Project Work – Algoritmi e Protocolli per la Sicurezza

Docenti: Carlo Mazzocca, Francesco Cauteruccio

A.A. 2024-2025

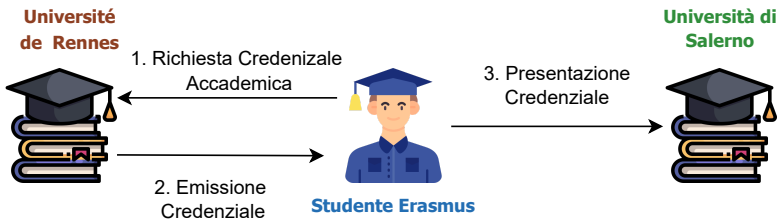

Figure 1: Condivisione selettiva di credenziali accademiche tra Université de Rennes e Università di Salerno.

Premessa. Nel contesto del programma Erasmus e, più in generale, della mobilità studentesca internazionale, la condivisione di credenziali accademiche (esami superati, titoli ottenuti, attestazioni di frequenza, etc.) tra enti di istruzione superiore pone numerose sfide in termini di sicurezza, privacy, interoperabilità e revocabilità. I meccanismi attualmente adottati si basano spesso su scambi manuali o su sistemi centralizzati che:

- richiedono la fiducia in autorità centrali per la verifica delle credenziali;
- non garantiscono la privacy dello studente, che spesso è costretto a rivelare più informazioni del necessario;
- non prevedono una gestione chiara e decentralizzata della revoca delle credenziali;

- risultano poco scalabili e difficilmente interoperabili tra i diversi sistemi nazionali e universitari.

Nel frattempo, tecnologie emergenti, offrono nuove opportunità per progettare meccanismi di rilascio, presentazione e revoca delle credenziali che siano:

- decentralizzati e resistenti alla censura;
- privacy-preserving, grazie a tecniche di *divulgazione selettiva*;
- interoperabili tra istituzioni diverse, anche in ambito transnazionale;
- in grado di supportare dinamiche di revoca robuste e verificabili pubblicamente.

Esempio. Si consideri il caso di uno studente iscritto al corso di laurea magistrale in Ingegneria Informatica presso l'Università di Salerno che partecipa a un periodo di mobilità Erasmus presso l'Université de Rennes. Durante la fase di riconoscimento degli esami sostenuti all'estero, lo studente deve dimostrare di aver completato con successo solo specifici insegnamenti presso l'università ospitante. In un sistema tradizionale, ciò comporta l'invio di documenti firmati o certificati digitali tramite canali centralizzati e spesso non interoperabili. La Figura 1 fornisce una visione di alto livello dello scambio di credenziali.

Utilizzando invece un meccanismo basato su credenziali digitali accademiche, l'Université de Rennes può rilasciare una credenziale che attesta il superamento di un determinato esame. Lo studente può quindi presentare all'Università di Salerno una versione della credenziale contenente solo le informazioni strettamente necessarie, preservando la propria privacy grazie a tecniche di divulgazione selettiva. Ad esempio, lo studente non dovrà rivelare le attività facoltative a cui ha preso parte. Inoltre, qualora la credenziale venisse revocata (es. per errore amministrativo), l'Università di Salerno potrebbe verificarne la validità.

Obiettivo. Progettare un meccanismo decentralizzato per la condivisione selettiva e la revoca di credenziali accademiche, da utilizzare in contesti di mobilità studentesca come il programma Erasmus.

Da considerare:

- solo gli utenti (studenti, università, enti di accreditamento) autenticati possono usufruire dei servizi offerti;
- progettare le credenziali accademiche, consentendo agli studenti di condividere solo sottoinsiemi delle informazioni contenute in modo verificabile senza dover interrogare direttamente l'ente che ha rilasciato le credenziali;
- è necessario definire un meccanismo che consenta di revocare le credenziali accademiche per comportamento scorretti (es. plagio, frode documentale).
- i meccanismi di divulgazione selettiva e revoca progettati dovrebbero minimizare i consumi di memoria e rete, consentendo il loro utilizzo anche su dispositivi con risorse limitati (es. wallet hardware).
- è fondamentale l'originalità del lavoro svolto; gli studenti devono dimostrare padronanza delle tecnologie e dei concetti affrontati durante il corso;
- il docente non si aspetta soluzioni rivoluzionarie per il sistema Erasmus, ma piuttosto l'applicazione competente delle conoscenze acquisite per proporre un modello realistico (funzionalità con parti oneste + threat model + proprietà di resilienza), una soluzione coerente, un'analisi critica e un'implementazione significativa.

Struttura. Il project work dovrà essere organizzato in 4 work packages. Tutte le scelte nei 4 work packages devono essere motivate, spiegate/illustrate e documentate.

