University of Trento

Advanced Programming of Cryptographic Methods

Confidential But Genuine Feedback

Graduate Student
Filippo De Grandi

Date: 19/11/2025

Contents

Description

Consider a university scenario where a professor is collecting feedback from students to improve the course. On one hand, students may be reluctant to share honest opinions without guarantees of anonymity, on the other, the professor wants to consider the opinions of only the students enrolled in the course. A similar scenario can be applied in a workplace where a manager seeks honest feedback from employees. The goal is to ensure that employees feel confident in their anonymity, allowing them to freely express their opinions without fear of reprisal, but still allow the manager to verify that the feedback is genuinely coming from the employees. An extra feature required is fairness in the submissions: to avoid that the opinion of a very vocal few unduly seems widespread, it should be possible to determine whether two messages were originated by the same entity. This feature would in fact allow for detecting multiple feedback submissions from the same individual.

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

> SR 2 **Unlinkability of Messages** : Apart from controlled fairness mechanisms, submissions must not be linkable to an identity or to other metadata that could reveal the originator.

> 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 **Verified Eligibility** : Only authorized individuals (students enrolled in a course or employees of a workplace) may submit feedback.

> SR 5 **Non-Transferable Authorization** : Feedback credentials must be bound to an individual and not transferable to others.

> SR 6 **Single-Submission Enforcement** : The system must ensure that each individual can submit feedback at most once, unless the system explicitly allows multiple submissions.

Fairness & Duplicate Detection

> SR 7 **Pseudonymous Consistency** : The system must allow determining whether two submissions come from the same entity without revealing the entity's identity.

> SR 8 **Duplicate Submission Detection** : It must be possible to flag multiple submissions from the same individual while preserving their anonymity.

Integrity

SR 9 **Message Integrity** : Feedback submissions must not be modifiable in transit or on the server without detection.

SR 10 **Result Integrity** : The professor or manager must be able to verify that collected feedback reflects genuine submissions from eligible individuals.

Threat Mitigation

SR 11 **Resistance to Impersonation** : Attackers must not be able to impersonate authorized individuals to submit feedback fraudulently.

SR 12 **Resistance to Deanonymization Attempts** : The system must not leak identifying metadata through network traffic, timing signals, or platform behavior.

SR 13 **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 eligibility 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, FERPA) depending on the environment.

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