**UNIVERSITÀ DEGLI STUDI DI SALERNO**

DIPARTIMENTO DI INGEGNERIA DELL’INFORMAZIONE

ED ELETTRICA E MATEMATICA APPLICATA



Algoritmi e Protocolli per la Sicurezza

Project Work – WP1

Gruppo 26

Membri:

|  |  |  |  |
| --- | --- | --- | --- |
| Antonio Carbone | a.carbone88@studenti.unisa.it | 0622702566 | WP x-x |
| Enrico Cavuoto | e.cavuoto1@studenti.unisa.it | 0622702565 | WP x-x |

[WP1 – Modello 3](#_Toc199067667)

[1.1. Introduzione 3](#_Toc199067668)

[1.2. Attori onesti del sistema 3](#_Toc199067669)

[1.2.1. Università estera 3](#_Toc199067670)

[1.2.2. Studente 3](#_Toc199067671)

[1.2.3. Università di origine 4](#_Toc199067672)

[1.3. Possibili attaccanti del sistema 4](#_Toc199067673)

[1.3.1. Man in the middle passivo 4](#_Toc199067674)

[1.3.2. Utente certificato malintenzionato 4](#_Toc199067675)

[1.3.3. Man in the middle attivo 5](#_Toc199067676)

[1.3.4. Ente certificatore fasullo 5](#_Toc199067677)

[1.3.5. Ente certificatore malintenzionato 6](#_Toc199067678)

[1.3.6. Sosia 6](#_Toc199067679)

[1.3.7. Revoca inefficace 7](#_Toc199067680)

[1.3.8. Università fantasma 7](#_Toc199067681)

[1.4. Proprietà 8](#_Toc199067682)

[1.4.1. Integrità dei dati 8](#_Toc199067683)

[1.4.2. Confidenzialità dei dati 8](#_Toc199067684)

[1.4.3. Autenticazione 8](#_Toc199067685)

[1.4.4. Non ripudio 8](#_Toc199067686)

[1.4.5. Efficienza 8](#_Toc199067687)

[1.5. Il formato della credenziale 9](#_Toc199067688)

[1.5.1. Struttura della credenziale 9](#_Toc199067689)

# WP1 – Modello

## Introduzione

Il progetto ha come obiettivo la realizzazione di una architettura per il rilascio e la diffusione di credenziali universitarie contenenti informazioni riguardanti attività svolte da uno studente universitario in Erasmus.

In particolar modo, si è alla ricerca di una soluzione che si discosti dalle tradizionali architetture dipendenti da una singola autorità centrale, permettendo verifiche di validità decentralizzate e divulgazione selettiva delle informazioni contenute all’interno.

Il possessore della credenziale, difatti, deve essere in grado di fornire parte delle informazioni contenute, consentendo all’ente verificatore di attestarne l’integrità e l’autenticità rispetto a quanto certificato dall’ente che le ha rilasciate.

Questo Work Package si pone l’obiettivo di:

1. Analizzare gli attori onesti del sistema
2. Individuare i threat model correlati a tutti i possibili attaccanti del sistema
3. Valutare le proprietà di sicurezza che l’architettura deve rispettare
4. Fornire una struttura alla credenziale universitaria

## Attori onesti del sistema

### Università estera

È, in questo scenario, l’organo preposto al rilasci

o di credenziali firmate e risulta pertanto un’entità fidata rispetto a tutti gli altri attori onesti del sistema. Quest’ultima, attraverso la generazione di tali credenziali, consente allo studente di certificare alla sua università di origine quanto svolto durante il suo soggiorno all’estero.

### Studente

Detiene il possesso della credenziale nei suoi dispositivi, i quali possono essere di svariata natura, ad es. Smartphone, PC, Tablet, Wallet Hardware.

Può generare una credenziale contenente un set ridotto delle informazioni contenute in essa, condividendo, a qualunque università o ad altri enti, esclusivamente quanto a lui necessario.

### Università di origine

Ha la possibilità di verificare la validità di una credenziale fornita dallo studente al rientro dall’esperienza Erasmus, garantendo che essa non risulti revocata, certificandone l’autenticità e l’integrità dei dati, seppur parziali, contenuti all’interno di quest’ultima.

Si richiede che la validità sia verificata in maniera decentralizzata, evitando di interrogare l’ente certificatore per effettuare questa operazione.

