University of Trento

Advanced Programming of Cryptographic Methods

Authentic Messages

Filippo De Grandi

Date: 23/11/2025

Contents

Description

In this scenario a user communicates with a server via Terminal User Interfaces (TUIs).

The user must register with the server and be able to send messages that cryptographically bind their identity to the message content. The server must verify both the authenticity of the sender and the integrity of each received message. It must also determine whether the user is already registered and manage key material in a quantum-resilient way.

Because adversaries may possess quantum capabilities, the system must rely on post-quantum secure cryptographic algorithms for registration, key generation, signing, and verification.

Requirements

Functional Requirements

FR 1 **Registration** : The user must be able to register to the server

FR 2 **Message Sending** : The user must be able to send a message

FR 3 **Message Receival** : The server must receive messages from users

Security Requirements

SR 1 **Message Integrity** : The server must verify that messages have not been altered in transit

SR 2 **Quantum-level Security** : Protection against quantum capable adversaries

SR 3 **Authentication** : Authentication of users to the server

Technical Details

Architecture

In this scenario, the system enables a user to register to a server and later send authenticated, integrity-protected messages through a TUI interface. Because adversaries may possess quantum capabilities, all long-term cryptographic guarantees must rely on post-quantum primitives.

Components

1. User Module:
   - Generates a post-quantum key pair during registration (e.g. Dilithium [1]), securely storing the private key, and producing signed messages
   - Interacts with the server through a TUI, ensuring that identity-binding messages are always signed locally.
2. Server Module:
   - Stores user public keys and registration records.
   - Verifies the signature against the stored public key
   - Checks message integrity.
   - Determines whether the sender is already registered. If registration is new, the server stores the submitted PQC public key.
3. Cryptographic Layer:
   - Post-quantum–secure digital signatures for identity binding, along with PQC key-encapsulation or TLS 1.3 with hybrid PQC ciphersuites to secure the communication channel (e.g. Kyber [2]).
   - Simple message structure (header, content, signature) ensures integrity and authenticity.

Security Considerations

Authentication

- Each user signs registration requests and messages using an EUF-CMA [3] post-quantum signature scheme.
- The server verifies signatures to ensure the sender is genuine and that messages are bound to a specific registered identity.

Integrity

- Since signatures cover the entire message, any modification by an attacker results in a failed verification. This protects both in-transit and stored messages.

Confidentiality

- Communication is secured via a PQC-augmented channel (e.g. TLS with Kyber hybrid key exchange) preventing both classical and quantum MITM attackers from learning message contents.

Resistance to Quantum Adversaries

- Long-term secrets (user keys, server-stored public keys, message signatures) rely on post-quantum primitives. Even if an attacker stores all traffic today, they cannot forge messages or break the confidentiality of communications in the future.

Threat Model

Even if the server is honest-but-curious, it only sees user public keys and signed messages, but cannot forge identities or alter messages undetected. Network attackers cannot impersonate users due to signature verification and cannot break the encrypted channel, even with quantum resources.

Bibliography

[1] CRYSTALS, “CRYSTALS-Dilithium.” [Online]. Available: https://pq-crystals.org/dilithium/

[2] Wikipedia, “Kyber.” [Online]. Available: https://en.wikipedia.org/wiki/Kyber

[3] “Existential unforgeability under chosen message attacks.” [Online]. Available: https://blog.cryptographyengineering.com/euf-cma-and-suf-cma/