POLITECNICO DI TORINO

Corso di Laurea in Ingegneria Informatica

Tesi di Laurea Magistrale

Passwordless authentication: Verso un mondo senza password

Relatore
Prof. Riccardo Sisto

Candidato
Adamo Sansone

Tutor Aziendali Liquid Reply Srl
Dr. Pietro Santoro
Dr.ssa Claudia Sergi

Anno Accademico 2022-2023

Sommario

Il rapido sviluppo dell'ecosistema digitale ha intensificato la complessità e la frequenza delle minacce di sicurezza, mettendo in pericolo la riservatezza, l'integrità e la disponibilità delle informazioni online. Per questo, l'inadeguatezza delle password, non garantisce una protezione efficace contro i vari attacchi informatici. Una soluzione di autenticazione più avanzata e sicura è lo standard FIDO2, una tecnologia emergente che promette di rivoluzionare l'autenticazione online, eliminando le password a favore di metodi più sicuri e intuitivi. La transizione al passwordless, tuttavia, presenta sfide significative. Tra queste, spiccano la resistenza al cambiamento da parte degli utenti, abituati ai tradizionali sistemi basati su password, e le difficoltà tecniche legate all'integrazione di una nuova tecnologia in sistemi IAM (Identity and Access Management) esistenti, oltre ai vari costi iniziali. Inoltre, la necessità di garantire una user experience fluida e sicura, senza compromettere la facilità d'uso, rappresenta un ulteriore ostacolo da superare. Per affrontare queste sfide, ho proposto una strategia di implementazione "soft", che prevede un passaggio graduale e consapevole al passwordless, minimizzando l'impatto sui processi utente esistenti e offrendo la possibilità di migrare in un secondo momento, al fine di evitare l'impatto negativo di un cambiamento obbligato e repentino. Questa strategia si è concretizzata nello sviluppo di flussi di autenticazione all'interno del laboratorio PingOne DaVinci: da un lato, un percorso tradizionale basato su password; dall'altro, un percorso innovativo che sfrutta le capacità di FIDO2. Attraverso le simulazioni dei vari scenari di autenticazione, sono state valutate l'efficacia e la correttezza dei nuovi flussi di autenticazione, mettendo in luce un aspetto critico: la dipendenza da un singolo dispositivo di autenticazione con FIDO2. Per risolvere questo problema e migliorare la flessibilità e la robustezza del sistema, è stata integrata la possibilità di aggiungere un secondo dispositivo come misura di Multi-Factor Authentication (MFA), essenziale sia per il recupero dell'account in caso di malfunzionamento che per la perdita del primo dispositivo. I risultati

dimostrano che, nonostante le iniziali sfide legate alla complessità tecnologica e alla resistenza al cambiamento, l'adozione di FIDO2 porta significativi benefici in termini di sicurezza e usabilità.

Indice

Elenco delle figure

Capitolo 1

Introduzione

1.1 Contesto

In un'era segnata dall'accelerazione tecnologica e dall'intensificarsi delle minacce cyber, l'autenticazione assume un ruolo critico nella protezione della sicurezza delle informazioni e delle transazioni online. Il metodo convenzionale basato sulle password, tuttavia, sta mostrando crescenti vulnerabilità sia in termini di sicurezza che di praticità. Le password, infatti, sono spesso esposte a rischi quali phishing, furto e violazioni dei dati, compromettendo la privacy degli utenti e l'integrità delle organizzazioni. La diffusione e l'uso quotidiano di un numero sempre maggiore di servizi e applicazioni online hanno portato gli utenti a dover gestire un'enorme quantità di credenziali, accentuando problemi come il riutilizzo delle password e, di conseguenza, aumentando il rischio di violazioni. Questa situazione sottolinea l'urgente necessità di evolvere verso metodi di autenticazione più sicuri, affidabili ed efficienti, che possano superare i limiti imposti dalle password tradizionali.
In questo scenario, l'emergere del protocollo FIDO2, che pone le basi per un'autenticazione senza l'uso di password, segna un passo avanti decisivo. Tuttavia, l'adozione e l'implementazione di questa tecnologia avanzata comportano sfide significative. Le organizzazioni devono non solo acquisire una conoscenza approfondita del funzionamento di FIDO2, ma anche navigare le complessità legate all'integrazione con le infrastrutture IT esistenti e all'aggiornamento delle politiche di sicurezza.

Questa tesi si immerge nell'indagine dell'autenticazione senza password, prestando particolare attenzione al protocollo FIDO2. Tramite l'implementazioni pratica, sulla piattaforma PingOne DaVinci, un prodotto sviluppato da PingIdentity e che l'azienda Reply utilizza per fornire soluzioni di sicurezza per i suoi clienti, si mira a valutare le capacità di questa tecnologia e a identificare strategie efficaci per affrontare le sfide associate alla transizione da un sistema basato su password. L'analisi copre anche le ripercussioni sull'esperienza dell'utente e l'impatto finanziario sulle organizzazioni, offrendo una panoramica completa delle dinamiche coinvolte nell'integrazione dell'autenticazione senza password nell'attuale panorama della sicurezza informatica.

1.2 Motivazione dello studio

L'impulso principale dietro questa ricerca risiede nella necessità di migliorare la sicurezza informatica e al contempo semplificare l'esperienza utente nell'ambito delle autenticazioni online. Con il continuo aumento delle minacce informatiche e delle violazioni della sicurezza, è imperativo esplorare soluzioni innovative e affidabili per proteggere le identità digitali degli utenti e le informazioni sensibili delle organizzazioni.
Le tradizionali autenticazioni basate su password, spesso soggette a furti e accessi non autorizzati, evidenziano chiaramente i loro limiti. La complessità delle password richieste e la necessità di gestire diverse credenziali contribuiscono al disagio degli utenti, spingendoli al riutilizzo di password e, di conseguenza, aumentando il rischio di compromissione dei dati.
La crescente adozione di servizi online, compresi quelli che gestiscono dati finanziari e personali, ha reso cruciale l'adozione di metodi di autenticazione più robusti e convenienti. In questo contesto, il protocollo FIDO2 si presenta come una soluzione innovativa che promette di rivoluzionare l'approccio all'autenticazione online.
Questa ricerca è motivata dalla volontà di esaminare approfonditamente il protocollo FIDO2 e comprenderne l'implementazione pratica. L'obiettivo è studiare come questa tecnologia possa essere efficacemente integrata nell'ambiente aziendale, mantenendo un equilibrio tra sicurezza e usabilità. Attraverso un approccio basato su prove concrete e sperimentazioni nel laboratorio

PingOne DaVinci, ci proponiamo di scoprire le sfide specifiche e le strategie per implementare con successo l'autenticazione senza password, contribuendo così all'avanzamento delle pratiche di sicurezza informatica.
La ricerca si propone anche di analizzare l'impatto sull'esperienza dell'utente durante la transizione al passwordless e di valutare le implicazioni finanziarie per le organizzazioni. Questo studio mira a fornire alle aziende un quadro completo e basato sull'evidenza per prendere decisioni informate sull'adozione dell'autenticazione senza password, promuovendo così un ambiente online più sicuro e accessibile per gli utenti di tutto il mondo.

1.3 Scopi e Obiettivi

Lo scopo fondamentale di questa ricerca è analizzare il campo dell'autenticazione senza password, tramite l'utilizzo del protocollo FIDO2. Si intende investigare a fondo le capacità e le innovazioni portate da questa tecnologia, analizzarne le sfide implementative e valutare le sue ripercussioni sugli utenti finali e sulle strutture organizzative. L'ambizione è quella di fornire un contributo significativo alla comprensione di come l'autenticazione senza password possa essere adottata efficacemente nel contesto attuale.
Obiettivi specifici:

- **Analisi approfondita di FIDO2**: Approfondire la conoscenza del protocollo FIDO2, esaminando le sue origini, le caratteristiche chiave e le applicazioni pratiche. L'obiettivo è stabilire una solida comprensione delle meccaniche operative di FIDO2 e del suo potenziale nel rafforzare la sicurezza online;
- **Implementazione su PingOne DaVinci**: Attraverso la realizzazione di un progetto pilota su DaVinci, questa ricerca mira a sperimentare l'applicazione del protocollo FIDO2 in un contesto pratico. Tale sforzo permetterà di osservare direttamente le dinamiche e i vantaggi dell'autenticazione senza password;
- **Analisi delle Sfide di Implementazione**: Identificare e analizzare le sfide specifiche legate all'integrazione di FIDO2 con le infrastrutture esistenti, comprendendo le modifiche necessarie e valutando l'impatto sul sistema di gestione delle identità e degli accessi (IAM);

- **Valutazione dell'Esperienza Utente durante la Transizione al Passwordless**: Valutare l'impatto dell'autenticazione senza password sull'esperienza dell'utente. Questo obiettivo mira a comprendere le reazioni, le sfide e le aspettative degli utenti durante la migrazione;
- **Analisi dell'Impatto Finanziario**: Analizzare le implicazioni finanziarie dell'adozione dell'autenticazione senza password sulle organizzazioni. Questo include la valutazione dei costi iniziali, dei benefici a lungo termine e dei potenziali risparmi legati alla gestione delle password;
- **Proporre Strategie di Transizione**: Sviluppare strategie pratiche per facilitare la transizione verso l'autenticazione senza password, compresi approcci soft che minimizzano l'impatto sugli utenti e sull'organizzazione.

Capitolo 2

Fondamenti Teorici

2.1 Autenticazione

Ogni giorno utilizziamo un numero considerevole di servizi web, la maggior parte dei quali richiede ai propri utenti di avviare processi di autenticazione per validarne l'identità. Ci sono diverse definizioni di autenticazione:

- **RFC-4949 (Glossario di sicurezza Internet)**:*"il processo di verifica di una affermazione che un'entità di sistema o una risorsa di sistema ha un certo valore attributo."* [1].

- **NIST IR 7298 (Glossario dei principali termini di sicurezza dell'informazione)** : *"verificare l'identità di un utente, processo o dispositivo, spesso come prerequisito per consentire l'accesso alle risorse in un sistema informativo."* [2].

2.1.1 Fattori di Autenticazione

Un importante punto comune di queste due definizioni è che, quando parliamo del processo di autenticazione, definiamo l'autenticazione di un attore, il che potrebbe non essere solo un essere umano (che interagisce tramite software in esecuzione su hardware), ma anche un componente software o un elemento hardware (che interagisce tramite software).

Fondamentalmente esistono i seguenti tre fattori di autenticazione, che possono essere usati nei processi di verifica dell'identità di un utente per accedere a un servizio:

- **Conoscenza**: L'autenticazione si basa su qualcosa che l'utente conosce, ad esempio una passphrase statica, un codice, un numero di identificazione personale. Il rischio associato è nello storage, nel modo in cui è possibile dimostrare quella conoscenza e nel modo in cui viene trasmessa.

- **Possesso**: L'autenticazione si basa su qualcosa che solo l'utente possiede (spesso chiamato "autenticatore"), ad esempio un token, una smart card, uno smartphone. I rischi associati possono essere nell'autenticatore stesso: può essere infettato da malware, o può essere rubato, clonato o utilizzato senza l'autorizzazione del proprietario.

- **Inerenza**: Qualcosa che l'utente è, ad esempio una caratteristica biometrica (come un'impronta digitale). I rischi associati possono essere nella falsificazione e nella privacy: è molto peggiore rispetto ai casi precedenti, perché ad esempio una caratteristica biometrica non può essere sostituita quando è "compromessa".