## Possibili attaccanti del sistema

### Immagine che contiene schermata, diagramma, testo, schizzo Il contenuto generato dall'IA potrebbe non essere corretto.Man in the middle passivo

Utente terzo che vuole leggere le info del certificato, questo può avvenire sia intercettando la comunicazione della credenziale completa dall’università estera allo studente, oppure quando quest’ultimo condivide parzialmente la credenziale al rientro dal periodo di Erasmus.

#### Risorse e capacità dell’attaccante

L’attaccante dispone di una potenza di calcolo limitata, ma ha accesso ai canali di comunicazione utilizzati dalle parti oneste.

### Immagine che contiene schermata, diagramma, testo, Carattere Il contenuto generato dall'IA potrebbe non essere corretto.Utente certificato malintenzionato

Utente possessore della credenziale intenzionato a modificarne il contenuto in modo tale da trarne vantaggio. Per esempio, sostituendo i voti ottenuti in Erasmus con voti più alti così da alzare la media al rientro nell’università italiana.

#### Risorse e capacità dell’attaccante

Immagine che contiene testo, diagramma, schizzo, schermata

Il contenuto generato dall'IA potrebbe non essere corretto.L’attaccante dispone di una potenza di calcolo limitata ma ha pieno accesso alla propria credenziale universitaria, ai canali di comunicazione e la sua identità è riconosciuta da tutte le parti oneste coinvolte.

### Man in the middle attivo

Utente terzo che vuole modificare le informazioni del contratto intercettato durante la comunicazione tra l’utente possessore delle credenziali e l’altra parte onesta. Questo può accadere sia in favore dell’utente certificato che in sfavore. Per esempio, l’utente terzo può essere un amico dell’utente possessore delle credenziali intenzionato ad aiutarlo alzandogli i voti ottenuti in Erasmus, oppure può essere un malintenzionato che vuole abbassarli o modificare dati sensibili in modo tale da creare problemi all’utente certificato.

#### Risorse e capacità dell’attaccante

Risorse computazionali limitate ma ha accesso ai canali di condivisione della credenziale.

### Immagine che contiene diagramma, schermata, origami, schizzo Il contenuto generato dall'IA potrebbe non essere corretto.Ente certificatore fasullo

Ente certificatore, all’apparenza affidabile, che rilascia credenziali con informazioni false che vengono però riconosciute dagli enti di validazione.

Ad esempio, un ente malevolo al quale lo studente si rivolge per acquistare una credenziale che attesti un’esperienza Erasmus mai avvenuta.

#### Risorse e capacità dell’attaccante

Dispone di risorse computazionali elevate e ha la possibilità di registrare delle credenziali totalmente conformi all’iter di verifica.

### Immagine che contiene schermata, diagramma, schizzo, bianco Il contenuto generato dall'IA potrebbe non essere corretto.Ente certificatore malintenzionato

In questo caso è un ente certificatore autorizzato ed inizialmente fidato che agisce in maniera fraudolenta rilasciando credenziali modificate con informazioni non veritiere.

Ad esempio, un’università che rilascia certificati modificati in modo da favorire i suoi studenti.

#### Risorse e capacità dell’attaccante

Immagine che contiene schermata, Carattere, diagramma, testo

Il contenuto generato dall'IA potrebbe non essere corretto.Dispone di risorse computazionali elevate ed ha la possibilità di registrare delle credenziali valide.

### Sosia

Utente terzo che vuole fingersi lo studente possessore della credenziale presentando il suo certificato, precedentemente ottenuto in qualche maniera.

Ad esempio, lo studente Mario Rossi potrebbe tentare di utilizzare la credenziale parziale contenente l’esito di un esame svolto da un suo collega, con lo scopo di ottenerne la convalida.

#### Risorse e capacità dell’attaccante

Dispone di risorse computazionali minime ma ha accesso ad una credenziale sottratta ad un altro studente.

### Forgiatore di credenziale

Utente terzo che vuole falsificare autonomamente una credenziale fasulla che certifica una esperienza di studio all’estero mai avvenuta al fine di trarne beneficio nella sua carriera universitaria.

Ad esempio, lo studente Mario Rossi potrebbe tentare di generare una credenziale a partire dalle specif

#### Risorse e capacità dell’attaccante

Dispone di risorse computazionali minime ma ha accesso ad una credenziale sottratta ad un altro studente.

