UNIVERSITÀ DEGLI STUDI DI SALERNO

DIPARTIMENTO DI INGEGNERIA DELL'INFORMAZIONE ED ELETTRICA E MATEMATICA APPLICATA

Corso di Laurea Magistrale in Ingegneria Informatica

eCRED

Nome	Cognome	Matricola	E-Mail
Michele	Martino	0622702424	m.martino48@studenti.unisa.it
Francesco	Quagliuolo	0622702412	f.quagliuolo@studenti.unisa.it
Emanuele	Relmi	0622702368	e.relmi@studenti.unisa.it
Benito	Senese	0622702425	b.senese1@studenti.unisa.it

ANNO ACCADEMICO 2023/2024

INDICE

CAPITOLO 1

WORK PACKAGE 1

In questo primo capitolo ci concentreremo sulla definizione degli attori onesti coinvolti nel sistema, analizzando i loro obiettivi e le funzionalità che si intendono realizzare. Gli attori onesti sono quegli individui o entità che agiscono in conformità con le regole e le politiche stabilite, cercando di raggiungere i loro obiettivi senza compromettere l'integrità del sistema.

Successivamente, esamineremo i possibili avversari (o threat models) che potrebbero essere interessati a compromettere il sistema, esaminando le loro risorse e le motivazioni che li spingono ad agire. Questa analisi ci permetterà di identificare gli attacchi che il sistema potrebbe subire e di comprendere quali misure di sicurezza dovranno essere adottate per contrastarli.

Una volta compreso il contesto in cui il sistema opera, identificheremo le proprietà di sicurezza che si vorrebbero preservare in presenza di attacchi. Queste proprietà sono fondamentali per garantire il corretto funzionamento del sistema e la protezione delle informazioni sensibili.
Di seguito un elenco dettagliato di tali attori e delle loro responsabilità.

1.1 Attori del Sistema

1.1.1 Utente

Gli utenti sono le persone che necessitano di accedere ai servizi qualificati offerti dai server. Ogni utente possiede una Carta d'Identità Elettronica (CIE) che contiene le credenziali rilasciate dalle autorità competenti. La CIE permette agli utenti di firmare digitalmente le loro richieste di accesso, garantendo così l'integrità e l'autenticità delle

credenziali presentate. I loro obiettivi sono: richiedere e ottenere le credenziali necessarie dalle autorità, per poi utilizzarle per accedere a servizi specifici in modo sicuro; mentre il loro compito è quello di proteggere CIE e PIN da accessi non autorizzati.

1.1.2 Server

I server sono entità che offrono servizi qualificati, accessibili solo ai possessori di specifiche credenziali. I server devono essere in grado di verificare le credenziali presentate dagli utenti e stabilire se sono rilasciate da autorità fidate. Il loro obiettivo è offrire servizi in modo sicuro e limitato solo agli utenti autorizzati. Sono, inoltre, responsabili di gestire le richieste di accesso, garantire la sicurezza e la privacy delle operazioni e minimizzare il coinvolgimento di terze parti fidate così da ridurre i rischi legati ad un singolo punto di fallimento.

1.1.3 Autorità di Rilascio delle Credenziali

Le autorità di rilascio sono enti fidati che emettono credenziali agli utenti, garantendo che queste siano valide e affidabili. Queste autorità verificano l'identità degli utenti e le informazioni correlate prima di rilasciare le credenziali. Esse possono essere enti governativi, istituzioni pubbliche o altre organizzazioni autorizzate a rilasciare certificati digitali. Sono, quindi, responsabili di:

- verificare e validare le informazioni degli utenti;
- emettere credenziali autentiche;
- garantirne la sicurezza e l'integrità;
- mantenere un registro delle credenziali emesse.

1.1.4 Autorità Rilascio CIE

Gli enti che si occupano dell'emissione della CIE con il PIN associato sono fondamentalmente due, l'ufficio anagrafe e l'Istituto Poligrafico e Zecca dello Stato (IPZS), che vengono accorpati in un'unica entità per convenienza e semplicità. Questa autorità si occupa della verifica dell'identità degli utenti, della gestione delle pratiche amministrative relative alla registrazione delle informazioni anagrafiche e della generazione e gestione delle chiavi crittografiche e dei certificati digitali necessari per la firma elettronica. È responsabile di:

- verificare l'identità degli utenti;
- registrare le informazioni anagrafiche;

- produrre e consegnare la CIE, insieme al suo PIN, all'utente;
- generare e memorizzare in modo sicuro le chiavi segrete e i certificati digitali all'interno della CIE;
- garantire che i certificati digitali siano validi e riconosciuti dalle autorità competenti;
- implementare misure di sicurezza avanzate per proteggere la CIE da contraffazioni e accessi non autorizzati.

