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

Security Requirements

In this section, we outline the security requirements for the anonymous but verifiable feedback system, focusing on anonymity, authenticity, fairness, integrity, and privacy.

Anonymity & Privacy

> SR 1 **Anonymity** : The system must ensure that individual student or employee identities cannot be linked to specific feedback submissions.

> SR 2 **Unlinkability** : Submissions must not be linkable to an identity or to other metadata that could reveal the originator (apart from fairness mechanisms).

> SR 3 **Submission Content Privacy** : The contents of feedback messages must remain private and inaccessible to unauthorized parties, including system operators.

Authenticity & Access Control

> SR 4 **Authorization** : Only authorized individuals (e.g. students enrolled in a course or employees of a workplace) may submit feedback. Furthermore, feedback credentials must be bound to an individual and not transferable to others.

> SR 5 **Single Submission** : The system must ensure that each individual can submit feedback at most once, unless the system explicitly allows multiple submissions.

Fairness & Duplicate Detection

> SR 6 **Duplicate Submission Detection** : The system must allow determining whether two submissions (if multiple submissions are enabled) come from the same entity without revealing the entity's identity.

Integrity

> SR 7 **Message Integrity** : Feedback submissions must not be modifiable in transit or on the server without detection.

> SR 8 **Result Integrity** : The professor or manager must be able to verify that collected feedback reflects genuine submissions from eligible individuals.

Threat Mitigation

> SR 9 **Resistance to Impersonation** : Attackers must not be able to impersonate authorized individuals to submit feedback fraudulently.

> SR 10 **Resistance to Deanonymization** : The system must not leak identifying metadata through network traffic, timing signals, or platform behavior.

> SR 11 **Secure Communication** : All communication must occur over secure channels to prevent eavesdropping or tampering.

Functional Requirements

In this section, we outline the functional requirements for the anonymous feedback system.

> FR 1 **Identity Verification** : The system must verify an individual's enrollment or employment status before issuing a submission credential.

> FR 2 **Anonymous Credential Issuance** : The system must provide a way to issue credentials that authenticate users while preserving anonymity.

> FR 3 **Feedback Submission** : Users must be able to submit feedback anonymously using the previously issued credential.

> FR 4 **Pseudonym Generation** : The system must generate pseudonyms or cryptographic tags that allow linking multiple submissions by the same individual while keeping identities hidden.

> FR 5 **Duplicate Detection Mechanism** : The system must detect multiple submissions from the same individual, enabling fairness enforcement.

> FR 6 **Submission Validation** : The server must validate that incoming submissions come from eligible users and have not been tampered with.

> FR 7 **Feedback Aggregation** : The system must aggregate feedback for the professor or manager in a way that preserves anonymity while ensuring authenticity.

Non-Functional Requirements

Performance

> NFR 1 **Efficient Verification** : Identity and credential verification should be fast and scalable to courses or workplaces with many participants.

> NFR 2 **Low Submission Overhead** : Feedback submission should require minimal computation and delay for users.

Scalability

> NFR 3 **Support for Large User Groups** : The system must scale to thousands of students or employees without degrading performance.

> NFR 4 **Efficient Pseudonym Handling** : The system must maintain efficient operations even when generating and comparing pseudonyms for duplicate detection.

Usability

> NFR 5 **Simple User Experience** : The submission process must be straightforward and accessible without requiring advanced technical knowledge.

> NFR 6 **Transparent Privacy Guarantees** : Users must be clearly informed that their anonymity is protected to encourage honest feedback.

Reliability & Availability

> NFR 7 **High Availability** : Users must be able to submit feedback reliably within the designated time window.

> NFR 8 **Fault Tolerance** : Failures or server restarts must not affect previously issued credentials or submitted feedback.

Compliance & Governance

> NFR 9 **Data Minimization** : The system must collect and store only the minimum necessary information for verification and aggregation.

> NFR 10 **Regulatory Compliance** : The system should comply with relevant privacy regulations (e.g. GDPR) depending on the environment.

> NFR 11 **Secure Data Retention Policies** : Stored feedback must be protected and deleted according to institutional or regulatory requirements.