2.1.2 Modello di Autenticazione

La combinazione di questi fattori costituisce la base di un processo di autenticazione, ovvero il processo di verifica che "l'utente sia chi dice di essere". Ogni fattore offre un determinato grado di sicurezza, ma ognuno presenta anche i propri problemi e le proprie debolezze. Durante il processo di autenticazione, diversi attori partecipano per garantire un accesso sicuro alle risorse:

- **Utente (o Richiedente)**: L'individuo o il sistema che richiede l'accesso a una risorsa, servizio o sistema. Questo può essere una persona che cerca di accedere a un account online o un'applicazione che richiede l'accesso a un altro servizio.

- **Sistema di Autenticazione (o Verificatore)**: Il componente responsabile della verifica delle credenziali fornite dall'utente contro un insieme

di credenziali conosciute o memorizzate. Questo può essere un server di autenticazione, un modulo software o un servizio cloud dedicato.

- **Database delle Credenziali (o Repository)**: Una base di dati o un archivio che mantiene un record delle informazioni di autenticazione degli utenti, come username, password, chiavi di sicurezza o dati biometrici. Questo database può essere interno al sistema di autenticazione o può essere un servizio esterno.
- **Fornitore di Identità (IdP, Identity Provider)**: Un'entità che crea, mantiene e gestisce le identità degli utenti. In alcuni processi di autenticazione, soprattutto quelli che utilizzano l'autenticazione federata o Single Sign-On (SSO), l'IdP fornisce le credenziali di autenticazione al sistema richiedente.
- **Servizi di Terze Parti**: In alcune implementazioni, servizi di terze parti possono essere coinvolti nel processo di autenticazione per fornire ulteriori livelli di verifica, come l'autenticazione a due fattori (2FA) tramite SMS, email o app dedicate.
- **Sistema o Servizio Protetto**: La risorsa, il servizio o il sistema a cui l'utente sta tentando di accedere. Questo componente è il destinatario finale dell'azione di autenticazione e determina se concedere o negare l'accesso basandosi sull'esito del processo di autenticazione.

Questi attori interagiscono tra loro durante il processo di autenticazione per garantire che solo gli utenti autorizzati possano accedere alle risorse protette.
Lo schema generale è composto da un attore e un RP, *Relying Party*: il primo è disposto a dimostrare la propria identità per costruire una sessione autenticata con il secondo, il quale può soddisfare le richieste dell'attore solo se autenticato. Prima, l'attore e il CSP, *Credential Service Provider*, eseguono un protocollo di registrazione; in questa fase, l'attore è chiamato richiedente. Quando termina con successo, il CSP memorizza gli attributi dell'attore, proprietà indispensabili per verificare la sua identità e li associa a esso. Talvolta, un autenticatore, come un certificato X.509, è fornito al richiedente ottenendo così una prova formale dell'identità: in questo caso, la presenza di un CSP affidabile lega l'autenticatore a quell'utente specifico. Una volta

che le credenziali sono fornite all'attore, esso può eseguire un protocollo di autenticazione con il *Verifier*: questa entità comunica con il CSP chiedendo gli attributi dell'utente. Se la fase di autenticazione è eseguita con un risultato positivo, il richiedente diventa autenticato e il Verifier scambia con l'RP asserzioni di autenticazione che assicurano che abbia proprietà specifiche.

Autenticazione Utente

L'autenticazione utente è un modello di autenticazione in cui un attore, in possesso di un'identità ID e del segreto associato S, desidera essere autenticato su un server, conoscendo l'ID dell'utente e un valore associato ottenibile dal segreto S dell'utente utilizzando la funzione g. Quando l'attore inizia la fase di autenticazione, invia il suo ID al server; di conseguenza, il server chiede una prova. Poi, l'utente invia un valore, risultato di una funzione f che prende come input il segreto S e una volta che questa prova è ricevuta dal server, lo confronta con il valore che ha precedentemente memorizzato come risultato di g(S), talvolta dopo aver eseguito alcuni algoritmi che prendono in ingresso la prova. Se il confronto ha successo, la prova è valida, altrimenti, la prova viene respinta e l'autenticazione non andrà a buon fine (figura 2.1).

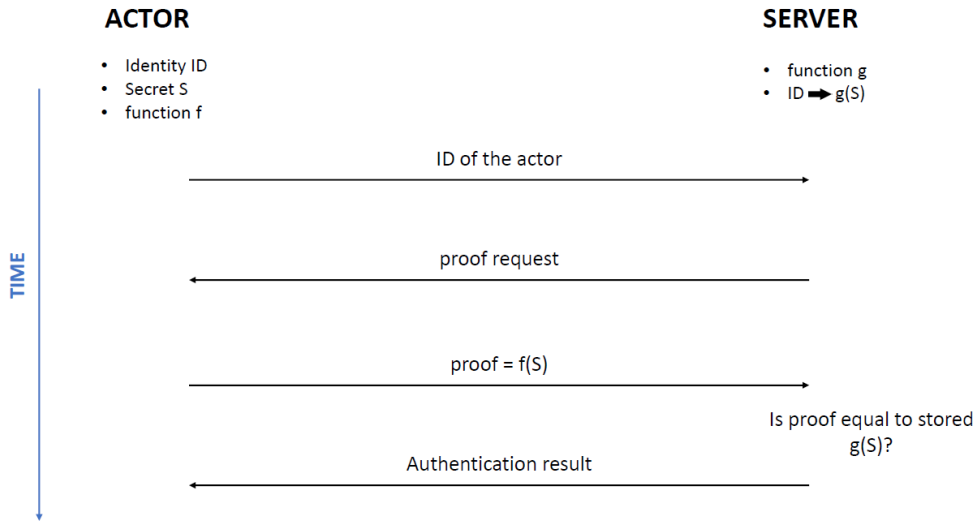

Figura 2.1. Modello autenticazione utente

2.2 Stato Attuale dell'Autenticazione a Due Fattori

L'autenticazione a due fattori (2FA) rappresenta oggi un importante passo avanti nel rafforzamento della sicurezza digitale, offrendo una risposta più robusta alle debolezze intrinseche delle password tradizionali. La crescente adozione di questa metodologia riflette una consapevolezza diffusa riguardo alle limitazioni della semplice autenticazione basata su password e alla necessità di un approccio di sicurezza più complesso in un panorama di minacce informatiche in continua evoluzione. L'implementazione dell'2FA, che integra la conoscenza di qualcosa che l'utente sa (la password) con il possesso di qualcosa che l'utente ha (come un token fisico o un codice OTP generato su smartphone) o con l'identificazione di qualcosa che l'utente è (un tratto biometrico), rappresenta indubbiamente un miglioramento significativo rispetto al modello di autenticazione *single-factor*. Questa combinazione di fattori diversi aumenta la difficoltà per gli attaccanti di ottenere accesso non autorizzato, mitigando alcuni dei rischi associati all'uso esclusivo delle password. Tuttavia, benché l'2FA introduca un livello aggiuntivo di sicurezza, non è esente da criticità. La dipendenza dalla password come primo fattore mantiene viva la problematica legata alla sua potenziale vulnerabilità. Lo sviluppo di attacchi, sempre più sofisticati e avanzati, potrebbero infatti aggirare i meccanismi di sicurezza, bypassando il secondo fattore di autenticazione. Inoltre, l'esperienza utente può risultare appesantita dai passaggi aggiuntivi richiesti per l'autenticazione, che possono rappresentare una frizione nell'accesso ai servizi. Questo aspetto solleva interrogativi sulla ricerca di un equilibrio ottimale tra sicurezza e usabilità.
Le linee guida emesse dal NIST [3], in particolare nella serie SP 800-63, forniscono un'indicazione chiara su come implementare efficacemente l'2FA, delineando i livelli di assicurazione dell'autenticatore (AAL) e sottolineando l'importanza di combinare fattori di autenticazione di diversa natura per garantire la massima protezione. Inoltre, il NIST raccomanda cautela nell'uso di SMS per l'invio di OTP a causa dei rischi associati al SIM swapping, privilegiando dispositivi o applicazioni dedicate alla generazione di codici.
In questo contesto, la ricerca e lo sviluppo di metodologie avanzate di autenticazione acquisiscono un'importanza cruciale. La direzione intrapresa

dall'industria e dalla comunità accademica punta a superare le limitazioni dell'2FA, cercando approcci che possano offrire una sicurezza ancora maggiore senza compromettere l'esperienza dell'utente. Questo impulso verso l'innovazione apre la strada a future soluzioni di autenticazione che, pur non menzionando specifiche tecnologie, promettono di ridefinire il concetto stesso di sicurezza digitale.
In conclusione, mentre l'autenticazione a due fattori segna un progresso decisivo rispetto ai metodi tradizionali, la sua adozione dovrebbe essere vista come un punto di passaggio, non come la destinazione finale. La ricerca di soluzioni più avanzate ed efficaci rappresenta un imperativo nel cammino verso un ecosistema digitale in cui la sicurezza e la facilità d'uso possano coesistere senza compromessi.

2.3 Introduzione allo Standard FIDO2

L'arrivo di FIDO2 [8] segna un punto di svolta nell'evoluzione delle tecnologie di autenticazione, ponendosi come una soluzione promettente contro i limiti delle password tradizionali. Questo standard, noto come "Fast Identity Online," mira a rivoluzionare il modo in cui verifichiamo la nostra identità online, spostando la sicurezza digitale verso un orizzonte senza password.
Al cuore di FIDO2 ci sono due tecnologie chiave: WebAuthn (Web Authentication) e CTAP (Client to Authenticator Protocol). Questi strumenti lavorano insieme per permettere un'autenticazione sicura senza ricorrere alle classiche password, utilizzando invece dispositivi fisici come chiavi di sicurezza USB o metodi biometrici. Il risultato? Un accesso più sicuro e diretto ai servizi online, che riduce sia i rischi legati alla sicurezza che gli ostacoli per gli utenti. Questo avanzamento tecnologico non solo migliora la sicurezza delle transazioni online ma offre anche una maggiore comodità. L'utente può, infatti, autenticarsi rapidamente senza dover memorizzare e digitare complesse combinazioni di caratteri, che spesso costituiscono un punto debole in termini di sicurezza informatica. Inoltre, l'implementazione di FIDO2 permette di affrontare direttamente problematiche come il phishing e gli attacchi di forza bruta, poiché l'autenticazione diventa intrinsecamente legata a un dispositivo specifico o a un attributo biometrico univoco dell'utente.

Nei prossimi capitoli, approfondiremo le origini e lo sviluppo di FIDO2, esplorando come questo standard stia influenzando il panorama dell'autenticazione digitale. Analizzeremo le caratteristiche tecniche di WebAuthn e CTAP, evidenziando come contribuiscano a creare un'infrastruttura di autenticazione più robusta e user-friendly. Esamineremo inoltre le sfide e le opportunità che FIDO2 presenta per le organizzazioni che cercano di adottarlo, così come il suo impatto potenziale sull'esperienza utente e sulla sicurezza generale nell'ambito digitale. Attraverso questo approccio innovativo, FIDO2 si propone di definire il futuro dell'autenticazione online, promuovendo un ambiente digitale dove la sicurezza e la facilità di accesso vanno di pari passo, marcando un netto distacco dalle tradizionali metodologie basate sulle password e orientandosi verso una visione più sicura e accessibile del web.