1.2 Attaccanti del Sistema

Nel contesto del sistema descritto, è fondamentale analizzare e comprendere i potenziali attaccanti che potrebbero cercare di comprometterlo, considerando le loro motivazioni e le risorse a loro disposizione. Questi attori e gruppi di attaccanti rappresentano diverse minacce al sistema e richiedono misure di sicurezza specifiche per essere contrastati efficacemente.

- **Anti-Tech Theorist**
  - **Tipologia:** passivo/attivo
  - **Descrizione:** avversario che si oppone all'innovazione e all'adozione di nuove tecnologie, sostenendo che qualunque dispositivo può essere compromesso, a discapito della privacy degli utenti. Il suo scopo è quello di amplificare notizie di violazioni di dati o problemi di privacy dei sistemi per influenzare l'opinione pubblica e screditare le nuove proposte nell'ambito della sicurezza informatica.
  - **Risorse**
    * Abilità comunicative elevate
    * Rete di contatti con altri oppositori delle nuove tecnologie
    * Accesso ai media e ai social network per diffondere messaggi allarmistici
- **The Eavesdropper**
  - **Tipologia:** passivo
  - **Descrizione:** avversario interessato a intercettare tutte le operazioni svolte tramite il sistema (autenticazione, dati della CIE, etc.). Questa tipologia di avversario può essere sia interna all'organizzazione che esterna. L'obiettivo principale è quello di collezionare le informazioni inerenti agli utenti, senza però compromettere i protocolli, i quali sono eseguiti onestamente.
  - **Risorse**

    * Conoscenza approfondita delle tecniche di intercettazione e analisi delle comunicazioni, nonché della crittografia utilizzata nel sistema per comprendere e interpretare correttamente i dati intercettati

    * Capacità di monitorare e intercettare le comunicazioni tra gli utenti e il sistema, compresi i messaggi di autenticazione, i dati della CIE e qualsiasi altra informazione scambiata

    * Disponibilità di risorse computazionali significative per analizzare e elaborare grandi quantità di dati intercettati

- **Malevolent Server**
  - **Tipologia:** attivo
  - **Descrizione:** server con comportamento malevolo. I suoi compiti includono: la corretta gestione delle connessioni, la verifica delle credenziali e l'erogazione del servizio richiesto. Tuttavia, questa tipologia di avversario sfrutta le informazioni ricevuti dagli utenti per scopi illeciti, come il riutilizzo di informazioni personali, la vendita dei dati carpiti a terzi, compromettendo la privacy degli utenti.
  - **Risorse**
    * Controllo completo sui dati e sulle risorse del server, inclusi database utenti, registri di accesso e altri dati sensibili

    * Possibilità di accedere alle credenziali ricevute per l'accesso al servizio, consentendo di utilizzare queste informazioni per scopi illeciti.

- **The Impersonator**
  - **Tipologia:** attivo
  - **Descrizione:** avversario che, essendo entrato in possesso di informazioni personali di un utente, si maschera personificando quest'ultimo. Mira ad ottenere uno o più servizi a nome della persona di cui ha i dati.
  - **Risorse**
    * Possesso di un vasto database di informazioni personali ottenute illegalmente, che consente la creazione di profili dettagliati delle vittime e di utilizzare le informazioni per scopi malevoli

- **Identity Thief**
  - **Tipologia:** attivo

  - **Descrizione:** avversario che mira a rubare identità o credenziali per impersonare gli utenti legittimi e ottenere accesso non autorizzato ai servizi. Potrebbe utilizzare tecniche di phishing, furto di credenziali o exploit delle vulnerabilità per ottenere informazioni sensibili e assumere l'identità di altri utenti.
  - **Risorse**
    * Disponibilità di risorse computazionali sufficienti per eseguire attacchi brute-force, decrittazione o altri metodi per ottenere informazioni sensibili o compromettere la sicurezza del sistema
    * Competenze nel phishing e nell'ingegneria sociale, accesso a database di credenziali rubate, capacità di creare siti web e messaggi convincenti

