomes)** | | | | | | | | | | | | | | | |
| Milestone No  (continuous numbering not linked to WP) | | Milestone Name | | Work Package No | | | Lead Beneficiary | Description | | | | Due Date  (month number) | | Means of Verification | |
| MS9 | | New Work Item in TC CYBER QSC WG | | 3 | | | ETSI | A new work item with three supporters will be reviewed by ETSI TC CYBER QSC WG and accepted by the committee. | | | | 4 | | Visible in ETSI TC CYBER QSC WG portal as a new work item | |
| MS10 | | Initial draft reviewed | | 3 | | | ETSI | An initial draft based on the scope of the NWI will be developed and submitted to an ETSI TC CYBER QSC WG meeting and reviewed. | | | | 8 | | Visible in ETSI TC CYBER QSC WG portal under current work items. | |
| MS11 | | Public draft | | 3 | | | ETSI | A late-stage draft of the TS will be made public for external review. | | | | 17 | | Visible in ETSI TC CYBER QSC WG portal and a public accessible docbox ETSI url. | |
| MS12 | | Conference submission | | 3 | | | ETSI | A presentation at a public European or international conference, like ETSI Security Week or ETSI QSC Conference | | | | 17 | | A conference proceedings listing this presentation. | |
| MS13 | | Final draft | | 3 | | | ETSI | A final draft of the specification after a few iterations of WG reviewed drafts submitted for approval. | | | | 20 | | Visible in ETSI TC CYBER QSC WG portal under current work items. | |
| MS14 | | Proof paper | | 3 | | | ETSI | A research paper containing a formal security proof of the construction. | | | | 26 | | Published externally. There will be a publicly reachable URL like eprint.iacr.org. | |
| MS15 | | Reference implementation | | 3 | | | ETSI | An open-source implementation of the specification. | | | | 26 | | A project in ETSI software repository. | |
| Deliverable No  (continuous numbering linked to WP) | | Deliverable Name | | Work Package No | | | Lead Beneficiary | Type | | Dissemination Level | | Due Date  (month number) | | Description  (including format and language) | |
| D3.1 | | TS on AQSHKEX | | 3 | | | ETSI | R *—* Document,report | | PU *—* Public | | 26 | | This will be a published TS in English according to existing ETSI specification practices and procedures. | |

|  |
| --- |
| **Estimated budget — Resources** |
| See TOTAL PROJECT COSTS table below. |

