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), contenente un certificato digitale di tipo X.509v3, e il PIN ad essa associato. La CIE ha una chiave segreta di firma, utilizzabile dall'utente durante la fase di richiesta delle credenziali, garantendo così

l'integrità e l'autenticità dei dati forniti alle CA. Il loro obiettivo è richiedere e ottenere le credenziali necessarie dalle autorità, per poi utilizzarle per accedere a servizi specifici in modo sicuro.

1.1.2 Server

I server sono entità che offrono servizi qualificati, accessibili solo ai possessori di specifiche credenziali. Essi 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 delle credenziali (CA) sono enti fidati che emettono credenziali agli utenti, garantendo che queste siano valide e autentiche. 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 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:

- produrre e consegnare la CIE, insieme al suo PIN, all'utente;
- generare e memorizzare in modo sicuro la chiave segreta e il certificato digitale 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 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 alle CA o ai server 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

    * 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 o 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.

- **Identity Thief**
  - **Tipologia:** attivo
  - **Descrizione:** avversario che possiede o mira a rubare identità e/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

    * 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

    * 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 questo tipo di attacchi)
    * 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, spyware 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**
    * Competenze avanzate in crittografia e conoscenza dei protocolli di sicurezza (The Cryptographer)
    * 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, firmando certificati falsi o accedendo ai servizi sfruttando le loro credenziali

1.3.2 Integrità

- **I1:** Preservare l'integrità delle credenziali rilasciate, garantendo che non possano essere alterate o falsificate
- **I2:** I server devono garantire che le credenziali esibite dagli utenti siano verificabili e autentiche, ovvero rilasciate da autorità riconosciute come affidabili
- **I3:** Verificare che la CIE sia riconducibile all'utente che la utilizza
- **I4:** 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 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

- **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

1.4 Completeness

In questo paragrafo verrà definita la completeness, la quale illustra il comportamento del sistema nel caso in cui tutte le parti coinvolte si comportino onestamente.
Nello specifico:

- l'utente possessore della CIE richiede le credenziali necessarie alle autorità di rilascio
- le CA verificano la firma della CIE e l'identità dell'utente e, in caso positivo, emettono le credenziali
- l'utente detentore delle credenziali può quindi richiedere l'accesso ad un servizio specifico, istanziato su un server
- il server sottopone l'utente ad un'autenticazione prima di permettere l'accesso al servizio
- l'utente onesto accede al servizio

CAPITOLO 2

WORK PACKAGE 2

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

- Richiesta e ottenimento, dalle CA, delle credenziali necessarie per l'accesso ai servizi specifici
- Autenticazione e accesso ai servizi qualificati
- Protezione della privacy e dell'integrità delle credenziali

2.1 Panoramica Generale di Funzionamento

Innanzitutto ogni utente possiede una CIE, con al suo interno un certificato X.509v3, ed il PIN ad essa associato. 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. Gli utenti interagiscono con la CA per la richiesta e l'ottenimento delle credenziali, e con il server per usufruire dei servizi offerti. Si inizierà descrivendo come un utente può richiedere una credenziale all'autorità, chiarendone anche il processo di rilascio. 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 un'alta 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:

- Le istituzioni che si occupano dell'emissione della CIE, con annesso il suo PIN, sono assunte come parte fidata
- Ogni utente dispone inizialmente della propria CIE e del PIN associato
- Il certificato digitale presente nella CIE è di tipo X509v3
- All'interno del certificato sono presenti i dati che sono leggibili su una carta di identità
- Le autorità di rilascio sono fidate ed emettono credenziali corrette
- Gli algoritmi e i protocolli utilizzati sono pubblici, così da avere maggiore trasparenza e dare modo agli utenti di verificarne gli aspetti critici

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)

Richiesta ed Emissione delle Credenziali

- Le comunicazioni tra le CA e gli utenti avvengono tramite canali cifrati con TLS

- L'utente invia il certificato X.509v3 relativo alla sua CIE alla CA, insieme alla richiesta della specifica credenziale
- La CA invia una *challenge* b di bit casuali inviandola all'utente
- L'utente inserisce il PIN della sua CIE e calcola l'hash $h = H(b)$ dei bit ricevuti
  NOTA: $H : \{0,1\}^n \to \{0,1\}^{256}$ è una funzione hash di tipo SHA-256, con dominio illimitato e codominio di dimensioni pari a 256 bit
- Viene inviata una query $Sign_{sk_{CIE}}(PIN, b)$ alla CIE
- La CIE verifica il PIN e, se corretto, rilascia una firma σ_{CIE} ECDSA del messaggio (la *challenge*) b.
- L'utente, infine, invia la firma σ_{CIE} all'autorità
- La CA verifica l'identità dell'utente e, se valida, emette una credenziale firmata digitalmente, sotto forma di certificato X.509v3, contenente le informazioni specifiche richieste dal soggetto

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 utilizzata per firmare il documento X.509, corrispondente alla chiave pubblica inclusa nello stesso. Anche in questo caso, le comunicazioni tra utenti e server sono protette da canali cifrati tramite TLS.