- **The Denier**
  - **Tipologia:** attivo
  - **Descrizione:** avversario il cui scopo è compromettere il sistema, colpendo gli utenti o i servizi contemporaneamente. Potrebbe utilizzare botnets, malware o attacchi DoS/DDoS per sovraccaricare o infiltrare il sistema, causando danni diffusi e gravi interruzioni del servizio.
  - **Risorse**
    * Capacità di coordinare attacchi su vasta scala
    * Accesso a risorse informatiche distribuite (come server cloud, dispositivi IoT compromessi o altre infrastrutture che possono essere sfruttate per eseguire attacchi distribuiti)
    * Possibilità di avere motivazioni finanziarie o ideologiche significative per condurre gli attacchi, come il lucro finanziario, il furto di dati sensibili o il danneggiamento delle infrastrutture critiche per fini politici o di estorsione

- **Evil Insider**
  - **Tipologia:** passivo/attivo
  - **Descrizione:** avversario interno al sistema, che agisce in modo malevolo per ottenere benefici personali o danneggiare l'organizzazione. Potrebbe rubare credenziali o informazioni sensibili, manipolare il sistema o sabotare le operazioni per raggiungere i suoi obiettivi.
  - **Risorse**
    * Autorizzazioni elevate all'interno del sistema, compreso l'accesso a dati sensibili e risorse critiche

    * Conoscenza interna dei processi e delle vulnerabilità

- **The Cryptographer**
  - **Tipologia:** attivo
  - **Descrizione:** avversario che mira a compromettere la sicurezza del sistema, attaccando le autorità di certificazione o le infrastrutture chiave del sistema di identificazione, sfruttando vulnerabilità nei protocolli crittografici utilizzati per proteggere le comunicazioni e le credenziali. Potrebbe condurre attacchi di tipo man-in-the-middle, falsificare certificati o compromettere le chiavi crittografiche per ottenere accessi non autorizzati.
  - **Risorse**
    * Comprensione approfondita dei protocolli crittografici, dei meccanismi di autenticazione e delle vulnerabilità delle autorità di certificazione
    * Accesso a risorse computazionali per analizzare e rompere algoritmi crittografici
- **Data Miner**
  - **Tipologia:** passivo/attivo
  - **Descrizione:** questo avversario mira a raccogliere e sfruttare i dati degli utenti per fini di analisi, profilazione o vendita a terzi
  - **Risorse**
    * Competenze nell'analisi dei dati
    * Accesso a tecnologie per l'estrazione e l'elaborazione dei dati
    * Comprensione delle leggi sulla privacy e delle normative sul trattamento dei dati
- **The Data Harvesters**
  - **Tipologia:** attivo
  - **Descrizione:** questo gruppo mira a raccogliere e sfruttare i dati degli utenti per scopi di profitto o di spionaggio. Utilizzano una combinazione di tecniche di intercettazione, furto di identità e analisi dei dati per ottenere informazioni sensibili
  - **Risorse**
    * Competenze nell'intercettazione delle comunicazioni e nell'analisi dei dati (The Eavesdropper)

    * Accesso a database di informazioni personali rubate (Identity Thief)

    * Capacità di elaborare grandi quantità di dati raccolti per identificare opportunità di profitto o informazioni sensibili (Data Miner)

- **The Insider Threat Alliance**
  - **Tipologia:** attivo/passivo
  - **Descrizione:** questa coalizione è composta da attaccanti con accesso privilegiato al sistema, che agiscono internamente per ottenere benefici personali o danneggiare l'organizzazione. Collaborano per compromettere le infrastrutture critiche e sfruttare le informazioni riservate.
  - **Risorse**
    * Autorizzazioni elevate e conoscenza interna dei processi (Evil Insider)

    * Comprensione approfondita dei protocolli crittografici e delle vulnerabilità (The Cryptographer)

    * Controllo completo sui dati e sulle risorse del server (Malevolent Server)

- **Crypto Conspirators**
  - **Tipologia:** attivo
  - **Descrizione:** si concentra sull'attacco alla crittografia e alla sicurezza del sistema. Utilizzano competenze avanzate in crittografia, furto di identità e infiltrazione interna per compromettere la sicurezza
  - **Risorse**
    * Autorizzazioni elevate e conoscenza interna dei processi Competenze avanzate in crittografia e conoscenza dei protocolli di sicurezza (The Cryptographer)

