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

Security Considerations