Automated tool to discover Quantum-vulnerable Crypto Algorithms

1	**Problem Statement**	Development of Automated Tool (combination of black box tester and security scanner agent on the target device itself) to scan target device for discovery of generic security vulnerabilities and Quantum-vulnerable cryptographic algorithms.
2	**Technology Area**	Post Quantum Cryptography (PQC), Vulnerability Assessment
3	**Project Introduction**	With the advents of quantum computers, classical public-key cryptosystems such as RSA, ECDH, and ECDSA shall no longer be secure as the underlying mathematical hard problems shall be efficiently solved using Shor's quantum algorithm. In addition, classical symmetric-key cryptosystems will suffer a quadratic loss in security due to Grover's quantum search algorithm. Given quantum threats, NIST is already standardizing post-quantum cryptographic algorithms as a replacement for currently used quantum-vulnerable classical cryptosystems. It is therefore necessary to migrate from traditional cryptosystems to quantum-safe cryptosystems in order to protect critical information from all kinds of future quantum attacks. The discovery of an automated migration tool shall demonstrate the instances of quantum-vulnerable cryptosystems such as their usages, purposes and dependencies on other systems. The insights provided by the automated software agent shall enable users to set priorities and develop effective quantum-safe migration strategies.

4	**Description**	The objective of this project is to develop an automated tool to identify and report the quantum-vulnerable algorithms used in target device. The tool shall list these vulnerable algorithms and generate a report. The target device may be using vulnerable crypto algorithms in network security application(s) or device security application(s). This tool should be capable to identify all the quantum-vulnerable algorithms & other security vulnerabilities, a target device is supporting/using. In the process of discovery, the tool should first list out all vulnerabilities and cryptographic algorithms and then differentiate between quantum-safe and quantum-vulnerable algorithms and finally provide a list of security vulnerabilities, specifically quantum-vulnerable algorithms with location of these algorithms in the device. To identify these algorithms, this tool can be developed in two parts with one manager/controller for reporting: **Web application:** This part of tool shall scan the target device from outside (black box testing: with login and without login) to discover generic security vulnerabilities & quantum-vulnerable algorithms and generate a consolidated report. **Security Scanner S/w Agent:** This part of tool shall installed & executed on the target device itself. The tool shall scan all the algorithms in different security libraries like OpenSSL, boringssl, crypto etc. and different configuration files of security application like IPSEC, VPN, SSH etc. to find out quantum-vulnerable algorithms and generate the report for the same. The software agent should be developed for Linux OS based systems as well as for Windows OS based systems. **Control Software:** To control & manage web application and security scanner agent, having following capabilities- o It shall be responsible for installation/uninstallation of the automated software agent on the target device(s). o Running of the web application for black box testing o Collecting the data from above mentioned agent & web application and providing a consolidated report on generatin security vulnerabilities & Quantum-vulnerable algorithms being used in the target device.
5	**Roles & Responsibilities of C-DOT**	C-DOT provide technical development assistance, infrastructure (in case of co-development project) and financial support to the project partner(s) selected through a process of evaluation and due diligence conducted by a committee of subject experts. Wherever deemed necessary and depending upon the project type (i.e. co-development or fully outsourced), C-DOT may arrange resources, equipment, training, testing infrastructure, mandatory clearances, statutory permissions,

		and provide gap funding to the partner(s) in realizing the respective target deliverables. Development costs of the module, whether developed from scratch or derived from existing background technology of partner(s), shall be borne by C-DOT. C-DOT shall use the final solution for integration with production grade software. C-DOT reserves the right to modify and enhance the solution and provide it to C-DOT customers or other Partner(s). C-DOT shall engage with Partner(s) on a non-exclusive basis and shall retain its right to develop similar projects/products through other developmental programs.
6	**Roles & Responsibilities of Partner(s)**	The Partner(s) may build the required module afresh or by modifying pre-existing background technologies available with them. As per the project demand or project type, the Partner(s) may utilize the available test and infrastructure facilities offered by C-DOT with no/some financial implication for its usage. All commercial proposals shall include manpower and cost breakup (Capital, Consumables, Travel, DA, Training, Contingency, Overhead, GST etc.). The proposal should include minimum of two years support for enhancements and capacity building for future enhancements in the product. Participation in the project shall be on a non-exclusive basis. All partner(s) shall be required to demonstrate commitment to the project by entering into a formal agreement with C-DOT as per the CCRP policy.
7	**Expected Deliverables**	• **Web application** (running on PC connected to target device either directly or over the network), which shall be responsible for listing out all the security vulnerabilities and quantum-vulnerable algorithms being used in the device. • **The security scanner software agent** (installed on the target device itself), which shall be responsible for listing out the quantum-vulnerable algorithms supported in the device software (for Linux and Windows OS both). • **Control software** to control web application and the security scanner software agent. This software will handle the installation/uninstallation of automated software tool on the device, running web application, collecting data from both the tools and providing a consolidated list of vulnerable algorithms.
8	**Ownership of Background & Foreground IP**	All technologies created during the project shall be owned by the respective development partner(s), individually or collectively as the case may be. Any agreement required for collective ownership shall be settled directly by the concerned partners, but the ownership/IPR of the final solution shall rest with C-DOT only with all the deliverables including complete source code etc.

#Note: The interested applicants are required to fill the application form in the Template attached and submit a signed PDF. Applicants are required to mention mandatory details including Expected Fund requirement, Expected Time of Delivery, current TRL Level of any product in this or a related product domain for the application to be accepted.

ACRONYMS AND ABBREVIATIONS

ECDH	Elliptic-Curve Diffie–Hellman
ECDSA	Elliptic-Curve Digital Signature Algorithm
IPSEC	Internet Protocol Security
PQC	Post-Quantum Cryptography
RSA	Rivest-Shamir-Adleman protocol
SSH	Secure Shell protocol
VPN	Virtual Private Network