    * Comprensione approfondita dei protocolli crittografici e delle vulnerabilità Accesso a informazioni personali rubate per ottenere accesso non autorizzato (Identity Thief)

    * Autorizzazioni elevate e accesso interno per facilitare gli attacchi (Evil Insider)

1.3 Proprietà

L'obiettivo è sviluppare un sistema che consenta l'accesso remoto a servizi riservati agli utenti in possesso delle credenziali richieste. In questo contesto, diverse autorità rilasciano

credenziali agli utenti, i quali le utilizzano per accedere a servizi qualificati, ossia servizi limitati ai possessori di specifiche credenziali.

Per garantire l'efficacia e la sicurezza del sistema, è necessario considerare diverse proprietà fondamentali: confidenzialità, integrità, trasparenza ed efficienza. Queste proprietà non solo assicurano che il sistema funzioni correttamente, ma proteggono anche contro potenziali minacce e abusi.

1.3.1 Confidenzialità

- **C1:** I dati sensibili degli utenti devono essere protetti, ovvero accessibili solo dalle parti autorizzate in modo controllato
- **C2:** Garantire la privacy delle comunicazioni tra gli utenti e i server che offrono i servizi, in modo che non sia possibile intercettare o rubare le credenziali trasmesse
- **C3:** Garantire la privacy delle comunicazioni tra gli utenti e le autorità di rilascio delle credenziali, in modo che non sia possibile carpire dati personali relativi agli utenti
- **C4:** Tutelare gli utenti contro i malintenzionati, di modo che questi ultimi non possano utilizzare l'identità di altri utenti, accedendo ai servizi sfruttando la loro CIE
- **C5:** Garantire che un utente non sia in grado di richiedere una CIE valida sfruttando informazioni non correlate alla sua persona

1.3.2 Integrità

- **I1:** Preservare l'integrità delle credenziali rilasciate, garantendo che non possano essere alterate o falsificate
- **I2:** Il sistema deve garantire che le credenziali esibite dagli utenti siano verificabili e autentiche, ovvero rilasciate da autorità riconosciute come affidabili
- **I3:** Verificare che le credenziali fornite dall'utente siano valide e corrispondano alle informazioni contenute nella CIE
- **I4:** La CIE restituisce una firma del messaggio solo se il PIN fornito corrisponde a quello memorizzato, garantendo che solo l'utente legittimo possa ottenere una firma valida
- **I5:** Verificare che la CIE sia riconducibile all'utente che la utilizza
- **I6:** Se un servizio è rivolto ad un individuo in possesso di due credenziali allora non deve essere possibile per due utenti, ciascuno avente una sola credenziale, combinare le loro informazioni per accedere al servizio

1.3.3 Trasparenza

- **T1:** Il sistema di autenticazione tramite CIE dovrebbe basarsi su algoritmi noti e verificabili, di modo da permettere una verifica di essi da parte degli utenti, rendendo arduo il processo di manomissione da parte di un malintenzionato, senza che quest'ultimo sia scoperto
- **T2:** Il processo di rilascio delle credenziali deve essere trasparente e verificabile da tutte le parti coinvolte, riducendo la dipendenza da terze parti fidate così da ridurre il rischio di abuso
- **T3:** Assicurarsi che le politiche di accesso ai servizi siano chiare e comprensibili, consentendo agli utenti di sapere quali credenziali siano necessarie per accedere agli stessi, limitando così la possibilità di accessi non autorizzati
- **T4:** La fiducia in specifiche parti deve essere giustificata da motivazioni concrete, come la possibilità di rilevare e punire abusi o il preservare la buona reputazione

1.3.4 Efficienza

- **E1:** Il sistema deve consentire ai server di controllare l'accesso utilizzando politiche avanzate e flessibili, permettendo di definire criteri di accesso complessi e specifici. Questo include la possibilità di esprimere condizioni logiche avanzate (come AND, OR, NOT) basate sulle credenziali degli utenti
- **E2:** Garantire che il processo di rilascio e verifica delle credenziali sia eseguito in modo rapido ed efficiente, riducendo al minimo i tempi di attesa e l'impatto sulle prestazioni del sistema
- **E3:** Assicurare che l'ottenimento delle credenziali tramite CIE avvenga in modo semplice e veloce, facilitando l'accesso remoto ai servizi digitali
- **E4:** Progettare il sistema in modo che possa gestire un grande numero di utenti e richieste contemporaneamente senza degradare le performance
- **E5:** Assicurarsi che il sistema sia compatibile con vari dispositivi e piattaforme, inclusi dispositivi mobili e desktop, per massimizzare l'accessibilità

