**SCIENTIFIC CYBER SECURITY ASSOCIATION**

*Independent Cryptographic Security Review*

# CERTIFICATE OF CRYPTOGRAPHIC SECURITY REVIEW

**Executive Summary — Public Release**

| | |
|---|---|
| **Subject** | Iris Hybrid Post-Quantum End-to-End Encryption Protocol |
| **Issuing Body** | Scientific Cyber Security Association (SCSA) |
| **Lead Reviewer** | Prof. Dr. Maksim Iavich |
| **Review Type** | Independent Cryptanalysis and Protocol Security Assessment |
| **Certificate Date** | 19 July 2026 |

## 1. Purpose of This Certificate

This document is the public executive summary of an independent cryptographic security review carried out by the Scientific Cyber Security Association (SCSA), led by Prof. Dr. Maksim Iavich. It summarizes the scope, methodology, and outcome of the review for general audiences and does not include implementation-level technical detail, which remains available to the reviewed party in the full confidential report.

## 2. Scope of the Review

The Iris protocol is a hybrid authenticated key-establishment and end-to-end encryption scheme designed to protect communication between two parties over an untrusted relay. The review examined the protocol's complete cryptographic construction, namely:

- SPAKE2 password-authenticated key exchange for mutual authentication;
- X25519 elliptic-curve Diffie–Hellman key agreement for classical confidentiality;
- ML-KEM-768 post-quantum key encapsulation, standardized under FIPS 203, for post-quantum confidentiality;
- HKDF-SHA-256 based hybrid key derivation and transcript binding;
- ChaCha20-Poly1305 authenticated encryption, directional key separation, and replay/nonce management.

The assessment considered passive and active network adversaries, man-in-the-middle and unknown key-share attacks, replay and reflection attacks, online guessing, and both classical and quantum-capable adversaries, including store-now-decrypt-later scenarios.

## 3. Summary of Findings

The review confirms that the Iris protocol's cryptographic design is sound. Every primary security objective evaluated during the assessment — authentication, confidentiality, integrity, forward secrecy, replay and reflection resistance, resistance to man-in-the-middle and unknown key-share attacks, transcript binding, hybrid key security, and post-quantum readiness — was achieved under the assumptions and adversarial model defined for the review.

| Security Objective | Result |
|---|---|
| Mutual Authentication | ✓ Achieved |

| | |
|---|---|
| Session Key Confidentiality & Indistinguishability | ✓ Achieved |
| Integrity Protection & Explicit Key Confirmation | ✓ Achieved |
| Forward Secrecy | ✓ Achieved |
| Replay & Reflection Resistance | ✓ Achieved |
| Unknown Key-Share Resistance | ✓ Achieved |
| Man-in-the-Middle Resistance | ✓ Achieved |
| Transcript Binding | ✓ Achieved |
| Hybrid (Classical + Post-Quantum) Key Security | ✓ Achieved |
| Store-Now-Decrypt-Later Resistance | ✓ Achieved |
| Post-Quantum Readiness | ✓ Achieved |

During the review process, several minor observations and hardening recommendations were raised regarding implementation-level details of the reviewed system. All such observations were addressed by the development team and verified as resolved prior to the issuance of this certificate. No unresolved protocol-level vulnerability remains outstanding.

## 4. Certification Statement

On the basis of the analysis summarized above, the Scientific Cyber Security Association certifies that the cryptographic design of the Iris protocol meets accepted contemporary standards for authenticated, confidential, and integrity-protected communication, including resilience against anticipated post-quantum threats through its hybrid classical/post-quantum construction.

This certificate reflects the state of the protocol as reviewed on the date above. It does not constitute a guarantee against risks arising from endpoint compromise, side-channel attacks, weak random-number generation, or other factors outside the cryptographic protocol itself, which remain the responsibility of the deploying organization.

**Prof. Dr. Maksim Iavich**
President, Scientific Cyber Security Association (SCSA)
Corresponding Member, Georgian National Academy of Sciences
Professor & Director, Cyber Security Center, Caucasus University
*Tbilisi, Georgia — 19 July 2026*