Capitolo 3

Autenticatori

Dopo aver esplorato i fondamenti teorici dell'autenticazione e le sue diverse forme nel contesto della sicurezza informatica, è cruciale comprendere come, in pratica, l'autenticazione venga realizzata attraverso l'uso di specifici strumenti e meccanismi, noti come autenticatori. Questi dispositivi o metodi fungono da chiave per accedere al mondo digitale in modo sicuro, rappresentando i pilastri su cui si basa l'efficacia del processo di autenticazione stesso. In questo capitolo, ci addentreremo nel dettaglio degli autenticatori, esaminando come ciascuno contribuisca a rafforzare la sicurezza e facilitare l'accesso per gli utenti.

3.1 Panorama degli Autenticatori: Diversità e Innovazione

La crescente complessità delle minacce informatiche ha reso indispensabile l'evoluzione dei metodi di autenticazione, portando alla nascita e allo sviluppo di autenticatori sempre più avanzati e diversificati, ciascuno con il proprio unico meccanismo di protezione, offrendo agli utenti diverse strade per salvaguardare la propria identità digitale. Questo sottocapitolo esplora l'ampio spettro degli autenticatori disponibili, evidenziando come ciascuno contribuisca a un ambiente digitale più sicuro e accessibile.

Password

Nonostante siano percepite come meno sicure rispetto ad altri metodi, le password e le frasi segrete continuano a rappresentare la prima linea di difesa in molti sistemi di autenticazione. La tendenza moderna vede un incremento nell'uso delle frasi segrete: combinazioni più lunghe e complesse di parole che formano una frase facilmente memorizzabile per l'utente ma difficile da decifrare per gli attaccanti. Questo approccio mira a bilanciare sicurezza e usabilità, incoraggiando gli utenti a creare credenziali uniche e robuste per ogni servizio.

Token Hardware

I token hardware, come le chiavi di sicurezza USB, rappresentano un metodo di autenticazione basato sul possesso. Questi dispositivi generano codici di sicurezza univoci o funzionano come supporti fisici per l'autenticazione, collegandosi direttamente al dispositivo dell'utente. La forza di questo metodo risiede nella difficoltà di essere intercettati o duplicati, offrendo un livello aggiuntivo di protezione particolarmente efficace per l'autenticazione multifattoriale. Utilizzano algoritmi come TOTP (Time-Based One-Time Password) o HOTP (HMAC-Based One-Time Password) per generare codici che cambiano periodicamente.

Smart Card

Le smart card, simili ai token hardware, sono carte dotate di un microchip che memorizza le credenziali di autenticazione dell'utente. Utilizzate spesso in contesti aziendali o governativi, richiedono un lettore di carte per l'accesso, combinando il possesso fisico della carta con la conoscenza di un PIN, per una sicurezza rafforzata. La comunicazione tra la smart card e il lettore avviene tramite protocolli crittografici, assicurando l'autenticità delle credenziali.

Autenticazione Biometrica

L'autenticazione biometrica utilizza caratteristiche fisiche uniche dell'individuo("ciò che sei"), come impronte digitali, riconoscimento facciale o scansione

dell'iride, per verificare l'identità. Questo tipo di autenticazione è notevolmente sicuro, data l'unicità dei tratti biometrici, e offre una comodità significativa eliminando la necessità di ricordare password o portare dispositivi addizionali.

Autenticatori Mobile

Gli autenticatori mobile, come app di generazione OTP o notifiche push, sfruttano i dispositivi mobili degli utenti come strumento di autenticazione. Questi metodi combinano la comodità di avere un dispositivo sempre a portata di mano con la sicurezza di codici che cambiano frequentemente o richieste di autenticazione in tempo reale.

Ogni autenticatore offre un mix unico di sicurezza e praticità, con la scelta del metodo più adatto che dipende dalle specifiche esigenze di sicurezza e dal contesto di utilizzo. L'evoluzione continua degli autenticatori testimonia l'impegno del settore della sicurezza informatica nel cercare soluzioni innovative per proteggere le identità digitali in un mondo sempre più connesso.

3.2 La Password: Pilastro e Punto di Fragilità

La password è *"Una stringa di caratteri (lettere, numeri e altri simboli) utilizzata per autenticare un'identità o per verificare l'autorizzazione all'accesso."* [4].

Essa è stata a lungo considerata e lo è tuttora la base dell'autenticazione digitale, un semplice ma potente strumento per proteggere l'accesso a dati e servizi online. Tuttavia, nel corso degli anni, le vulnerabilità intrinseche delle password e le sfide legate alla loro gestione hanno evidenziato significativi punti di fragilità.

3.2.1 Modelli di autenticazione basati su password e vulnerabilità

Nel modello di autenticazione basato su password vi è il segreto S, che come già detto già in precedenza è una sequenza di cifre, che viene inviato dall'utente al server in chiaro tramite la funzione identità I(x) = x.

Dal lato del server, S può essere memorizzato in chiaro, utilizzando nuovamente la funzione identità I come funzione di memorizzazione g e una volta che la prova arriva al server, lo confronta con quello memorizzato.(figura 3.1).

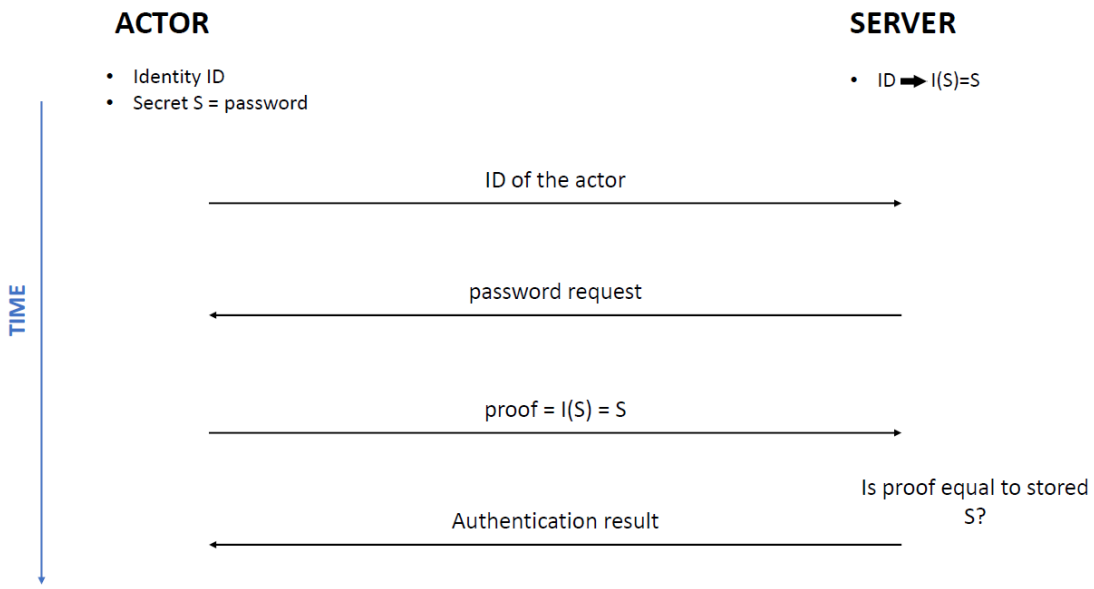

Figura 3.1. Modello di autenticazione basata su password

Sebbene sia semplice e intuitiva, questa tecnica di memorizzazione è insicura e offre vulnerabilità che possono essere sfruttate dai criminali, un hacker malintenzionato può accedere al database e vedere facilmente il segreto. Per fronteggiare questa vulnerabilità, il server può memorizzare le informazioni relative alla password come risultato di una funzione hash che prende S come input, consentendo così una protezione più forte dagli accessi malevoli al database. Anche se il valore viene divulgato, sarebbe impraticabile invertire la funzione hash estraendo così il segreto. In questo caso, quando la prova è

ricevuta dal server, prima applica la funzione hash sul valore ricevuto e poi confronta il risultato con quello memorizzato (figura 3.2).

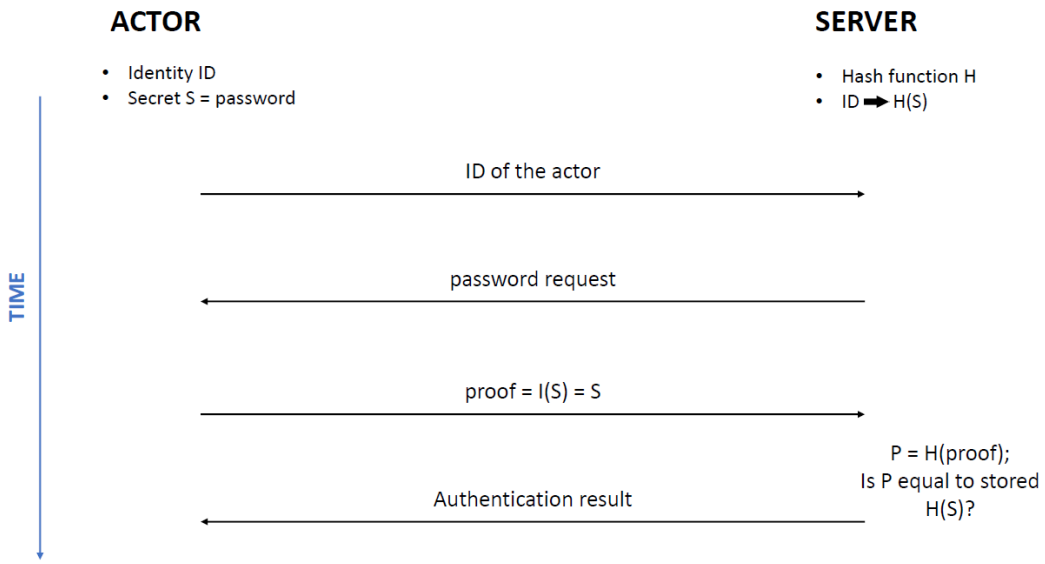

Figura 3.2. Modello di autenticazione basata su password con l'uso di una funzione di hash sul lato server

Anche se il sistema è ora più sicuro di prima, il server può ancora essere vittima di hacker che eseguono dictionary attacks, utilizzando ad esempio le rainbow tables. Il nucleo di questo tipo di attacchi è il pre-calcolo: l'attaccante esegue la nota funzione hash su password prevedibili costruendo così una tabella che le collega ai loro digest associati. Una volta costruita la tabella, l'attaccante può confrontare questi valori digest con quelli presenti nel database attaccato: se trova valori uguali, allora le password associate sono quelle effettivamente utilizzate. L'esistenza di questo tipo di attacchi rende di nuovo vulnerabile il server e per evitare questa minaccia, quest'ultimo dovrebbe utilizzare un salt, una sequenza di cifre casuali, prima della funzione di cifratura. Quindi, la password viene prima concatenata a questo salt e poi inserita come input dell'algoritmo hash (figura 3.3). Così facendo, il dictionary attack non può essere eseguito.