#### Work Package 4

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Work Package 4: PP - QKD Common Criterial Protection Profile – Key Processing Module** | | | | | | | | | | | | | | | |
| **Duration:** | | | M3 - M35 | | **Lead Beneficiary:** | | | | ETSI | | | | | | |
| **Objectives** | | | | | | | | | | | | | | | |
| * To develop a new Group Specification that is a Common Criteria Protection Profile for a Key Processing Module that can work with other such modules to agree secret random keys across a trusted node QKD network, including between nodes that are not directly connected by a single QKD link. * Support the certification of products producing keys shared across multiple QKD links for use in quantum-safe networks. | | | | | | | | | | | | | | | |
| **Activities and division of work (WP description)** | | | | | | | | | | | | | | | |
| Task No  (continuous numbering linked to WP) | Task Name | | | | | Description | | | | | Participants | | | | In-kind Contributions and Subcontracting  (Yes/No and which) |
| Name | | Role  (COO, BEN, AE, AP, OTHER) | |
| T4.1 | Create and approve New Work Item | | | | | A New Work Item proposal will be submitted with the support of four Members from ISG QKD and proposing a Rapporteur. The NWI will be approved and added to the ETSI Work Programme. | | | | | ETSI,  ISG QKD Chair | | COO | | In-kind |
| T4.2 | Review of protocols | | | | | Consider various protocols used to agree keys from QKD keys established over multiple QKD links. Write a contribution with an overview of each known protocol commenting on implications for interfaces and modelling and obtain approval by ETSI ISG QKD. | | | | | ETSI | | COO | | Yes, subcontracting |
| T4.3 | TOE boundary / interfaces | | | | | Lead discussions within ETSI ISG QKD and seek consensus on the TOE description, including the TOE boundary and a set of interfaces that can be applicable to a range of common QKD network architectures and implementations. Write a contribution explaining the agreed TOE description (not necessarily in formal CC language) and obtain approval by ETSI ISG QKD. | | | | | ETSI | | COO | | Yes, subcontracting |
| T4.4 | Outline security modelling | | | | | Lead discussions within ETSI ISG QKD and seek consensus on core aspects of the security modelling for the PP. Write a contribution explaining the agreed modelling (not necessarily in formal CC language) and obtain approval by ETSI ISG QKD. | | | | | ETSI | | COO | | Yes, subcontracting |
| T4.5 | Early draft of PP | | | | | Develop an early draft of the PP based on the agreed TOE definition and security modelling. Submit this draft to ETSI ISG QKD and present this to a meeting. | | | | | ETSI | | COO | | Yes, subcontracting |
| T4.6 | Develop testing methods | | | | | Lead discussions within ETSI ISG QKD and develop a set of testing methods for TOE using common protocols. Submit this draft to ETSI ISG QKD. | | | | | ETSI | | COO | | Yes, subcontracting |
| T4.7 | Refine PP | | | | | Gather comments from ETSI ISG QKD and the independent reviewers under T4.8. Lead discussions in ETSI ISG QKD (call Rapporteur Group Meetings if appropriate) to resolve concerns and refine the PP. | | | | | ETSI | | COO | | Yes, subcontracting |
| T4.8 | Independent review | | | | | CC experts who were not involved in the development work will be engaged to review the PP for conformance to the CC / CEM, internal consistency etc. and report any problems found to ETSI ISG QKD for correction. The CC experts could be a small team from a single evaluation laboratory, for example. | | | | | ETSI | | COO | | Yes, subcontracting |
| T4.9 | Finalise PP, approval, and publication | | | | | Finalise the PP, obtain approval for publication from ETSI ISG QKD, and progress to publication by ETSI ISG QKD. | | | | | ETSI | | COO | | Yes, subcontracting |
| **Milestones and deliverables (outputs/outcomes)** | | | | | | | | | | | | | | | |
| Milestone No  (continuous numbering not linked to WP) | | Milestone Name | | Work Package No | | | Lead Beneficiary | Description | | | | Due Date  (month number) | | Means of Verification | |
| MS16 | | NWI for PP in Work Programme | | 4 | | | ETSI | New Work Item (GS for PP) approved and added to ETSI Work Programme. | | | | 4 | | Visible in ETSI online Work Programme | |
| MS17 | | Approved contribution on review of protocols | | 4 | | | ETSI | Contribution documenting the review of protocols approved by ETSI ISG QKD. | | | | 9 | | Decision visible in ETSI portal | |
| MS18 | | Approved contribution on TOE boundary / interfaces | | 4 | | | ETSI | Contribution documenting the agreed TOE description but not necessarily in formal CC language approved by ETSI ISG QKD. | | | | 12 | | Decision visible in ETSI portal | |
| MS19 | | Approved contribution outlining security modelling | | 4 | | | ETSI | Contribution documenting the agreed outline security modelling for the PP but not necessarily in formal CC language approved by ETSI ISG QKD. | | | | 14 | | Decision visible in ETSI portal | |
| MS20 | | Early draft of PP | | 4 | | | ETSI | Early draft of major parts of the PP submitted to ETSI ISG QKD. | | | | 18 | | Early draft visible in ETSI portal | |
| MS21 | | Approved contribution on testing methods | | 4 | | | ETSI | Draft testing methods submitted in contribution approve by ETSI ISG QKD. | | | | 26 | | Decision visible in ETSI portal | |
| MS22 | | Stable draft of PP | | 4 | | | ETSI | Stable draft of PP submitted to ETSI ISG QKD. | | | | 30 | | Stable draft visible in ETSI portal | |
| MS23 | | Report on independent review | | 4 | | | ETSI | Report on independent review of PP contributed to and approved by ETSI ISG QKD. | | | | 32 | | Decision visible in ETSI portal | |
| Deliverable No  (continuous numbering linked to WP) | | Deliverable Name | | Work Package No | | | Lead Beneficiary | Type | | Dissemination Level | | Due Date  (month number) | | Description  (including format and language) | |
| D4.1 | | Quantum Key Distribution (QKD); Common Criterial Protection Profile - Key Processing Module | | 4 | | | ETSI | R *—* Document,report | | PU *—* Public | | 35 | | Publication of Group Specification by ETSI in English claiming conformance to the Common Criteria.  NOTE: The name of this deliverable might change as discussions on terminology of QKD network architecture and the TOE boundary etc. evolve. | |

|  |
| --- |
| **Estimated budget — Resources** |
| See TOTAL PROJECT COSTS table below. |