WP 1: Modello. Questo work package si occuperà di definire i vari attori onesti del sistema e i loro obiettivi, specificando quindi la funzionalità che si intende realizzare. Dovranno essere poi discussi i possibili avversari (threat model) interessati a compromettere il sistema (specificando le loro risorse/capacità). Vanno identificate le proprietà che si vorrebbe poter preservare in presenza di attacchi. Il soddisfacimento della funzionalità e delle proprietà individuate permetterà poi di misurare (non in questo WP)

la bontà di una progettazione che prova a realizzare tale funzionalità in presenza di avversari. In questo WP dovrà essere anche definita la struttura (campi) della credenziale.

Nota 1.1: questo WP non deve mostrare una soluzione al problema.

Nota 1.2: è importante discutere in modo comprensibile, dettagliato e non ambiguo la funzionalità che si vuole realizzare, i possibili obiettivi/attacchi degli avversari (incluse le loro risorse), le proprietà di resilienza del sistema in presenza di attacchi. Non è necessario presentare definizioni formali (presentarne anche solo qualcuna è un plus).

WP 2: Soluzione. Dato il modello identificato in WP 1, mostrare un sistema di gestione delle credenziali accademiche con l'obiettivo di raggiungere un ragionevole compromesso tra efficienza, trasparenza, confidenzialità e sicurezza. La progettazione deve descrivere dettagliatamente tutte le azioni delle parti oneste coinvolte nel sistema.

Nota 2.1: Questo WP non richiede di dimostrare che la soluzione proposta soddisfi le proprietà descritte in WP 1. La progettazione, quindi, non deve presentare attacchi, eccetto che nel motivare, commentare e discutere le scelte progettuali si possano, ove utile, indicare le criticità che si prova a mitigare attraverso di esse.

Nota 2.2: Si richiede l'uso corretto degli strumenti studiati durante il corso, non è necessario individuare/studiare nuovi strumenti. Si consiglia di non risparmiare risorse sulla progettazione nel timore di dover implementare troppo in WP4. Nel caso ci sia un eccesso di contenuti da implementare, è possibile contattare i docenti e definire un sottoinsieme di funzionalità da implementare in WP4.

WP 3: Analisi della sicurezza. Questo work package ha lo scopo di analizzare la sicurezza della soluzione presentata in WP2 rispetto al modello presentato in WP1. Gli studenti devono verificare attentamente che non ci siano ovvie modifiche apportabili a WP2 che portino benefici in alcune proprietà senza alcuna perdita in altre.

WP 4: Implementazione e prestazioni. Implementare il sistema di gestione delle credenziali accademiche progettato in WP2 (anche solo una parte di esso se le funzionalità sono tante) in un ambiente simulato (ad es., non è necessario sviluppare un'applicazione per smartphone, la si può simulare

mediante applicazione stand-alone in esecuzione su un computer). Mostrare anche le prestazioni ottenute con la sperimentazione come dimensione delle credenziali e presenazioni, e latenza di verifica.

Valutazione. La valutazione massima del project work è di 12 punti. Ogni work package è valutato da 0 a 3 punti e questo forma il punteggio di partenza assegnabile ai membri del gruppo supponendo che:

- gli studenti abbiano equamente contribuito al project work;
- gli studenti abbiano adeguatamente presentato il contenuto del project work durante il colloquio;
- il punteggio di partenza corrisponda anche alla qualità del lavoro svolto nel suo complesso. Quando invece il contributo del singolo studente (inclusa la sua capacità di presentare il lavoro svolto), sulla base delle linee di indirizzo dei project work, sarà valutato negativamente, allora il punteggio assegnato dalla commissione a tale studente sarà proporzionalmente ribassato

Gli studenti possono in qualunque momento contattare i docenti per palesare criticità dovute a contributi insoddisfacenti di altri membri del gruppo o altre informazioni utili ad un'equilibrata valutazione.

Consegna. La consegna consiste di un file pdf che illustrerà WP1, WP2, WP3 e le scelte implementative di WP4 insieme con eventuali analisi/discussioni. I sorgenti relativi a WP4 saranno invece allegati in un file di archivio o condiviso tramite repository GitHub.

Entro la fine del corso dovrà essere consegnato almeno il 50% nella seguente modalità: si richiede il 100% di WP1 ed una bozza principalmente di WP2 e, addizionalmente, di WP3 che corrisponda approssimativamente ad almeno il 50% del totale WP2+WP3. La consegna completa del project work deve avvenire entro una settimana prima dell'appello che si intende sostenere.

La consegna completa dovrà indicare anche il "responsabile" per ogni WP. Ogni studente sarà responsabile di 2 WP.

Validità. La valutazione ottenuta dura 12 mesi dalla consegna. In caso di mancato superamento dell'esame nei 12 mesi successivi alla consegna, lo

studente può coordinarsi col docente per discutere la necessità di eventuali integrazioni al project work.

Tutti gli studenti del gruppo devono partecipare insieme alla discussione e valutazione del proprio project work, resta tuttavia possibile sostenere la prova orale (scritta) anche separatamente.