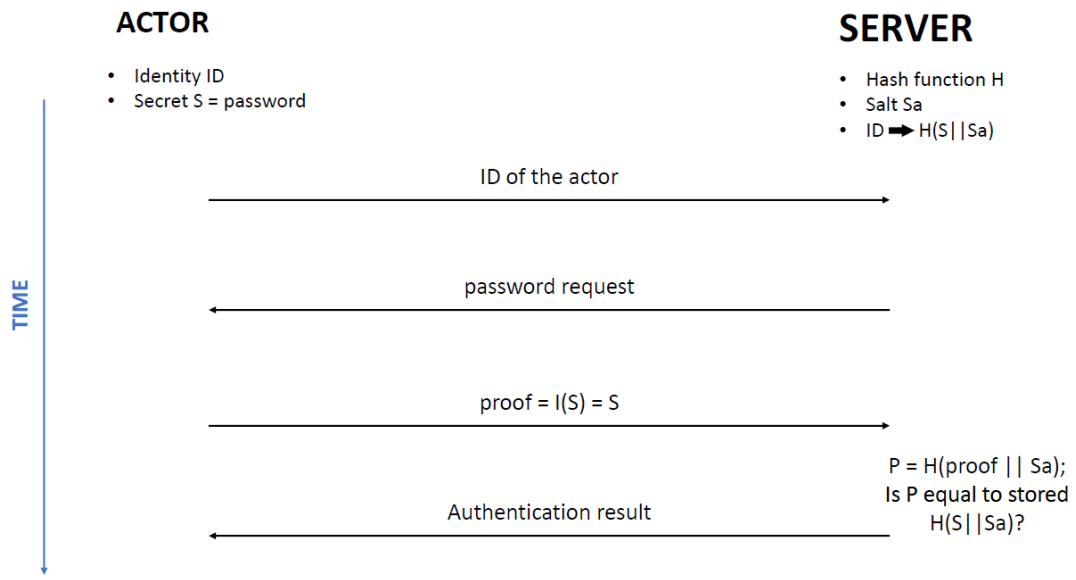

Figura 3.3. Modello di autenticazione basata su password con l'uso di una funzione di hash e un salt sul lato server

Sebbene un problema sia risolto, l'autenticazione basata su password continua a presentare numerose debolezze. Inizialmente, è fondamentale riconoscere che la gestione della password non si limita al solo ambiente server: la sua conservazione lato utente richiede elevati standard di sicurezza per prevenire accessi non autorizzati. In aggiunta, il trasferimento della password senza opportune misure di cifratura espone a rischi elevati, aprendo la porta a potenziali intercettazioni da parte di hacker. Questi, sfruttando canali di trasmissione non protetti, possono ottenere accesso diretto alle credenziali segrete o, attraverso la creazione di server fraudolenti, attuare attacchi *Man In The Middle* (MITM), intercettando le comunicazioni tra l'utente e il server legittimo.
La semplicità delle password, inoltre, le rende vulnerabili ad attacchi di tipo *brute force*, nei quali gli aggressori utilizzano software avanzati per generare e testare una vasta gamma di combinazioni nella speranza di indovinare la corretta sequenza. Questa strategia è particolarmente efficace contro password deboli o di comune utilizzo.

Un altro grave rischio è rappresentato dai leak di dati, situazioni in cui grandi quantità di credenziali utente vengono esposte a seguito di violazioni dei sistemi di sicurezza delle aziende. Questi eventi non solo mettono a nudo le password degli utenti ma forniscono anche ai criminali informatici il materiale per orchestrate attacchi di credential stuffing. In questi attacchi, le credenziali rubate vengono utilizzate per tentare l'accesso a una varietà di servizi online, sfruttando la comune pratica di riutilizzo delle password da parte degli utenti. Nella figura 3.4 sono presenti statitische ricavati da vari articoli [5] [6] [7].

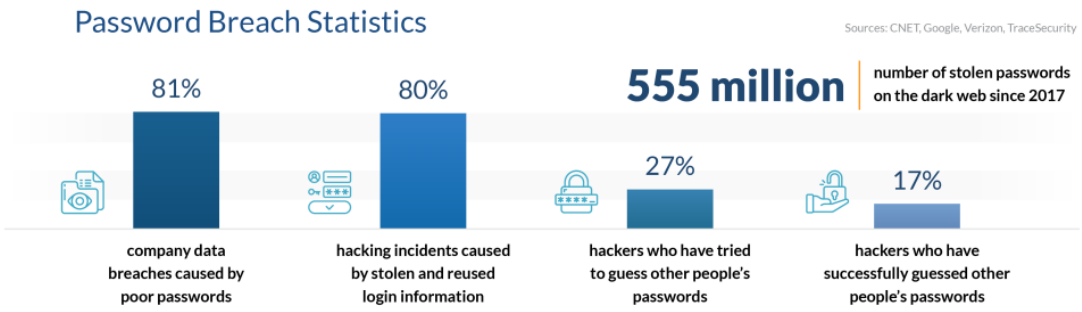

Figura 3.4. Statistiche sulle violazioni delle password

3.2.2 Gli Ulteriori Svantaggi delle Password

Come discusso nel sottocapitolo precedente questo meccanismo è lontano dall'essere inattaccabile, esponendo sistemi e utenti a una varietà di rischi. Benché le vulnerabilità intrinseche delle password rappresentino una sfida significativa, ci sono ulteriori dimensioni del problema che meritano attenzione.

Problemi di Usabilità

- **Sovraccarico di Memoria**: Gli utenti spesso faticano a ricordare password complesse e uniche per ogni servizio che utilizzano, portando a pratiche insicure come l'uso della stessa password per più account o la scelta di password semplici e facilmente indovinabili;

- **Gestione delle Password**: La necessità di gestire un grande numero di password diverse può essere onerosa senza l'ausilio di gestori di password, che tuttavia introducono un ulteriore livello di complessità e potenziali rischi di sicurezza;

Vincoli e Limitazioni

- **Politiche di Creazione Password**: Molti sistemi impongono politiche di creazione password che richiedono una certa lunghezza e complessità, spesso risultando in password difficili da ricordare per gli utenti;
- **Reset e Recupero Password**: I processi di reset o recupero delle password possono essere sia un punto di vulnerabilità che una fonte di frustrazione per l'utente, specialmente se le procedure sono eccessivamente complicate o non sufficientemente sicure;

Politiche di Sicurezza Insufficienti

- **Mancanza di Verifica a Due Fattori**: Assenza di una sicurezza aggiuntiva oltre alla password;
- **Assenza di Cambiamenti Periodici**: Assenza di politiche che richiedono la modifica regolare delle password.

Nonostante la loro ubiquità, le password rappresentano un punto di fragilità nell'ecosistema della sicurezza digitale, esponendo gli utenti a una varietà di rischi e complicazioni. La crescente consapevolezza di queste vulnerabilità ha spinto verso lo sviluppo e l'adozione di metodi di autenticazione alternativi, come l'autenticazione a due fattori (2FA), l'autenticazione biometrica e le soluzioni basate sul protocollo FIDO, che offrono un equilibrio migliore tra sicurezza e usabilità. Nel frattempo, la gestione prudente delle password, l'uso di gestori di password affidabili e la sensibilizzazione degli utenti rimangono strumenti essenziali nella lotta contro le minacce informatiche.

Capitolo 4

FIDO2 Standard

4.1 Origini e Sviluppo del Protocollo FIDO2

Il protocollo FIDO2 rappresenta un'evoluzione cruciale nel campo dell'autenticazione online, unendo gli sforzi e le innovazioni tecnologiche di diversi anni per offrire una soluzione che mira a superare le problematiche legate all'uso delle password. La sua storia è segnata da momenti chiave e collaborazioni strategiche che hanno plasmato il suo sviluppo e la sua adozione a livello globale.

La nascita del protocollo FIDO2 trova le sue radici nell'impegno congiunto della FIDO Alliance [9] e del World Wide Web Consortium (W3C) [10]. La FIDO Alliance, fondata nel luglio 2012 da leader tecnologici come PayPal e Lenovo, ha iniziato il suo cammino con l'obiettivo di rivoluzionare l'autenticazione online, promuovendo soluzioni più sicure e meno dipendenti dalle tradizionali password. Il lancio delle specifiche FIDO 1.0 nel febbraio 2014 e l'introduzione di FIDO U2F nel dicembre dello stesso anno hanno segnato i primi passi verso questo obiettivo, offrendo un metodo di autenticazione a due fattori basato su dispositivi fisici.

Un punto di svolta significativo si è verificato nel 2019 con l'ufficializzazione di WebAuthn come standard web dal W3C. Questa mossa ha permesso di integrare direttamente le funzionalità di autenticazione sicura nei browser web, facilitando l'adozione della tecnologia passwordless su una scala più ampia. La collaborazione tra la FIDO Alliance e il W3C ha garantito che FIDO2 fosse non solo tecnicamente avanzato ma anche ampiamente accessibile.

Il nuovo protocollo si distacca dalle soluzioni precedenti introducendo un'architettura basata su crittografia a chiave pubblica, che elimina la necessità di memorizzare o trasmettere password. Questa innovazione non solo rafforza la sicurezza ma semplifica anche l'esperienza dell'utente, consentendo l'autenticazione tramite smartphone, token hardware e tecnologie biometriche. La resistenza ai comuni attacchi informatici, come il phishing, è un altro valore aggiunto di FIDO2, che indirizza efficacemente le vulnerabilità associate ai metodi di autenticazione tradizionali.
Il suo impatto sul futuro dell'autenticazione è incontestabile. La sua adozione da parte di giganti tecnologici e la sua implementazione in un'ampia varietà di piattaforme e dispositivi sottolineano il suo ruolo come standard de facto per un'autenticazione sicura e senza password. L'ampia adozione di WebAuthn, sostenuta dal supporto nei principali browser e sistemi operativi (figura 4.1), ha reso l'autenticazione senza password una realtà pratica per milioni di utenti, segnando un passo significativo verso un internet più sicuro e accessibile.
Il viaggio di FIDO2, dalle sue origini all'ampia adozione, illustra un percorso di innovazione continua e collaborazione strategica. Con la promessa di un futuro senza password, esso non solo migliora la sicurezza online ma anche l'usabilità, offrendo agli utenti un'esperienza di autenticazione senza precedenti. Il suo sviluppo e la sua implementazione rappresentano un capitolo fondamentale nella storia della sicurezza informatica, con implicazioni durature per l'evoluzione delle pratiche di autenticazione nel mondo digitale.

Figura 4.1. Tecnologie che supportano WebAuthn

4.2 Caratteristiche Chiave

Il protocollo FIDO2 si distingue nel panorama dell'autenticazione digitale per le sue caratteristiche innovative che rispondono alla crescente domanda di soluzioni di sicurezza più robuste e user-friendly. Queste caratteristiche chiave lo definiscono come uno standard all'avanguardia per l'autenticazione online.

- **WebAuthn (Web Authentication)**: Una delle colonne portanti di FIDO2, WebAuthn, permette agli utenti di effettuare l'autenticazione tramite browser in maniera sicura e senza password. Questa API JavaScript facilita l'uso di metodi di autenticazione biometrica, token hardware e PIN, creando un'esperienza di accesso fluida e altamente sicura;

- **CTAP (Client to Authenticator Protocol)**: CTAP è l'elemento che consente la comunicazione tra il dispositivo dell'utente e l'autenticatore esterno. Questo protocollo è fondamentale per l'integrazione di dispositivi esterni nell'ecosistema FIDO2, permettendo un'autenticazione senza password anche su dispositivi che non supportano nativamente WebAuthn;

- **Crittografia a Chiave Pubblica**: FIDO2 si basa sulla crittografia asimmetrica per l'autenticazione. Durante la registrazione con un servizio, viene generata una coppia di chiavi (pubblica e privata) unica per quell'interazione. La chiave privata è memorizzata in modo sicuro sul dispositivo dell'utente, mentre la chiave pubblica è condivisa con il servizio online. Questo meccanismo garantisce che solo il possessore della chiave privata possa autenticarsi, migliorando significativamente la sicurezza rispetto alle password tradizionali;

- **Resistenza ai Comuni Attacchi Informatici**: Grazie alla sua architettura, FIDO2 offre una protezione robusta contro vari attacchi informatici, inclusi phishing, man-in-the-middle e attacchi replay. Questo è possibile perché l'autenticazione si basa su una sfida crittografica unica per ogni sessione, che non può essere riutilizzata da un attaccante;

4.3 Protocolli

FIDO consente agli utenti di registrarsi, autenticarsi e autorizzare e confermare operazioni. Gli attori dei protocolli utilizzati sono:

- Utente finale;
- Dispositivo dell'utente, diviso in:
  - Autenticatore FIDO, gestisce e controlla le chiavi asimmetriche dell'utente;
  - FIDO Client, la parte del meccanismo FIDO che opera sul lato utente;
  - User Agent, la parte client dell'applicazione web che può essere un'applicazione o un programma, spesso eseguito in un browser.
- Relying Party, diviso anch'esso a sua volta in:
  - Applicazione Web, la parte server dell'applicazione web;
  - FIDO Server, la parte del meccanismo FIDO che opera sul lato server.

