University of Trento

Advanced Programming of Cryptographic Methods

Authentic Messages

Graduate Student
Filippo De Grandi

Date: 19/11/2025

Contents

Requirements

Security Requirements

In this section, we outline the security requirements for the quantum-resistant identity-binding messaging system, focusing on post-quantum resilience, authenticity, integrity, and secure key management.

Quantum-Resilient Confidentiality & Integrity

SR 1 **Post-Quantum Security** : All cryptographic primitives must be secure against quantum-capable adversaries, including signature schemes, key-exchange mechanisms, and hashing algorithms.

SR 2 **Message Integrity** : Messages sent by the user must be protected so the server can detect any tampering during transmission.

SR 3 **Identity Binding** : Each secured message must be cryptographically bound to the user's identity in a way that is resilient to both classical and quantum attacks.

Authentication & Registration

SR 4 **Authenticated Registration** : The system must ensure that only legitimate users can register and obtain a valid key pair.

SR 5 **Key Ownership Proof** : Users must be able to prove ownership of the private key corresponding to their registered public key without revealing the private key.

SR 6 **Secure Key Storage** : Users and servers must securely store key material to prevent extraction by a quantum-enabled attacker.

Message Verification & Replay Protection

SR 7 **Sender Authenticity Verification** : The server must verify that each message is signed by the user corresponding to the registered key pair.

SR 8 **Replay Attack Resistance** : The system must detect and reject replayed valid messages to prevent malicious reuse.

SR 9 **Freshness Guarantees** : Messages must include mechanisms (timestamps, counters, or nonces) ensuring they are recent and not reused.

Communication Security

SR 10 **Secure Channel Establishment** : The TUI communication must be secured against eavesdropping and man-in-the-middle attacks, using post-quantum secure protocols.

SR 11 **Metadata Protection** : Communication metadata should be minimized to reduce risks of profiling by quantum-enabled adversaries.

Functional Requirements

In this section, we outline the functional requirements for the identity-binding message system with post-quantum protections.

FR 1 **User Registration** : Users must be able to register with the server, creating or uploading a post-quantum secure public key.

FR 2 **Key Pair Generation** : Users must be able to generate a post-quantum key pair compatible with the system's signature requirements.

FR 3 **Message Creation** : Users must be able to create messages that include both content and cryptographic bindings to their identity.

FR 4 **Message Signing** : Users must be able to digitally sign messages using a post-quantum secure signature algorithm.

FR 5 **Message Transmission** : Users must be able to send secured messages via the TUI for server verification.

FR 6 **Message Verification** : The server must verify submitted messages by checking signature validity and verifying user registration.

FR 7 **Registration Lookup** : Upon receiving a message, the server must determine whether the sender is already registered with an existing key pair.

FR 8 **Error Feedback** : The system must notify users when registration fails, verification fails, or the message format is invalid.

Non-Functional Requirements

Performance

NFR 1 **Efficient Verification** : The server must verify post-quantum signatures with acceptable latency, despite their larger size compared to classical schemes.

NFR 2 **Reasonable Key Sizes** : Key generation and transmission must remain usable despite larger post-quantum key and signature sizes.

Scalability

NFR 3 **Support for Many Users** : The server must handle registration, key management, and message verification for a large number of users.

NFR 4 **Efficient TUI Interaction** : Operations performed through TUIs must remain efficient and responsive even in high-load environments.

Usability

NFR 5 **Straightforward Registration** : Users must be able to register and manage keys through a simple, understandable TUI workflow.

NFR 6 **Clear Verification Feedback** : The system must clearly communicate success or failure conditions without exposing sensitive details.

Reliability & Availability

NFR 7 **High Availability** : Both message submission and verification services must remain available and robust against failures.

NFR 8 **Fault Tolerance** : Registration data and keys must be stored so they remain intact even in case of server failures.

Compliance & Governance

NFR 9 **Secure Audit Logging** : The system must log registration and verification events securely without exposing sensitive cryptographic material.

NFR 10 **Long-Term Security Compliance** : Cryptographic choices must align with current and evolving post-quantum security standards and recommendations.

NFR 11 **Key Lifecycle Policies** : The system must support secure key rotation, expiration, and revocation in a quantum-resilient manner.