Autenticazione dell'Utente

Quando l'utente desidera accedere a un servizio, utilizza lo schema di firma di Schnorr per autenticarsi al server. Nello specifico, l'utente rappresenta il *prover* P, mentre il server il *verifier* V. In questo modo, l'utente dovrà dimostrare al server di essere a conoscenza del segreto (la sk_{utente}, indicata con x) a partire dalla pk_{utente} (indicata con $y = g^x$).
Il protocollo si articola come segue:

- l'utente seleziona un valore casuale $r \in \mathbb{Z}_q$, calcola $a = g^r$ e invia quest'ultimo al server
- il server sceglie una stringa casuale $c \in \mathbb{Z}_q$ e lo invia all'utente
- l'utente invia al server il valore $z = r + cx$, con $z \in \mathbb{Z}_q$

Il server, poiché $g^z = ay^c$, riesce a capire che, a richiedere il servizio, è la persona realmente in possesso delle credenziali.

Verifica delle Credenziali

- Il servizio riceve, dall'utente, la credenziale tramite certificato X.509 e ne verifica la firma digitale
- Verifica, inoltre, che il numero di serie della credenziale non sia incluso nell'elenco delle revocazioni più aggiornato (CRL)
- Controlla che le informazioni contenute nella credenziale soddisfino i requisiti di accesso

Accesso ai Servizi

- Per garantire un accesso sicuro e affidabile ai servizi, è stata implementata una strategia anti-spam basata su puzzle parametrizzati, la quale funge da PoW (Proof of Work)
- Durante il processo di accesso, il server genera un puzzle matematico complesso che richiede l'elaborazione da parte dell'utente per essere risolto. La corretta risoluzione del puzzle costituisce quindi un requisito fondamentale per l'accesso ai servizi qualificati.
- Superato il puzzle parametrico, il client procede con l'autenticazione basata su Schnorr
- Una volta fatto ciò, il server verifica la firma dell'emittente del certificato e se le credenziali sono ancora valide
- 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 Configurazione certificati X.509v3

I certificati adottano la struttura standard, la quale prevede:

- la specifica della versione;
- il numero seriale;
- il tipo di algoritmo di firma e i suoi parametri;
- la CA che ha emesso il certificato;
- il periodo di validità, indicato da una data d'inizio e una di fine;
- il richiedente;
- informazioni sulla chiave pubblica del richiedente, ovvero l'algoritmo utilizzato e la chiave pubblica stessa;
- ID univoco dell'autorità
- ID univoco soggetto

Certificato digitale interno alla CIE

Per questo tipo di certificato sono presenti anche le seguenti estensioni:

- Key Usage: Digital Signature
- Extended Key Usage: Client Authentication

Inoltre, anche i dati anagrafici, presenti sulla CIE, sono incorporati nel documento:

- Comune o Ufficio Consolare emettitore
- Nome
- Cognome
- Luogo di nascita
- Data di nascita
- Sesso
- Statura
- Cittadinanza
- Codice fiscale
- Indirizzo di residenza

Certificato digitale per le credenziali

In questo X.509v3, sono presenti le seguenti estensioni:

- Custom Extension: Credenziale Richiesta dall'Utente
- CRL Distribution Point: URL della lista di revoca dei certificati (CRL)

2.2.5 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
- Periodicamente, 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

2.2.6 PoW: Puzzle Parametrizzato

Quando l'utente cerca di connettersi al server erogatore di un servizio, deve innanzitutto risolvere un puzzle parametrizzato. Per la sua costruzione si è scelto SHA-256, ottenendo Z, un sottoinsieme del codominio della CRHF, composto quindi da stringhe di 256 bit. L'obiettivo è quello di chiedere all'utente di trovare un valore x tale che $H(rand||x) \in \mathbb{Z}$.

2.3 Specifiche degli algoritmi utilizzati

2.3.1 Gen

L'algoritmo $Gen(1^n)$ è utilizzato per generare la coppia di chiavi pubblica e privata. Tramite questo algoritmo si va ad istanziare il problema del logaritmo discreto ($DLog$) ottenendo $\mathbb{G}_q$, q, g come informazioni, dove:

- $\mathbb{G}_q$ è un gruppo ciclico di ordine primo q
- q è il numero di elementi presenti nel gruppo
- g è un generatore del gruppo

A questo punto, è possibile selezionare un certo valore $x \in \mathbb{Z}_q$ e calcolare $y = g^x \bmod q$.
La chiave pubblica, indicata con pk, è:

$$\langle G_q, q, g, y \rangle$$

La chiave privata, indicata con sk, è:

$$\langle G_q, q, g, x \rangle$$

2.3.2 Sign$_{sk}$

$Sign_{sk}(m)$ è un algoritmo di firma digitale, in particolare, si fa riferimento allo schema di firma di Schnorr. Quest'ultimo, prendendo in input un messaggio m ed una chiave privata sk, restituisce una coppia (z, a), rappresentante la firma indicata generalmente con σ, dove:

- a rappresenta un contributo casuale del gruppo, tale che $a = g^r \bmod q$, con $r \in \mathbb{Z}_q$
- $z = r + H(y||a||m)x$, dove $H(\cdot)$ è un *random oracle*, implementato con SHA-256

2.3.3 Verify$_{pk}$

La funzione $Vrfy_{pk}(m, \sigma) : 0, 1$, prendendo in input una chiave pubblica pk, un messaggio m e una firma $\sigma = (z, a)$, verifica che σ sia una firma valida per m, ciò avviene verificando che $g^z \equiv ay^c \bmod q$.

2.4 Protezione della Privacy e Integrità delle Credenziali

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

- L'utilizzo di firme digitali e connessioni TLS garantisce la sicurezza e l'integrità delle comunicazioni
- 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 del protocollo TLS per le comunicazioni e dello schema di firma di Schnorr per l'autenticazione, 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.

CAPITOLO 3

WORK PACKAGE 3

CAPITOLO 4

WORK PACKAGE 4