

# Project Work – Algoritmi e Protocolli per la Sicurezza

Docenti: Carlo Mazzocca, Francesco Cauteruccio

A.A. 2024-2025

**Premessa.** Nel sistema sanitario moderno, la condivisione di referti medici (esami diagnostici, cartelle cliniche, prescrizioni, certificazioni) tra ospedali, laboratori e medici di base è essenziale per garantire continuità assistenziale e diagnosi accurate. Tuttavia, la trasmissione di questi dati sensibili comporta rischi significativi:

- violazioni della privacy del paziente;
- falsificazione o manomissione dei referti;
- difficoltà nella verifica dell'autenticità;
- mancanza di tracciabilità e controllo delle versioni.

Un protocollo sicuro per la trasmissione di referti medici può migliorare la fiducia tra le strutture, ridurre gli errori clinici e garantire la conformità alle normative (es. GDPR).

**Esempio.** Si consideri il caso di un paziente che effettua un esame diagnostico (es. risonanza magnetica) presso un laboratorio privato convenzionato. Il referto deve essere trasmesso all'ospedale pubblico dove il paziente è in cura, affinché il medico specialista possa consultarlo e proseguire con la diagnosi.

In un sistema tradizionale, il referto viene inviato via email o caricato su una piattaforma centralizzata, spesso senza garanzie di integrità, autenticità o tracciabilità. Inoltre, il paziente non ha controllo su chi accede al documento, e l'ospedale non può verificare se il referto sia stato modificato o se sia ancora valido (es. non revocato per errore diagnostico).

**Obiettivo.** Progettare, analizzare e implementare un protocollo per la trasmissione sicura, verificabile e tracciabile di referti medici tra strutture sanitarie:

**Da considerare:**

- autenticazione delle parti coinvolte (laboratori, ospedali, medici, pazienti);
- i referti non devono poter essere modificati e l'ente che li ha emessi non può ripudiarli;
- protezione della privacy del paziente, solo l'utente deve poter rendere accessibile il contenuto dei referti;
- possibilità di revoca e aggiornamento dei referti in caso di possibili errori;
- tracciabilità completa del ciclo di vita del referto: ogni accesso, modifica, revoca o aggiornamento deve essere registrato e verificabile;
- 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 package. Tutte le scelte nei 4 work package devono essere motivate, spiegate/illustrate e documentate.

**WP 1: Modello.** Questo work package si occuperà di definire i vari attori onesti del sistema (es. laboratorio diagnostico, ospedale, medico curante, paziente) e i loro obiettivi, specificando quindi la funzionalità che si intende realizzare: trasmissione sicura di referti medici, con garanzie di autenticità, integrità, privacy e revocabilità.

Dovranno essere poi discussi i possibili avversari (threat model) interessati a compromettere il sistema (specificando le loro risorse/capacità), come ad esempio:

- un attaccante che intercetta o modifica i referti;
- un ente che nega di aver emesso un referto (ripudio);
- un utente non autorizzato che accede ai dati sensibili del paziente.

Vanno inoltre identificate le proprietà che si vorrebbe poter preservare in presenza di attacchi:

- **Autenticità:** il referto deve provenire da un ente sanitario riconosciuto;
- **Integrità:** il contenuto del referto non deve essere alterabile;
- **Confidenzialità:** solo il paziente può autorizzare l'accesso al contenuto;
- **Revocabilità:** un referto può essere invalidato in caso di errore;
- **Auditabilità:** ogni accesso e modifica devono essere tracciabili.

*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 protocollo per la trasmissione sicura dei referti medici, 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, includendo:

- il formato dei messaggi;
- le operazioni crittografiche;
- il flusso di comunicazione tra le parti;
- le modalità di accesso controllato ai referti;

- il meccanismo di revoca e aggiornamento.

*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 protocollo 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 un'applicazione stand-alone in esecuzione su un computer). Mostrare anche le prestazioni ottenute con la sperimentazione, come la dimensione dei referti e la latenza di generazione/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 (in-

clusa 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.