4.3.1 Registrazione

Per registrarsi a un servizio che richiede autenticazione FIDO, è necessario seguire un processo specifico illustrato nella figura 4.2. La comunicazione avviene tramite un canale HTTPS, che utilizza il protocollo crittografico TLS, con il fine di fornire autenticazione, integrità dei dati e confidenzialità. Inizialmente, l'utente, tramite il proprio browser o app (1), invia una richiesta di registrazione all'applicazione web interessata. Quest'applicazione, a sua volta, passa la richiesta al server FIDO (2). La richiesta iniziale da parte dell'utente include solitamente dati basilari come il nome, cognome, nome utente e come si preferisce essere chiamati nell'interfaccia utente. Dopo aver ricevuto questa richiesta, il server FIDO elabora una nuova richiesta di registrazione e la invia indietro al dispositivo dell'utente, specificando certe "regole del gioco", come i tipi di chiavi e gli algoritmi che accetta (2). Ricevendo questa informazione, il dispositivo dell'utente, sotto la guida del client

FIDO e tramite l'interazione con l'autenticatore (un dispositivo o software per la gestione delle credenziali di sicurezza), inizia il processo vero e proprio di creazione dell'identità digitale dell'utente presso il servizio. Al termine, l'utente avrà un set di chiavi crittografiche nuove, uniche per quel servizio, memorizzate sull'autenticatore (3). Con le chiavi create, viene generata un'attestazione di registrazione che, assieme alla chiave pubblica, viene inviata al server FIDO come parte della risposta di registrazione (4). Quest'ultima contiene la firma digitale che autentica l'attestatore, ovvero il dispositivo del cliente, garantendo che sia legittimo e autorizzato a registrarsi, metadata e quindi informazioni aggiuntive sul dispositivo del cliente, come ad esempio il modello, il tipo di autenticatore utilizzato e altre caratteristiche rilevanti. A questo punto, il server ha tutto ciò che gli serve per controllare se tutto è stato fatto secondo le regole stabilite e, se l'attestazione è valida, procede a salvare la chiave pubblica dell'utente (5).

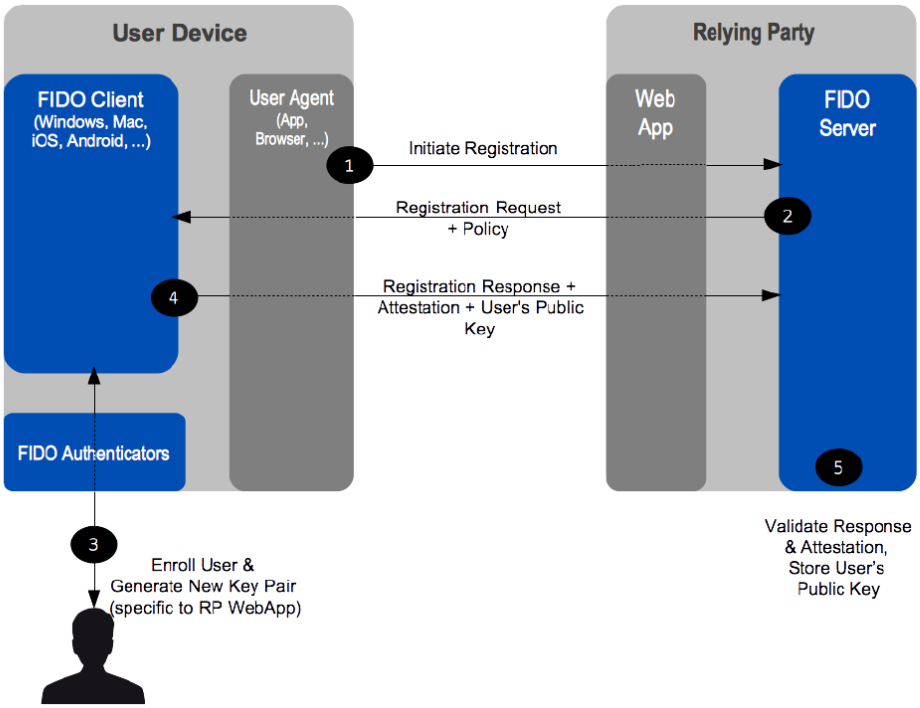

Figura 4.2. Meccanismo di registrazione

Questo è quello che succede dietro le quinte, lontano dagli occhi degli utenti. Ma FIDO, come abbiamo già più volte ribadito, si distingue, oltre che per l'efficacia, per la sua facilità d'uso.
Poniamo il caso che un utente scelga di utilizzare il proprio smartphone come dispositivo di autenticazione (figura 4.3). Se quest'ultimo intende utilizzare un servizio che implementa il sistema FIDO, deve inizialmente procedere con la registrazione di una coppia di chiavi unica per quell'entità specifica. Per completare questa fase di iscrizione, l'utente deve connettersi con l'entità presso la quale vuole registrarsi, confermando la sua registrazione, ad esempio, tramite un elemento biometrico, come l'impronta digitale. Dopo che il suo smartphone ha confermato l'autenticità dell'utente, il sistema procede alla creazione di una nuova coppia di chiavi, conservando quella privata direttamente sul dispositivo mobile dell'utente e depositando la chiave pubblica nel database del server di FIDO.

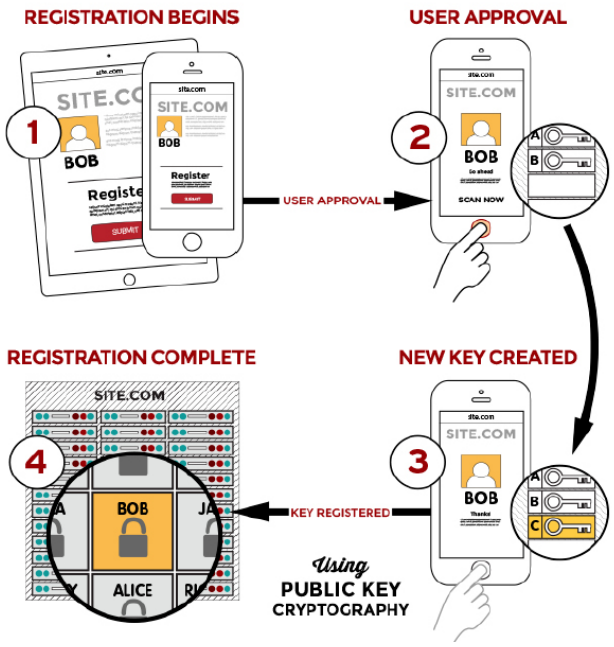

Figura 4.3. Meccanismo di registrazione dal punto di vista dell'utente

4.3.2 Autenticazione

Dopo essersi registrato l'utente ha la possibilità di autenticarsi, accedendo così a varie risorse e servizi forniti dall'RP, effettuando il login (come illustrato nella figura 4.4). Il processo inizia quando l'utente, tramite il proprio browser o applicazione (User Agent), invia una semplice richiesta di autenticazione, che include solitamente solo il suo nome utente e un codice identificativo(1). Successivamente, il sistema genera e invia al dispositivo dell'utente una richiesta basata su delle politiche prestabilite che specificano le condizioni sotto le quali un'operazione di autenticazione può essere considerata valida. Esse includono requisiti di sicurezza o determinate proprietà che il dispositivo deve avere. In parallelo, viene anche generata una challenge unica, ovvero un valore casuale sul server e utilizzato per confermare l'identità dell'utente e generare una firma digitale unica per la transazione di autenticazione(2). A questo punto, l'utente risponde a questa sfida dimostrando di avere il diritto di accedere, sbloccando la chiave segreta salvata sul proprio dispositivo e legata all'RP. Utilizzando questa chiave privata, viene calcolata una firma digitale come risposta autenticata da inviare indietro al server FIDO nei passi successivi (3 e 4). Infine, il server FIDO verifica l'autenticità della firma confrontandola con la chiave pubblica dell'utente, che era stata salvata sul server durante la fase di registrazione e con la sfida generata precedentemente(5). Questo confronto, se corrisponde, conferma l'identità dell'utente e gli consente l'accesso alle risorse richieste.

Analogamente a quanto avviene per la registrazione, il processo di accesso per l'utente si rivela estremamente intuitivo (figura 4.5). Quando l'utente intende accedere al servizio dell'entità con cui si è precedentemente registrato, si collega a quest'ultima e inizia la procedura di login. Questa viene semplicemente confermata utilizzando l'autenticatore, che può essere o un'impronta digitale o una chiavetta USB. Terminata questa fase di convalida, lo smartphone dell'utente identifica automaticamente la chiave privata corretta, ossia quella associata specificamente a tale entità e la impiega per attivare funzioni asimmetriche necessarie a completare l'accesso. Lo stesso procedimento vale se l'utente vuole autorizzare una qualsiasi operazione.

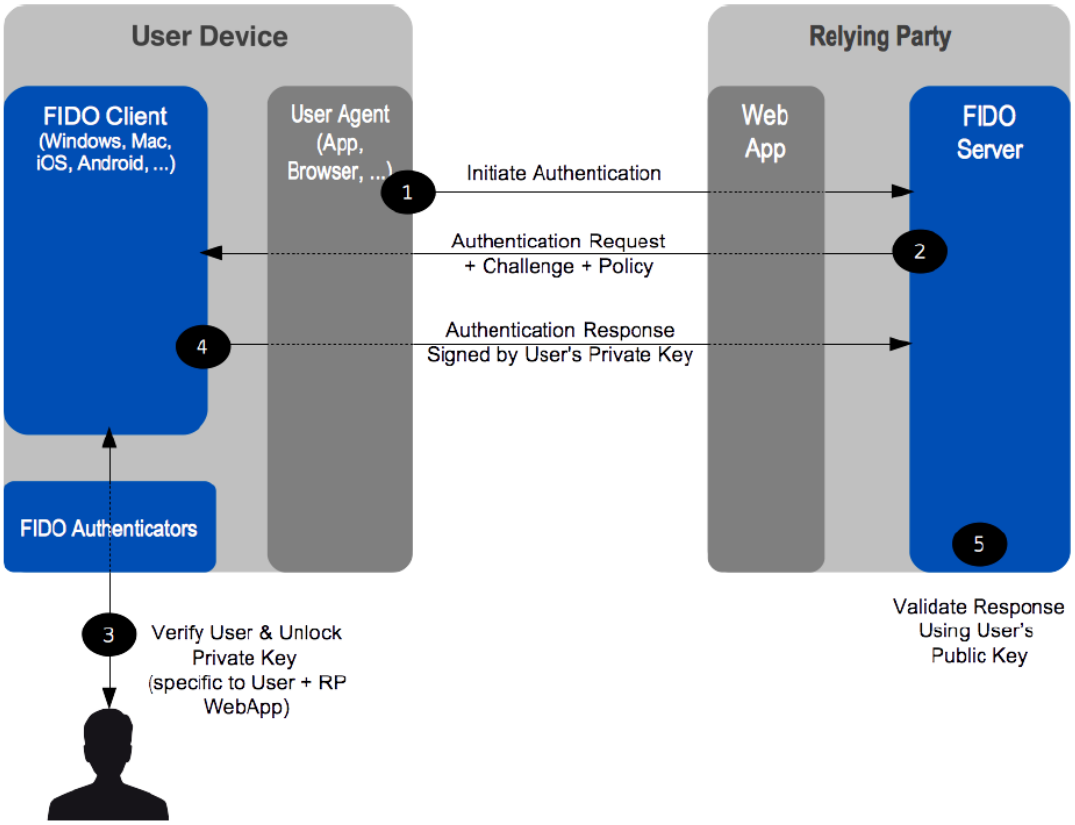

Figura 4.4. Meccanismo di autenticazione

4.4 Applicazioni Pratiche nel Contesto della Passwordless Authentication

L'introduzione di FIDO2 ha aperto nuove possibilità nel campo dell'autenticazione, con applicazioni pratiche che vanno oltre il semplice accesso ai siti web. La sua flessibilità e sicurezza lo rendono ideale per una varietà di contesti.