CAPITOLO 2

WORK PACKAGE 2

In questo capitolo concentreremo la nostra attenzione nel presentare una soluzione che risponde al modello identificato nel *Work Package 1 (WP1)*. L'obiettivo è quello di proporre un sistema che riesca a raggiungere un ragionevole compromesso tra efficienza, trasparenza, confidenzialità e sicurezza.
Concentreremo la nostra attenzione sui seguenti problemi chiave:

- Richiesta e ottenimento della CIE
- Richiesta e ottenimento delle credenziali necessarie per l'accesso ai servizi specifici
- Autenticazione e accesso ai servizi qualificati
- Protezione della privacy e dell'integrità delle credenziali
- Minimizzazione del coinvolgimento di terze parti fidate

2.1 Panoramica Generale di Funzionamento

Innanzitutto, a valle di una richiesta apposita, viene emessa una CIE con il PIN associato per ogni utente. Ciascuno di essi, tramite l'utilizzo della CIE, può richiedere delle credenziali ad un'autorità di rilascio delle stesse. Esistono varie autorità che rilasciano credenziali agli utenti e, una volta entratone in possesso, è possibile utilizzarle per identificarsi e accedere ai servizi qualificati. È consentito, all'utente, l'accesso ai servizi qualificati solo se le credenziali soddisfano i requisiti di accesso imposti dal servizio stesso.

2.2 Generazione e Utilizzo delle Credenziali

In questa sezione verrà sviluppato un protocollo per la generazione e l'utilizzo di un sistema di identificazione tramite credenziali per l'accesso a servizi digitali qualificati. Questo processo coinvolge i seguenti attori chiave: l'utente, l'autorità di rilascio delle credenziali e il server del servizio. I partecipanti interagiscono con l'autorità per la richiesta e la generazione delle credenziali e con il server del servizio per usufruire dei servizi offerti. Si inizierà descrivendo come un utente può richiedere una credenziale all'autorità, chiarendo anche il processo di rilascio telematico della stessa. Successivamente, verrà delineato il contenuto e la struttura delle credenziali, affinché possano essere utilizzate come strumento digitale per l'identificazione e l'accesso ai servizi, mantenendo la massima riservatezza delle informazioni contenute. Infine, analizzeremo il processo di identificazione e accesso a un servizio digitale.

2.2.1 Supposizioni

Il funzionamento del protocollo proposto si basa sulle seguenti supposizioni:

- L'utente ha ottenuto la CIE e il PIN associato
- L'autorità di rilascio è fidata, emette credenziali corrette e rispetta il protocollo descritto
- Le informazioni necessarie alla verifica delle credenziali sono pubbliche, incluse gli algoritmi e i protocolli utilizzati
- L'autorità di rilascio possiede certificati validi per firmare le credenziali e per la comunicazione TLS con l'utente

Si procede adesso con l'analisi dettagliata di quanto delineato fino a questo momento.

2.2.2 Processo di Richiesta e Rilascio delle Credenziali

Generazione di una coppia di chiavi

- Ogni utente genera una coppia di chiavi pubblica/privata
- La chiave pubblica pk_{utente} è generata in accordo all'algoritmo Gen(1^n)
- La chiave pubblica dell'utente è registrata presso le autorità competenti

Richiesta delle Credenziali

- L'utente invia la sua chiave pubblica e la CIE alla CA
- La CA verifica l'identità dell'utente e, se verificata, emette una credenziale firmata digitalmente (X.509) contenente informazioni specifiche

- Ogni certificato X.509 emesso contiene un numero di serie univoco che identifica in modo univoco la credenziale associata all'utente

Emissione della Credenziale

- L'autorità firma digitalmente la credenziale utilizzando la propria chiave privata, creando così un documento X.509 che attesta le informazioni specifiche dell'utente

2.2.3 Processo di Identificazione e Accesso ai Servizi

Quando un utente presenta una credenziale per accedere a un servizio, il servizio deve verificare che l'utente possieda effettivamente la chiave privata corrispondente alla chiave pubblica inclusa nel documento X.509.

