HellasQCI

Ανάπτυξη προηγμένων εθνικών συστημάτων Κβαντικών Υποδομών Επικοινωνίας (QCI) στην Ελλάδα

Πρόσκληση για παροχή πληροφοριών (RFI)

Πρόσκληση για δοκιμή Proof of Concept (PoC) για ερευνητικούς σκοπούς για κβαντική κρυπτογράφηση οπτικού δικτύου

Κύριος(-οι) δικαιούχος(-οι): Εθνικό Δίκτυο Υποδομών Τεχνολογίας και Έρευνας Α.Ε, ΕΘΝΙΚΟ ΚΑΙ ΚΑΠΟΔΙΣΤΡΙΑΚΟ ΠΑΝΕΠΙΣΤΗΜΙΟ ΑΘΗΝΩΝ

Δημιουργός : Τεχνικό Συμβούλιο HellasQCI

Ημερομηνία: 23 Ιουνίου 2023

Επίπεδο διάχυσης: Δημόσιο

Περίληψη:

Πρόσκληση για δοκιμή Proof of Concept (PoC) για ερευνητικούς σκοπούς για κβαντική κρυπτογράφηση οπτικού δικτύου. Στόχος είναι να εντοπιστούν οι κατάλληλες τεχνικές λύσεις για την υλοποίηση των δικτύων και δοκιμών χρήσης του HellasQCI. Οι προμηθευτές ή η κοινοπραξία προμηθευτών παρακαλούνται να διαβιβάσουν τις προτάσεις τους μέσω ηλεκτρονικού ταχυδρομείου στη διεύθυνση hellasqci-technicalboard@lists.grnet.gr έως την Παρασκευή 7 Ιουλίου 2023.

Co-funded by the European Union

Το Έργο «HellasQCI» χρηματοδοτείται στο πλαίσιο της Σύμβασης Επιχορήγησης με αριθμό 101091504

Πίνακας Περιεχομένων

1. Ακρωνύμια

QCI	Κβαντική Υποδομή Επικοινωνίας
EuroQCI	Ευρωπαϊκή Πρωτοβουλία για ασφαλείς Κβαντικές Υποδομές Επικοινωνίας
DV- QKD	Διακριτή μεταβλητή Διανομής Κβαντικών Κλειδιών
QKD	Διανομή Κβαντικών Κλειδιών
ETSI	Ευρωπαϊκό Ινστιτούτο Τηλεπικοινωνιακών Προτύπων
KMS	Σύστημα Διαχείρισης Κλειδιών
OTN	Δίκτυο Οπτικής Μεταφοράς
SKR	Ρυθμός απόρρητου κλειδιού
GS	Ομαδικές Προδιαγραφές
RFI	Πρόσκληση για Παροχή Πληροφοριών
BB84	Πρωτόκολλο Διανομής Κβαντικών Κλειδιών που αναπτύχθηκε από τους Charles Bennett και Gilles Brassard το 1984

2. Εισαγωγή

Το έργο HellasQCI αποσκοπεί στην ανάπτυξη προηγμένων Εθνικών συστημάτων και δικτύων QCI (**Κβαντικών Υποδομών Επικοινωνίας)** στην Ελλάδα. Η αρχιτεκτονική του αποτελείται από τρεις μητροπολιτικούς χώρους δοκιμών (test-sites) που βρίσκονται σε πόλεις της Ελλάδας και συγκεκριμένα: HellasQCI-Κέντρο (Αθήνα), HellasQCI-Βόρεια (Θεσσαλονίκη) και HellasQCI-Νότια (Ηράκλειο-Κρήτη).

Κάθε χώρος δοκιμών χωρίζεται σε διαφορετικούς τομείς (test-beds) όπως: κυβερνητικό, βιομηχανικό και ακαδημαϊκό τομέα , που επιτρέπουν στο έργο να διερευνήσει την ανάπτυξη των τεχνολογιών QKD σε μια πληθώρα ρεαλιστικών σεναρίων και περιπτώσεων χρήσης που αφορούν στην εθνική ασφάλεια, τη δημόσια υγεία, τις κρίσιμες υποδομές και τον τομέα των ΤΠΕ. Το ακαδημαϊκό test-bed θα επιτρέψει την ανάπτυξη νέων κβαντικών τεχνολογιών, και θα προχωρήσει σε δοκιμές για το Κβαντικό Διαδίκτυο.

Στόχος του έργου HellasQCI, το οποίο αποτελεί μέρος του ευρωπαϊκού δικτύου EuroQCI, είναι να συμβάλει στην ασφαλή φύλαξη κρίσιμων δεδομένων και υποδομών, σε τομείς όπως η ηλεκτρονική διακυβέρνηση, η υγειονομική περίθαλψη και σε πολλούς άλλους κρίσιμους τομείς. Αυτό θα επιτευχθεί με την ενσωμάτωση συστημάτων και τεχνολογιών που βασίζονται στις αρχές της κβαντικής τεχνολογίας, και πιο συγκεκριμένα με τη διανομή κβαντικών κλειδιών (QKD) στις υπάρχουσες υποδομές επικοινωνίας, οι οποίες θα προσφέρουν μια εξαιρετικά ασφαλή μορφή κρυπτογράφησης, και ένα επιπλέον επίπεδο ασφάλειας.

Το Εθνικό Δίκτυο Υποδομών Έρευνας και Τεχνολογίας (ΕΔΥΤΕ Α.Ε.), που λειτουργεί υπό την αιγίδα του Υπουργείου Ψηφιακής Διακυβέρνησης, είναι ο συντονιστής του έργου HellasQCI και σε συνεργασία με 13 εταίρους, προκηρύσσουν την παρούσα Πρόσκληση Πληροφόρησης (RFI) για τον εντοπισμό κατάλληλων τεχνικών λύσεων για την υλοποίηση των ων περιπτώσεων χρήσης του HellasQCI.