### Immagine che contiene testo, diagramma, schermata, schizzo Il contenuto generato dall'IA potrebbe non essere corretto.Revoca inefficace

Una credenziale revocata dall’emittente potrebbe passare i controlli applicati da un ente verificatore, a causa di un meccanismo di revoca lento, inefficace o inaffidabile.

Tale vulnerabilità permetterebbe ad un malintenzionato di continuare a trarre beneficio, per un periodo successivo alla revoca, da una credenziale non più valida.

#### Risorse e capacità dell’attaccante

L’attaccante non dispone di risorse computazionali considerevoli, l’attacco può avere successo o meno a seconda di fattori che non sono da lui direttamente controllabili.

### Immagine che contiene schizzo, testo, disegno, diagramma Il contenuto generato dall'IA potrebbe non essere corretto.Ente verificatore curioso

Un ente verificatore curioso è un soggetto terzo inizialmente fidato che tenta di ricavare informazioni ulteriori rispetto a quelle che gli vengono comunicate.

Questo può avvenire attraverso:

* Analisi statistiche sulla credenziale fornita.
* Attacchi di forza bruta su specifiche informazioni divulgate selettivamente, sfruttando conoscenze pregresse.

Ad esempio, un attaccante potrebbe analizzare le prove Merkle fornite per cercare l'hash di un esame superato di cui conosce il nome e, potenzialmente, i CFU. Tenterebbe di indovinare il voto e la data di convalida, iterando su possibili valori all'interno di un intervallo ristretto.

#### Risorse e capacità dell’attaccante

Dispone di risorse computazionali medio-alte e ha accesso ad una credenziale parzialmente condivisa ottenuta in maniera legittima.

## Proprietà

### Integrità dei dati

|  |  |
| --- | --- |
| ID | Proprietà |
| I.1. | Le informazioni certificate attraverso la credenziale non devono poter essere modificabili da nessuna parte onesta o meno. |

### Confidenzialità dei dati

|  |  |
| --- | --- |
| ID | Proprietà |
| C.1. | Le credenziali devono essere condivise tra le parti oneste garantendo la confidenzialità |
| C.2. | Lo storage della credenziale da parte dello studente deve avvenire in maniera sicura |

### Autenticazione

|  |  |
| --- | --- |
| ID | Proprietà |
| A.1. | Le informazioni contenute all’interno delle credenziali rilasciate dall’ente fidato devono essere autentiche ed essa deve poter essere verificata da chi riceve tali informazioni. |
| A.2. | Le identità delle parti coinvolte nello scambio di informazioni (credenziali totali o parziali) devono essere verificabili. |

### Non ripudio

|  |  |
| --- | --- |
| ID | Proprietà |
| NR.1. | L’ente certificatore non può ripudiare una credenziale dopo averla rilasciata. |

### Efficienza

|  |  |
| --- | --- |
| ID | Proprietà |
| E.1. | Il meccanismo di storage delle credenziali deve essere efficiente, consentendo l’utilizzo di hardware-wallet o dispositivi con risorse computazionali limitate. |
| E.2. | Il meccanismo di verifica delle credenziali deve essere efficiente e decentralizzato. |

## Il formato della credenziale

Immagine che contiene testo, schermata, Carattere, numero

Il contenuto generato dall'IA potrebbe non essere corretto.Si è scelto di implementare la credenziale con uno schema che risulta condiviso tra la credenziale completa rilasciata dall’università ospitante e la credenziale parziale che può essere generata dall’owner. Il formato è il seguente:

### Struttura della credenziale

La credenziale può essere suddivisa in 2 sezioni principali, la prima comprende:

* tutti i campi che sono relativi all’ente che ha emesso la certificazione
* data di emissione e l’identificativo univoco del documento
* informazioni anagrafiche sull’owner del certificato

Nella seconda sezione, denominata properties, sono presenti tutte le informazioni che devono essere inserite nel certificato, comprendendo ad esempio gli esami di profitto svolti, le attività extra, il luogo di residenza all’estero ma anche informazioni riguardanti eventuali compensi economici che lo studente ha ricevuto durante la sua esperienza Erasmus.

Una credenziale parziale derivata da quest’ultima può contenere un numero inferiore di properties ma deve necessariamente contenere la restante parte delle informazioni della parte fissa.