University of Trento

Advanced Programming of Cryptographic Methods

Confidential But Genuine Feedback

Filippo De Grandi

Date: 21/11/2025

Contents

Description

A professor (or manager) collects feedback from students (or employees). Individuals must be free to express honest opinions while maintaining anonymity. At the same time, the professor or manager must verify that submissions come only from eligible participants.

An additional fairness requirement mandates that the system must detect when multiple messages originate from the same person, without revealing the person's identity.

The system must therefore support anonymous authentication, controlled pseudonymity and duplicate detection balancing privacy, authenticity, and fairness.

Requirements

Functional Requirements

FR 1 **Feedback Submission** : The submitters must be able to submit feedbacks

FR 2 **Feedbacks Access** : The receivers must be able to access the feedbacks

FR 3 **Duplicate Detection Mechanism** : The receiver must be able to distinguish if two feedbacks come from the same submitter

Security Requirements

SR 1 **Hidden Submitter Identity** : The receiver must not learn the identity of the submitter by the submitted feedbacks

SR 2 **Authorized Submission** : Only authorized submitters must be able to submit feedbacks

Non-Functional Requirements

NFR 1 **Privacy** : The system must comply with local privacy regulations and data protection laws to securely handle each user's data.The submitters must be aware of the inner functioning of the system

Technical Details

Architecture

Security Considerations