## Total Project costs



#### 4.3 Subcontracting

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| Work Package No | Subcontract No  (continuous numbering linked to WP) | Subcontract Name  (subcontracted action tasks) | Description  (including task number and BEN/AE to which it is linked) | | Estimated Costs  (EUR) | Justification  (why is subcontracting necessary?) | Best-Value-for-Money  (how do you intend to ensure it?) |
| 1-4 | NA | NA | From Task 1.2 to Task 4.9 | | 498 445 | Expertise not available in ETSI Secretariat | Subcontractors are selected on a case-by-case basis in the context of an open call through a clearly defined process (typically one or more of the following, publication of the call through ETSI Collective letters (see section 2.3 above) to the membership, Technical Body mailing lists or explicit calls for tender).  Travel costs are included in the subcontracting cost. |
| Other issues:  *If subcontracting for the project goes beyond 30% of the total eligible costs, give specific reasons.* | | | | Each subcontractor/expert is allocated to specific tasks with an expected level of contribution. The financial resources allocated to the subcontractor are calculated on this principle. For reasons linked to French social Regulations and to avoid a risk of subordinate relationship that could trigger negative consequences for ETSI, on advice of its lawyers, ETSI has abandoned the principle of a daily rate to contract its experts and ETSI works now under the principle of service contracts.  ETSI Secretariat (Funded Activities, Technical officers…) will ensure the project planning and controlling with the Technical Committee without charging the related costs to the project, as the EC funds ETSI through an Operating Grant, whereas subcontractors will perform the development and technical execution of the project.  ETSI Secretariat has no expert as staff thus all tasks are subcontracted. Besides the technical project management (WP1) will be handled by the selected subcontractor as Project Leader to ensure the technical tasks execution and quality by the other subcontractors. | | | |

#### Timetable

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Timetable (projects of more than 2 years)** | | | | | | | | | | | | | | | | |
| **ACTIVITY** | **YEAR 2024** | | | | **YEAR 2025** | | | | **YEAR 2026** | | | | **YEAR 2027** | | | |
| **Q 1** | **Q 2** | **Q 3** | **Q 4** | **Q 1** | **Q 2** | **Q 3** | **Q 4** | **Q 1** | **Q 2** | **Q 3** | **Q 4** | **Q 1** | **Q 2** | **Q 3** | **Q 4** |
| **Task 1.1 – Project Setup** |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| **Task 1.2 – Project Management** |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| **Task 2.1 – New Work Item in TC CYBER QSC WG** |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| **Task 2.2 – Initial draft reviewed** |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| **Task 2.3 – Final draft reviewed** |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| **Task 2.4 – Publication of standard** |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| **Task 3.1 – New Work Item in TC CYBER QSC WG** |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| **Task 3.2 – Initial draft reviewed** |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| **Task 3.3 – Initial sketch of proof** |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| **Task 3.4 – Public draft** |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| **Task 3.5 – Conference submission** |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| **Task 3.6 – Final draft** |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| **Task 3.7 – Proof paper** |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| **Task 3.8 – Reference implementation** |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| **Task 3.9 – Standard publication** |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| **Task 4.1 – New Work Item** |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| **Task 4.1 – Review of protocols** |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| **Task 4.2 – TOE boundary/interfaces** |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| **Task 4.3 – Outline modelling** |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| **Task 4.4 – Early draft of PP** |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| **Task 4.5 – Develop testing methods** |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| **Task 4.6 – Refine PP** |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| **Task 4.7 – Independent Review** |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| **Task 4.8 – Finalise PP and approval** |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |

#§WRK-PLA-WP§#

#@ETH-ICS-EI@#

## 5. OTHER

### 5.1 Ethics

|  |
| --- |
| **Ethics** |
| Not applicable. |

#§ETH-ICS-EI§# #@SEC-URI-SU@#

### 5.2 Security

|  |
| --- |
| **Security** |
| Not applicable. |

#§SEC-URI-SU§# #@DEC-LAR-DL@#

## 6. DECLARATIONS

|  |  |
| --- | --- |
| **Double funding** | |
| **Information concerning other EU grants for this project**  *Please note that there is a strict prohibition of double funding from the EU budget (except under EU Synergies actions).* | **YES/NO** |
| We confirm that to our best knowledge neither the project as a whole nor any parts of it have benefitted from any other EU grant *(including EU funding managed by authorities in EU Member States or other funding bodies, e.g. EU Regional Funds, EU Agricultural Funds, etc)*. If NO, explain and provide details. | YES |
| We confirm that to our best knowledge neither the project as a whole nor any parts of it are (nor will be) submitted for any other EU grant *(including EU funding managed by authorities in EU Member States or other funding bodies, e.g. EU Regional Funds, EU Agricultural Funds, etc)*. If NO, explain and provide details. | YES |

|  |
| --- |
| **Financial support to third parties (if applicable)**  *If in your project the maximum amount per third party will be more than the threshold amount set in the Call document, justify and explain why the higher amount is necessary in order to fulfil your project’s objectives.* |
| Not applicable. |