Verifica delle Credenziali

- Il servizio decodifica la credenziale X.509 e verifica la firma digitale dell'autorità
- Controlla che le informazioni contenute nella credenziale soddisfino i requisiti di accesso
- Verifica che il numero di serie della credenziale non sia incluso nell'elenco delle revocazioni più aggiornato (CRL)

Autenticazione dell'Utente

- Quando l'utente desidera accedere a un servizio, utilizza la firma di Schnorr per autenticarsi al server
- La firma di Schnorr permette di dimostrare la conoscenza della chiave privata senza rivelarla, aumentando così la sicurezza

Accesso ai Servizi

- Se le credenziali soddisfano i requisiti di accesso imposti dal servizio e non sono state revocate, l'utente ottiene l'accesso al servizio richiesto
- Il server registra l'accesso dell'utente in modo sicuro e trasparente, mantenendo un log degli accessi per future verifiche

2.2.4 Politiche di Revoca e Aggiornamento della Certificate Revocation List (CRL)

- Ogni certificato X.509 emesso contiene un numero di serie univoco

- Se un utente sospetta che la sua chiave privata sia stata compromessa o persa, può richiedere alla CA la revoca del certificato corrispondente
- La CA mantiene un database dei numeri di serie dei certificati emessi e revocati
- Quotidianamente, la CA genera una Certificate Revocation List (CRL) contenente i numeri di serie dei certificati revocati e la firma digitale della CA
- La CRL include anche un campo CRL Distribution Point che indica l'URL da cui è possibile ottenere l'ultima versione della CRL
- I server dei servizi verificano la validità delle credenziali confrontando il numero di serie della credenziale con la CRL più aggiornata

2.3 Minimizzazione del Coinvolgimento di Terze Parti Fidate

Per minimizzare il coinvolgimento di terze parti fidate durante gli accessi ai servizi:

- Le credenziali sono emesse una sola volta come documenti X.509 e non richiedono la verifica continua da parte delle autorità di rilascio durante ogni accesso
- I server dei servizi qualificati verificano autonomamente i documenti X.509 delle credenziali utilizzando le informazioni pubbliche rese disponibili dalle autorità di rilascio
- L'utilizzo di firme digitali e connessioni TLS garantisce la sicurezza e l'integrità delle comunicazioni

2.4 Protezione della Privacy e Integrità delle Credenziali

Per proteggere la privacy degli utenti e l'integrità delle credenziali:

- Le credenziali sono emesse come documenti X.509 e contengono solo le informazioni strettamente necessarie per l'accesso ai servizi, riducendo l'esposizione di dati personali
- L'identità dell'utente non è rivelata al server del servizio qualificato attraverso i documenti X.509 delle credenziali, a meno che non sia strettamente necessario
- Le credenziali sono firmate digitalmente dalle autorità di rilascio, garantendo che non possano essere alterate o falsificate

2.5 Conclusione

La soluzione proposta mira a raggiungere un compromesso tra efficienza, trasparenza, confidenzialità e sicurezza. Il sistema descrive dettagliatamente le azioni delle parti oneste coinvolte, garantendo che le credenziali siano emesse e verificate in modo sicuro e trasparente. L'uso di certificati X.509 firmati digitalmente dalle autorità di certificazione (CA) assicura che le credenziali siano autentiche e non alterabili. Inoltre, l'adozione della firma di Schnorr per l'autenticazione al server minimizza il coinvolgimento di terze parti fidate durante l'accesso ai servizi, proteggendo la privacy e l'integrità degli utenti. Questa architettura bilancia le esigenze di sicurezza e confidenzialità con la necessità di un sistema efficiente e utilizzabile, riducendo al minimo i rischi associati agli attacchi su larga scala e garantendo un alto livello di affidabilità e trasparenza.

2.6 Proposta di Soluzione

2.6.1 Possibile vulnerabilità

2.6.2 Proposta #2 di Soluzione

2.7 Specifiche degli algoritmi utilizzati

2.7.1 Gen

CAPITOLO 3

WORK PACKAGE 3

CAPITOLO 4

WORK PACKAGE 4