- **Accesso Aziendale**: Le aziende possono implementare FIDO2 per garantire un accesso sicuro alle reti aziendali e ai dati sensibili. L'uso di autenticatori biometrici o token hardware può semplificare il processo di accesso per i dipendenti mantenendo elevati standard di sicurezza;

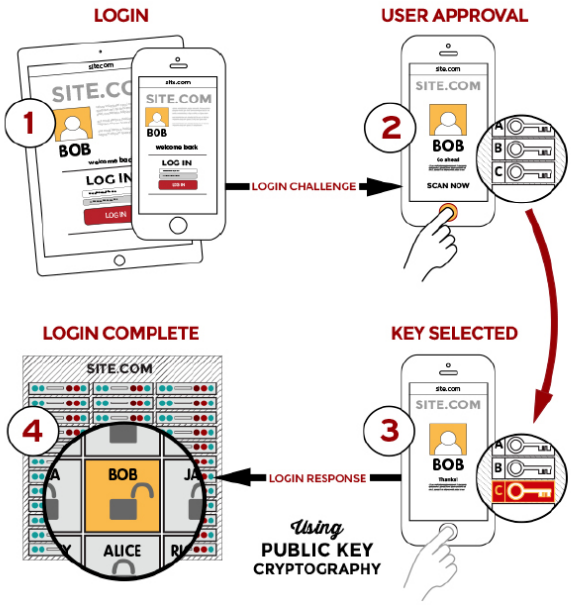

Figura 4.5. Meccanismo di autenticazione dal punto di vista dell'utente

- **Servizi Bancari e Finanziari**: Il settore bancario e finanziario beneficia enormemente di FIDO2, utilizzandolo per proteggere le transazioni e l'accesso ai conti online. L'autenticazione biometrica e i token hardware offrono un livello di sicurezza superiore per le operazioni finanziarie, riducendo il rischio di frodi;
- **E-commerce**: I siti di e-commerce possono utilizzare FIDO2 per semplificare il processo di checkout, migliorando l'esperienza dell'utente. L'autenticazione senza password riduce gli ostacoli all'acquisto, potenzialmente aumentando il numero di transazioni concluse e rafforzando la fiducia del cliente;
- **Governo e Servizi Pubblici**: L'adozione di FIDO2 da parte delle agenzie governative facilita l'accesso dei cittadini ai servizi online, migliorando l'efficienza e la sicurezza. L'autenticazione senza password può semplificare le procedure per ottenere documenti, accedere a informazioni sanitarie e partecipare a servizi pubblici.

In conclusione, FIDO2 rappresenta un passo significativo verso un futuro

senza password, in cui l'autenticazione è sia sicura che intuitiva. Le sue applicazioni pratiche dimostrano il potenziale di questa tecnologia di cambiare il modo in cui accediamo ai servizi digitali, offrendo una soluzione che è al contempo più sicura per le organizzazioni e più comoda per gli utenti. Con l'ampia adozione di FIDO2, possiamo aspettarci una riduzione delle violazioni dei dati e una maggiore fiducia nell'ecosistema digitale.

Capitolo 5

Implementazione e Configurazione del Laboratorio PingOne DaVinci

PingOne DaVinci è una piattaforma di PingIdentity [11], utilizzata per la creazione di esperienze utente digitali, basata sul low-code. Attraverso un'interfaccia intuitiva di tipo drag-and-drop è stato possibile progettare flussi per la gestione degli accessi e percorsi utente dinamici adattabili a qualsiasi esigenza, dalla registrazione all'autenticazione fino alla gestione di autorizzazioni e verifiche. Inoltre, ha reso possibile testare in tempo reale ciò che si è creato e di integrare i flussi anche in applicazioni esterne.
Secondo Andrey Durand, CEO di Ping Identity, la chiave per distinguersi nel mercato digitale odierno non risiede solo nella sicurezza, ma anche nell'offrire un'esperienza utente fluida e senza interruzioni. PingOne DaVinci si propone proprio di risolvere questa sfida, permettendo agli sviluppatori di creare percorsi utente che non solo sono sicuri, ma anche piacevoli da percorrere.
All'interno della piattaforma, vi è una libreria che include oltre 100 connettori preconfigurati, coprendo una varietà di servizi di identità, IT e automazione.

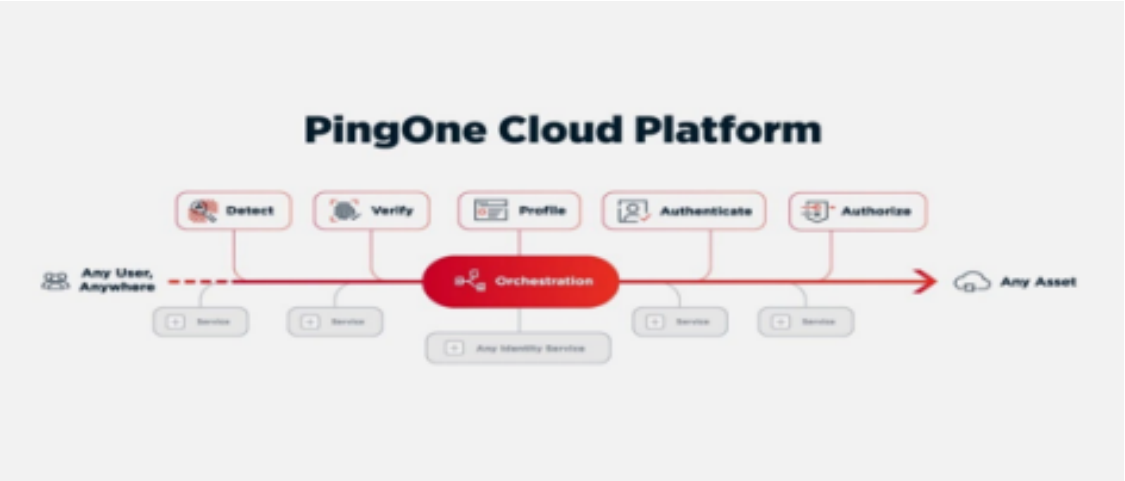

Figura 5.1. Piattaforma Cloud PingOne

5.1 Componenti DaVinci

Al centro di queste operazioni ci sono i flussi. Un flusso è una serie di blocchi interconnessi che consente di creare un'esperienza utente personalizzata secondo necessità. Ci sono diversi blocchi che hanno funzionalità diverse. Ogni blocco o nodo può avere funzionalità puramente grafiche, interazione visiva con l'utente o comunicare qualcosa al backend per indicare quale logica deve essere implementata. I nodi possono anche fare riferimento a servizi esterni, andando così a recuperare informazioni da servizi di terze parti, cambiare il valore di variabili o altri parametri. Questi nodi sono collegati tra loro attraverso operatori logici, che in base all'esito dell'azione eseguita sul nodo precedente, determinano il percorso da seguire all'interno di un flusso.
Pertanto, ci sono 3 componenti fondamentali per la costruzione di un'esperienza utente in DaVinci:

- **Flusso**: Rappresenta un percorso dell'utente che può essere registrazione, autenticazione o autorizzazione. Il flusso è composto da nodi e operatori logici e inizia dal nodo più a sinistra e progredisce verso destra fino a quando non si verifica un errore o si raggiunge la fine del percorso;
- **Nodo**: Rappresenta l'azione di un dato blocco. Questa azione può restituire vero, falso o generare un errore imprevisto. In caso di un

errore imprevisto, il flusso si interrompe;

- **Operatore Logico**: Determina il percorso da seguire dopo l'azione di un nodo, e la decisione si basa sul risultato restituito dal nodo precedente.

Sebbene l'elenco esatto dei connettori(nodi) disponibili possa variare nel tempo, poiché nuovi ne vengono aggiunti e aggiornati regolarmente, ecco alcuni esempi di tipi di connettori disponibili in PingOne DaVinci [12]:

- **HTTP**: Permette la creazione di moduli e pagine HTML personalizzate oppure di effettuare chiamate API REST;
- **PingOne**: Utilizzato per creare e gestire account utente in PingOne, inclusa la reimpostazione delle password e la gestione di gruppi e accordi;
- **PingOne Authentication**: Autentica gli utenti e gestisce le sessioni di autenticazione degli utenti PingOne. Questo connettore è necessario per integrare i flussi in un'applicazione utilizzando i metodi di reindirizzamento;
- **PingOne Credentials**: Utilizza le credenziali PingOne per emettere, verificare e gestire credenziali verificabili digitali;
- **PingOne MFA**: Utilizza PingOne MFA per l'autenticazione a più fattori (MFA) e la registrazione del dispositivo;
- **Variable**: Memorizza gli attributi del flusso e dell'utente come variabili;
- **Device Policy**: Controlla lo user agent, le informazioni sul browser e la versione del sistema operativo;
- **Error Message**: Mostra messaggi di errore personalizzabili;
- **Functions**: Dirama il flusso utilizzando condizioni logiche o in base al risultato del codice JavaScript personalizzato;
- **Flow Analytics**: Registra i dettagli sui risultati del flusso da utilizzare nell'analisi del flusso.

Ed è grazie alla capacità di orchestrare questi elementi che è stato possibile sviluppare i due flussi, quello di registrazione e quello di login, indispensabili per l'accesso ai servizi digitali. Questi flussi, descritti nei dettagli nelle sezioni seguenti, rappresentano esempi concreti di come la tecnologia possa essere impiegata per migliorare l'esperienza utente mantenendo al contempo elevati standard di sicurezza.
Tuttavia, all'interno della piattaforma PingOne DaVinci, la sezione Identities svolge un ruolo centrale, agendo come fulcro per la gestione avanzata dell'identità degli utenti (IAM). Questa componente critica della piattaforma è stata essenziale per l'implementazione efficace e il funzionamento ottimale dei flussi di registrazione e login, offrendo un contesto robusto e versatile per configurare policy, selezionare autenticatori, e gestire i privilegi e i ruoli utente. Grazie alla sua flessibilità è stato possibile personalizzare le policy nella directory service per soddisfare le specifiche esigenze di sicurezza e conformità.
Attraverso le opzioni disponibili, si è resa possibile la scelta degli autenticatori accettabili per ogni flusso, come quella passwordless con autenticatori FIDO2, a fianco di metodi tradizionali.
In sintesi, Identities in PingOne DaVinci si è rivelata una componente imprescindibile nell'architettura dei flussi realizzati, permettendo una gestione dell'identità e dell'accesso (IAM) sia sofisticata che intuitiva, dando la possibilità di personalizzare policy e autenticatori.