#§DEC-LAR-DL§#

Annex I Response to the Request for Proposals  
CfE – STF 684 (REFERENCE BODIES CYBER – ISG QKD)  
Deadline: 19 November 2024

**If you are an ETSI Member \***

**ETSI membership status (Indicate your status):**

 Full

 Associate

 Observer

**If you are not an ETSI Member \***

Please indicate:

**Full name of the ETSI member supporting the application (list of ETSI members on etsi.org):**

-\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**Official contact name of the ETSI member supporting the application:**

-\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

*Note: A formal confirmation of the support from the Official contact is required (e.g. by e-mail sent to STFLINK@etsi.org) and an “ETSI Member Support Letter” will be required if you are selected.*

|  |  |  |  |
| --- | --- | --- | --- |
| **Contractor information \*** | | | |
|  | | | |
| **Contractor name \*:**  *Indicate the Company/Organization Name* | |  | |
|  | | | |
| **Contact person for the technical aspects** | | **Contact person for Decision on ETSI financial offer to this project (if any)** | |
| Title |  | Title |  |
| First name |  | First name |  |
| Last name |  | Last name |  |
| Role |  | Role |  |
| e-mail |  | e-mail |  |
| Phone |  | Phone |  |

|  |  |  |
| --- | --- | --- |
|  | | |
|  | **Yes** | **No** |
| Do you or any employee of your Company/Organization hold an elected or appointed position in the Reference Body requesting the STF? | o  Indicate in which position:  ----------------------------------- | o |
| **If you are self-employed candidate:**  Do you currently have other contracts in progress with ETSI? | o | o |

All fields marked with an asterix (\*) are mandatory

**1.1 Introduction**

A short presentation of the technical structure responsible for this activity, e.g.:

* Business area, number of employees, link to WEB site,
* Department(s)/team(s)/experts in charge of the technical activities related to this Project,
* Reference to products/services of your Company/Organization or supporting Member to which the standards developed by this Project will apply,
* Motivation for your Company/Organization or supporting Member to participate in this Project.

**1.2 Proposed approach**

**Proposed contribution to tasks & related cost**

Identify the tasks to which your Company/Organization is proposing to contribute by filling-in the table below:

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Tasks No | Tasks Description | Max Budget Allocated in Euro | Amount in Euro (mandatory) | % of whole Task (mandatory) |
| T0 | T1.1 Project set-up | 0 |  |  |
| T1 | T1.2 Project Management | 15 600 |  |  |
| T2 | T2.1 New Work Item in TC CYBER QSC WG | 1 540 |  |  |
| T3 | T2.2 Initial draft reviewed | 21 560 |  |  |
| T4 | T2.3 Final draft reviewed | 53 900 |  |  |
| T5 | T2.4 Publication of standard | 10 780 |  |  |
| T6 | T3.1 New Work Item in TC CYBER QSC WG | 1 540 |  |  |
| T7 | T3.2 Initial draft reviewed | 5 390 |  |  |
| T8 | T3.3 Initial sketch of proof | 48 510 |  |  |
| T9 | T3.4 Public draft | 43 120 |  |  |
| T10 | T3.5 Conference submission | 10 780 |  |  |
| T11 | T3.6 Final draft | 21 560 |  |  |
| T12 | T3.7 Proof paper | 43 120 |  |  |
| T13 | T3.8 Reference implementation | 32 340 |  |  |
| T14 | T3.9 Standard publication | 10 780 |  |  |
| T15 | T4.1 Create and approve New Work Item | 1 540 |  |  |
| T16 | T4.2 Review of protocols | 11 500 |  |  |
| T17 | T4.3 TOE boundary / interfaces | 11 500 |  |  |
| T18 | T4.4 Outline security modelling | 17 300 |  |  |
| T19 | T4.5 Early draft of PP | 22 500 |  |  |
| T20 | T4.6 Develop testing methods | 22 500 |  |  |
| T21 | T4.7 Refine PP | 33 085 |  |  |
| T22 | T4.8 Independent review | 16 500 |  |  |
| T23 | T4.9 Finalise PP, approval, and publication | 5 600 |  |  |
|  |  | **462 245** |  |  |