Στην παρούσα δοκιμαστική φάση, τυχόν κόστος που προκύψει για την υλοποίηση του PoC θα πρέπει να αναληφθεί από τους προμηθευτές ή την κοινοπραξία των προμηθευτών. Με βάση τα αποτελέσματα του PoC που προβλέπεται να εκτελεστεί από τον Σεπτέμβριο του 2023 έως τον Δεκέμβριο του 2023, οι τελικές προδιαγραφές των συστημάτων μπορεί να συμπεριληφθούν σε επικείμενη προμήθεια από το HellasQCI.

Η παρούσα πρόσκληση για PoC προορίζεται μόνο για σκοπούς ενημέρωσης και σχεδιασμού και δεν αποτελεί πρόσκληση υποβολής προσφορών. Κάθε πληροφορία ή/και δεδομένο που λαμβάνεται σε απάντηση της παρούσας πρόσκληση και χαρακτηρίζεται ως "Εμπιστευτικό", πρέπει να αντιμετωπίζεται ως τέτοιο. Η συμβολή/ανταπόκρισή σας στην παρούσα, δεν επιστρέφεται, δεν αποτελεί προσφορά, δεν είναι δεσμευτική ούτε μπορεί να οδηγήσει σε σύναψη δεσμευτικής σύμβασης.

Οι προμηθευτές ή οι κύριοι δικαιούχοι κοινοπραξιών προμηθευτών παρακαλείστε να διαβιβάσετε τις πληροφορίες μέσω ηλεκτρονικού ταχυδρομείου στη διεύθυνση hellasqci-technicalboard@lists.grnet.gr μέχρι την Παρασκευή 7 Ιουλίου 2023.

3. Τεχνικές προδιαγραφές

Προκειμένου να δοκιμαστεί ένα κβαντικά κρυπτογραφημένο οπτικό δίκτυο, προσβλέπουμε στην ακόλουθη επίδειξη PoC με τουλάχιστον τρεις κόμβους δικτύου μεταξύ του ΕΔΥΤΕ και του Εθνικού Καποδιστριακού Πανεπιστημίου Αθηνών (ΕΚΠΑ), όπου κάθε κόμβος υλοποιεί:

1. ένα οπτικό επίπεδο δεδομένων με ικανότητα για κρυπτογραφημένη συνδεσιμότητα OTN και ethernet,

2. ένα επίπεδο μετάδοσης κβαντικών κλειδιών QKD για τη δημιουργία και διανομή τους,

3. ένα επίπεδο για το Σύστημα Διαχείρισης Κλειδιών KMS για το χειρισμό των κλειδιών QKD και τη διασύνδεση με τις κρυπτομηχανές,

4. ένα επίπεδο κρυπτογράφησης για την κατανάλωση κλειδιών QKD.

Συγκεκριμένα, οι τρεις κόμβοι θα συνδέονται με δακτύλιο και θα πρέπει να χρησιμοποιούν δύο ζεύγη DV-QKD με τον μεσαίο κόμβο να εκτελεί λειτουργία αναμετάδοσης κλειδιών. Η απόσταση μεταξύ των κόμβων θα είναι μικρότερη από 50 χιλιόμετρα. Οι προδιαγραφές για το DV-QKD παρατίθενται στον πίνακα 1.

Οι κόμβοι πρέπει να υποστηρίζουν συνδεσιμότητα OTN με ταχύτητα έως 400Gbps ή/και συνδεσιμότητα ethernet 4x100Gbps. Επιπλέον, οι κόμβοι θα πρέπει να χρησιμοποιούν ένα σύστημα κρυπτογράφησης (π.χ. L1 ή/και L2) για την κατανάλωση των κλειδιών QKD με μεταβλητό ρυθμό. Τα συστήματα κρυπτογράφησης θα πρέπει να περιλαμβάνουν AES 256.

Το σύστημα διαχείρισης κλειδιών θα πρέπει να είναι σε θέση να διασυνδέει τις κρυπτομηχανές με το επίπεδο QKD (π.χ. χρησιμοποιώντας το πρότυπο ETSI QKD 14) και θα πρέπει να χειρίζεται

αποτελεσματικά τα κλειδιά QKD (π.χ. εκτελώντας τη λειτουργία αναμετάδοσης και την ανταλλαγή κλειδιών, διαχειριζόμενο τη δεξαμενή κλειδιών σε κάθε κόμβο, και επίσης να μεταβαίνει σε μη κβαντική κρυπτογράφηση σε περίπτωση που ένα ή περισσότερα συστήματα QKD αποτύχουν (π.χ. προκαλώντας πολύ μεγάλη εξασθένηση σε μια γραμμή).

Περιγραφή	Απαιτήσεις
Διάρκεια και ημερομηνίες PoC	Σεπτέμβριος 2023 – Δεκέμβριος 2023
Αριθμός κόμβων	3
Στρώμα οπτικών δεδομένων	Κρυπτογραφημένη συνδεσιμότητα OTN και ethernet 400Gbps OTN και /ή 4x100Gbps ethernet ανά κόμβο
Κρυπτογράφηση	OTNsec, MACsec, AES 256
Πρωτόκολλο DV-QKD	Decoy state BB84
Εύρος μεταξύ των κόμβων	<50kms
Ρυθμός απόρρητου κλειδιού	>1kb/s
Σύστημα Διαχείρισης Κλειδιών (KMS)	ETSI QKD 014 GS KMS λογισμικό QKD λογισμικό διαχείρισης και ελέγχου
Μήκος κύματος κβαντικού καναλιού	C-band