**Amount in Euro (mandatory)**: Indicate the price offered for your contribution to the task(s)

**% of whole task (mandatory)**: Indicate to which percentage of the execution of the whole task your offer corresponds

Provide a description of the proposed approach, competences, reference to related activities:

* Explain which part of the task is corresponding to the requested percentage that your Company/Organization will handle,
* Explain the scope that your Company/Organization will cover,
* Explain your approach to the management of the quality and,
* Explain your approach to the management of the risks and their mitigation,
* Describe and justify the proposed costs to achieve this project objectives.

Annex II Terms and Conditions  
CfE – STF 684 (REFERENCE BODIES CYBER – ISG QKD)  
Deadline: 19 November 2024

**2.1 Submission of Proposals**

All proposals in response to this CfE shall be submitted before the deadline indicated in thisCollective Letter, using exclusively the WEB application on the ETSI Portal at the following address: <https://portal.etsi.org/cfe>.

Proposals shall be composed of Curriculum Vitae of the proposed service providers’ personnel and the Annex I of this CfE duly filled-out.

Proposals that will be partial or incomplete at the deadline will not be accepted.

The Terms and Conditions in this Annex will apply.

**2.2 Modification and Withdrawal of Proposals**

Applicants may, without prejudice to themselves, modify or withdraw their proposal by written request, provided that the request is received by ETSI prior to the due date and time, at the address to which their proposal was submitted. The applicant may submit a new proposal provided that such new proposal is received prior to the deadline for responding which is specified in this Collective Letter.

**2.3 Assessment of Proposals**

The ETSI Director-General, in consultation with the Reference Body Chairman, is responsible for the selection of the service providers that will be contracted to perform this Project work. The ETSI Director-General and the Reference Body Chairman may be assisted by a Selection Panel to assess the applications received and make the final decision.

As per article 1.10.4 of the ETSI Directives, the Director-General may discard proposals that could be identified as creating potential conflict of interest.

The ETSI Secretariat will only communicate to the applicants the result of the selection (accepted or not accepted). Should applicants need more information on the rationale for the selection, they must address a formal request to the ETSI Director-General.

The following evaluation criteria will be applied to all proposals, in order of priority:

* Evidence that the applicant has the necessary structure and expertise to ensure delivery
* Reference to current or previous activities in the specific technical domain of this project
* Critical review of the most efficient way to achieve the objectives in this Project ToR
* Effective proposed approach/methodology for the execution of the tasks
* Implementation schedule
* Clear pricing policy

Compliance with the first two (2) criteria is mandatory.

Proposals that are not considered compliant with these criteria will be discarded.

Priority will be given to technical quality of the proposals. Pricing considerations will be taken into account to ensure that the best value for money is achieved. Compatibility with the maximum budget allocated to this Project will be verified before placing a Service Contract.

Following the assessment process, ETSI reserves the right to grant contracts to other than the cheapest proposals, to accept or reject any offer completely or in part, or to reject all proposals, without providing the reasons. If no offer is accepted, ETSI may decide to abandon the work or proceed in any other manner ETSI may select.

**2.4 IPR and confidentiality Agreements**

The information provided in this CfE, as well as the fact that the applicant has received the CfE, is considered confidential and protected under copyright laws. The applicant may not discuss, share, or use the information in this CfE for any purpose other than the response to this CfE.

ETSI will not disclose the content of any proposals to other applicants or any other party, with the exception of the persons involved in the assessment process described in §2.3 above.

However, ETSI reserves the right to make use of the information provided in this proposal to improve this project definition for the purpose of this CfE or any other manner in which ETSI may decide to proceed to select the service providers.

If successful, the applicant will be required to sign a Service Contract, which includes IPR and Confidentiality clauses aligned with the relevant policies in the ETSI Directives.

**2.5 Preparation cost**

ETSI will not be responsible for any costs or expenses that the applicant may incur in preparing and/or submitting the proposal.

**2.6 Service Contract**

A Service Contract will be proposed to the applicants that will be selected to perform the work.

Details on the Terms and Conditions of this contract can be found on the ETSI Portal, at the following address: <https://portal.etsi.org/STF/STFs/Contracts.aspx>