5.2 Design del Progetto

Lo scopo del progetto è stato implementare i meccanismi di FIDO2 sulla piattaforma DaVinci. In questo capitolo, saranno mostrati il design e l'implementazione dei sistemi.

5.2.1 Design della Rete

Come detto in precedenza, lo standard FIDO2 ha bisogno di diversi componenti:

- Server FIDO2;
- Applicazione Web lato server;

- Applicazione Web lato client.

Come vedremo in seguito, attraverso la piattaforma, è stato possibile creare un'applicazione web utilizzando i connettori HTTP, gestire le utenze direttamente tramite il database di DaVinci e collegare il server FIDO2 senza la necessità di crearli ex novo. Nella figura 5.2 è raffigurata quella che è la struttura della rete.

Figura 5.2. Design della rete

5.2.2 Configurazione Iniziale

Nel processo di configurazione iniziale per l'implementazione dei flussi di autenticazione, un passaggio cruciale è stata la creazione di una nuova Population(figura 5.3). Questa fase ha permesso di definire e personalizzare aspetti fondamentali legati agli utenti, alle loro identità e alla gestione di queste ultime, gettando le basi per un'efficace gestione dell'Identity and Access Management (IAM). Un elemento centrale di questa configurazione è stata la definizione delle policy di autenticazione. Data l'intenzione di perseguire una migrazione "soft" verso il passwordless, che evitasse cambiamenti improvvisi e disorientanti per gli utenti, è stato essenziale integrare e gestire con attenzione le policy relative sia a FIDO che alle password. Ciò ha implicato un attento bilanciamento tra l'introduzione di nuove tecnologie di autenticazione e il mantenimento di un certo grado di familiarità per gli utenti. Durante la configurazione delle policy FIDO(figura 5.4), è stato possibile specificare e gestire gli autenticatori accettabili tramite la selezione dalla Global Authenticator Table(figura 5.5). Questa operazione, ha fornito

una struttura chiara per l'adozione di autenticatori conformi agli standard FIDO2, garantendo al contempo sicurezza e compatibilità. Parallelamente, è stata rivolta un'attenzione particolare alle policy relative alle password, partendo da una configurazione di default è stato possibile selezionare i vari vincoli, come illustrato nella figura 5.6. Nella realizzazione del flusso, il primo connettore ha svolto un ruolo chiave nell'assegnazione di vari identificativi a specifiche variabili d'ambiente(figura 5.7). Questa strategia ha facilitato l'utilizzo di tali identificativi nei connettori successivi, semplificando l'intero processo di autenticazione e rendendolo più agile e configurabile in base alle esigenze specifiche del progetto.

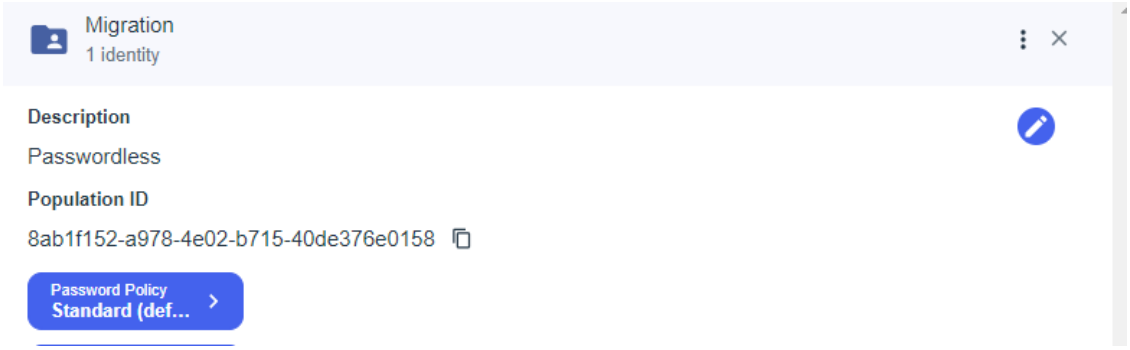

Figura 5.3. Creazione di una nuova Population

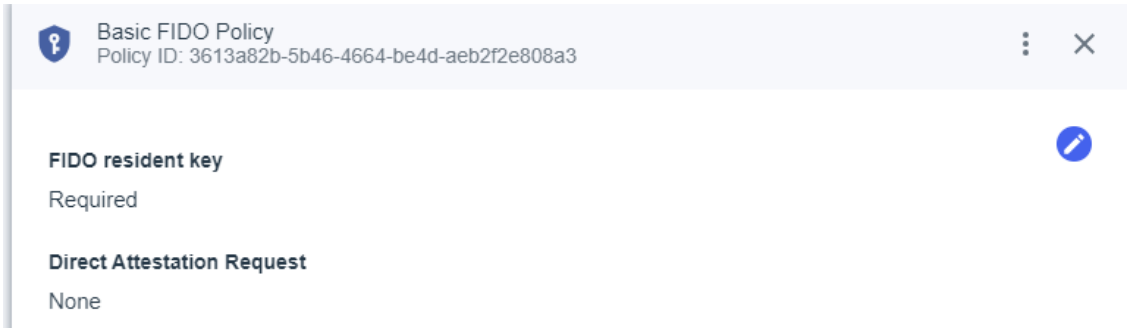

Figura 5.4. Integrazione delle policies di FIDO

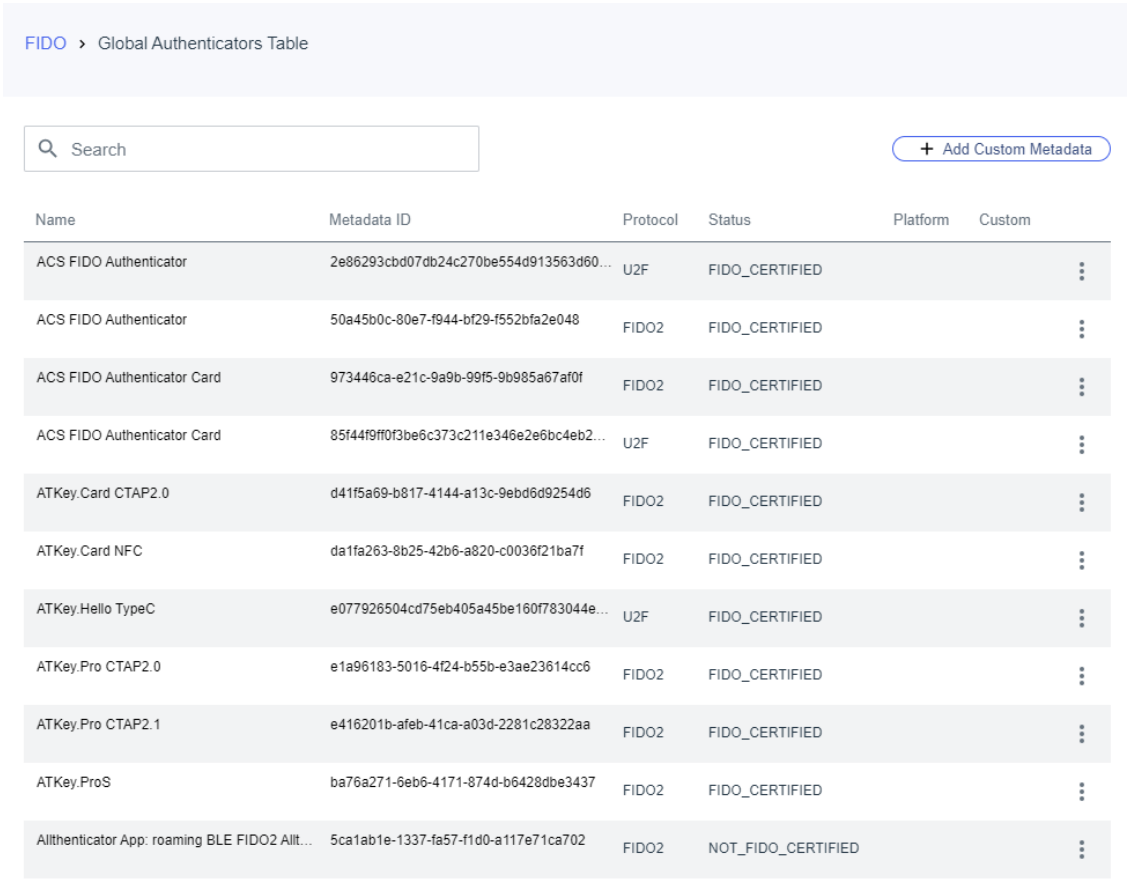

Figura 5.5. Tabella degli autenticatori

5.3 Flusso di Registrazione

1. **Richiesta e Verifica dell'Email**: L'utente inizia con l'immissione dell'indirizzo email in un form. Segue una verifica immediata che controlla sia la validità del formato dell'email sia che non sia già associata a un account esistente(figura 5.8);

2. **Convalida dell'Email**: Attraverso un'email inviata all'indirizzo fornito, l'utente è invitato a confermare la propria identità inserendo il codice OTP presente nell'Email, completando così un passaggio essenziale per la sicurezza e l'accuratezza dei dati(figura 5.9);

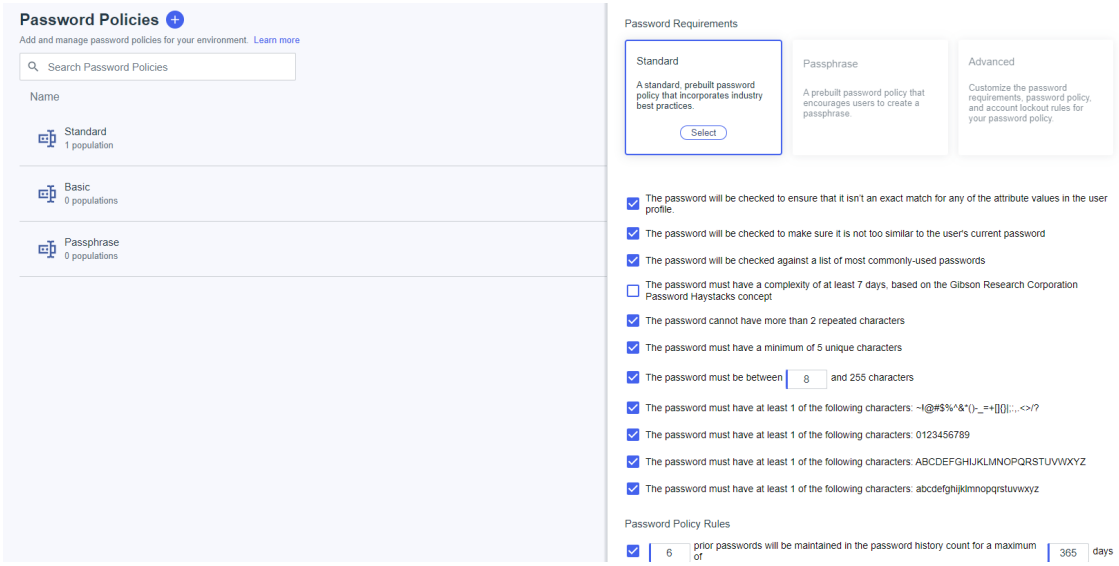

Figura 5.6. Interfaccia per la configurazione delle policies della password

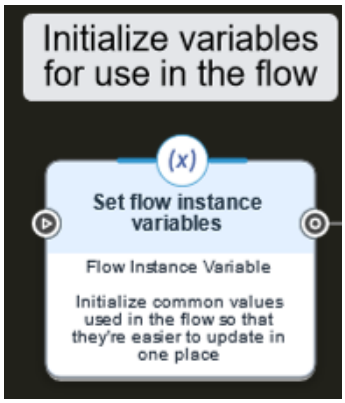

Figura 5.7. Connettore per la configurazione delle variabili d'ambiente

3. **Scelta del Metodo di Autenticazione**: Dopo la convalida, si apre una fase decisiva: l'utente si trova davanti a una scelta tra due percorsi distinti per procedere con la registrazione:

   - Optare per la creazione di una password tradizionale, avviando il sottoflusso con Password

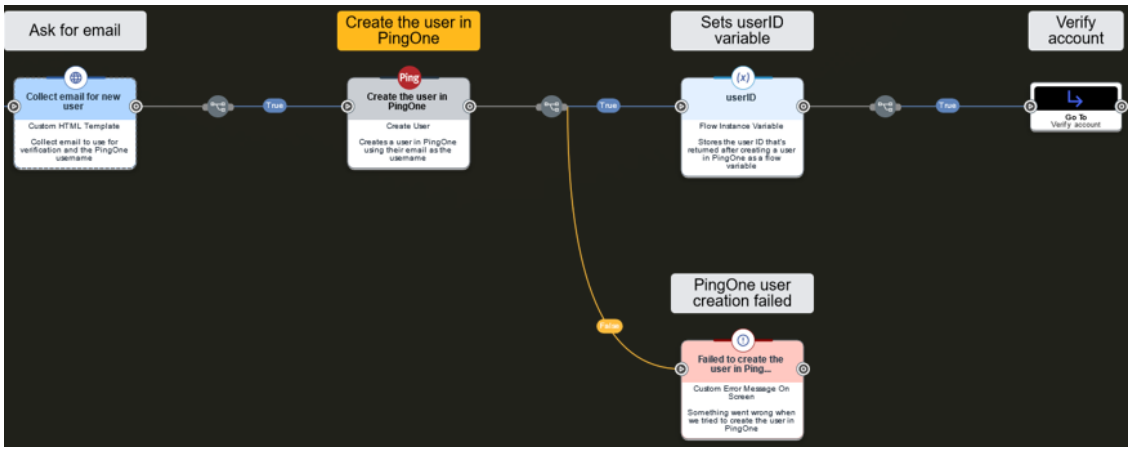

Figura 5.8. Prima parte del flusso di registrazione

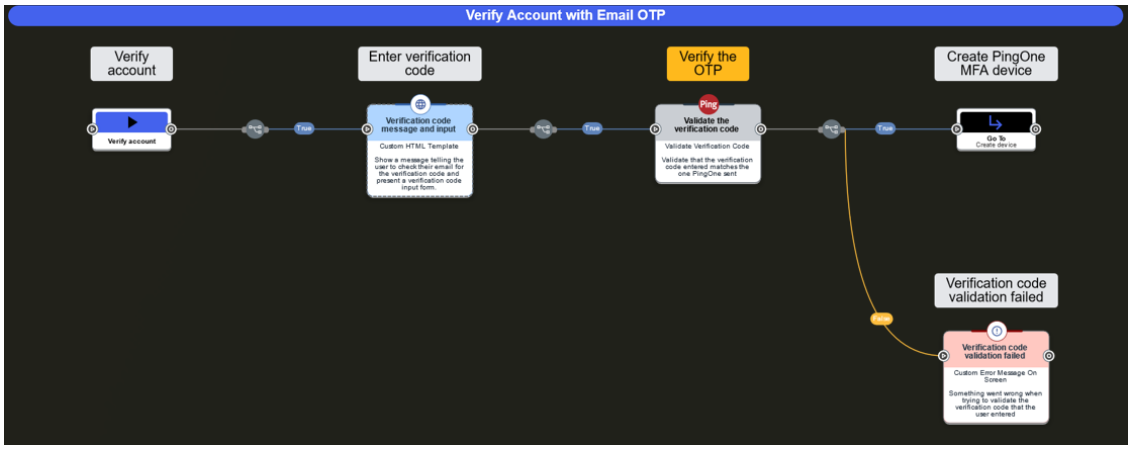

Figura 5.9. Convalida dell'Email

- Scegliere un approccio più moderno e sicuro, il sottoflusso Passwordless con Autenticatori FIDO2, rappresentando un punto di divergenza fondamentale nel processo di registrazione.

4. **Sottoflusso con Password**

4.1. **Inserimento e Verifica della Password**: L'utente crea una password che deve soddisfare criteri di sicurezza ben definiti. Viene fornito feedback in tempo reale per assicurare la conformità ai

requisiti;

4.2. **Completamento della Registrazione**: Con una password adeguata, il processo di registrazione si conclude positivamente, integrando l'utente nel database come nuovo membro autenticato tramite password(figura 5.10).

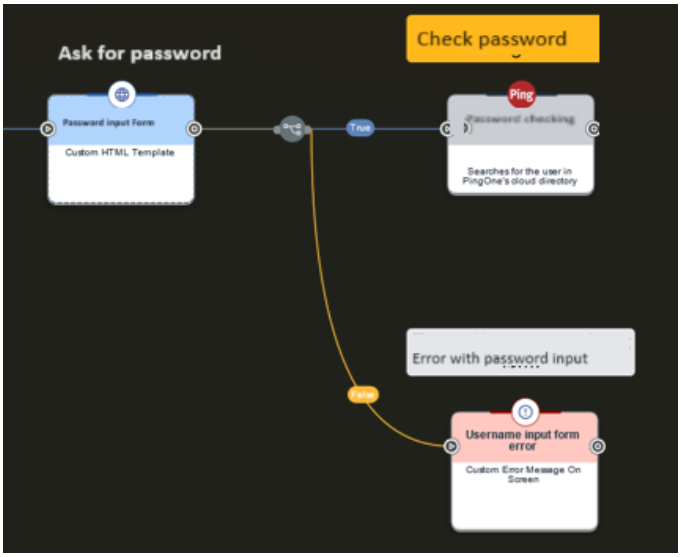

Figura 5.10. Creazione password

5. **Sottoflusso Passwordless con Autenticatori FIDO2**

5.1. **Selezione dell'Autenticatore FIDO2**: L'utente è invitato a scegliere tra diversi autenticatori FIDO2, come chiavette YubiKey, biometria o Windows Hello, dopo l'opportuna selezione dalla tabella inserita in precedenza. In questo passaggio vi è la creazione dell'identificativo del dispositivo e la generazione della coppia di chiavi crittografiche uniche. Questa coppia è composta da una chiave pubblica e una chiave privata. La chiave privata è segretamente e in modo sicuro conservata all'interno dell'autenticatore e non viene mai condivisa. La chiave pubblica, invece, sarà condivisa con il server per essere utilizzata nelle future operazioni di autenticazione(figura 5.11);

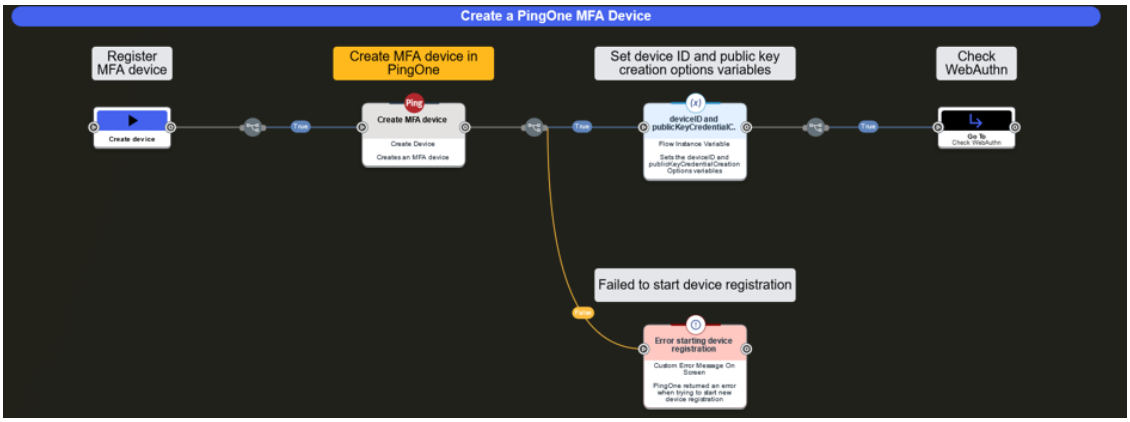

Figura 5.11. Creazione dispositivo

5.2. **Verifica del Supporto API WebAuthn**: In questo passaggio, il sistema verifica innanzitutto che il browser dell'utente supporti l'API WebAuthn, necessaria per procedere con l'autenticazione passwordless. Questo passaggio è trasparente per l'utente ma essenziale per la fattibilità del processo(figura 5.12);

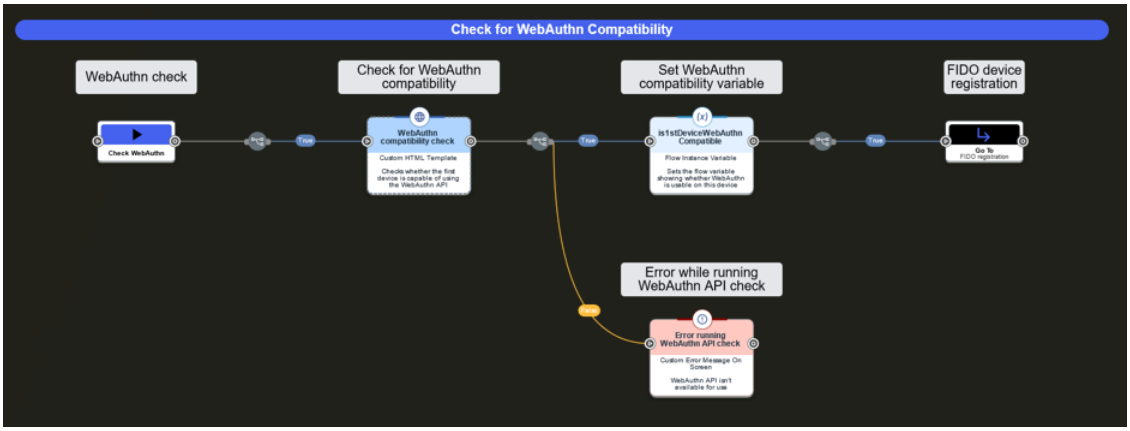

Figura 5.12. Controllo della compatibilità con WebAuthn

5.3. **Enrollment con WebAuthn**: Seguendo istruzioni chiare e semplici, l'utente procede con la registrazione del dispositivo FIDO2

scelto, collegandolo al proprio account. Questo processo è essenziale per stabilire un metodo di autenticazione sicuro e personale ed è basato, come già detto in precedenza, su crittografia asimmetrica. L'autenticatore crea quindi un attestato, che è un pacchetto di dati firmati che include la chiave pubblica generata, l'identificativo dell'autenticatore e altre informazioni pertinenti. Quest'attestato è firmato digitalmente utilizzando la chiave privata dell'autenticatore e viene inviato al server, che verifica l'autenticità dell'autenticatore e registra la chiave pubblica associata all'account dell'utente(figura 5.13);

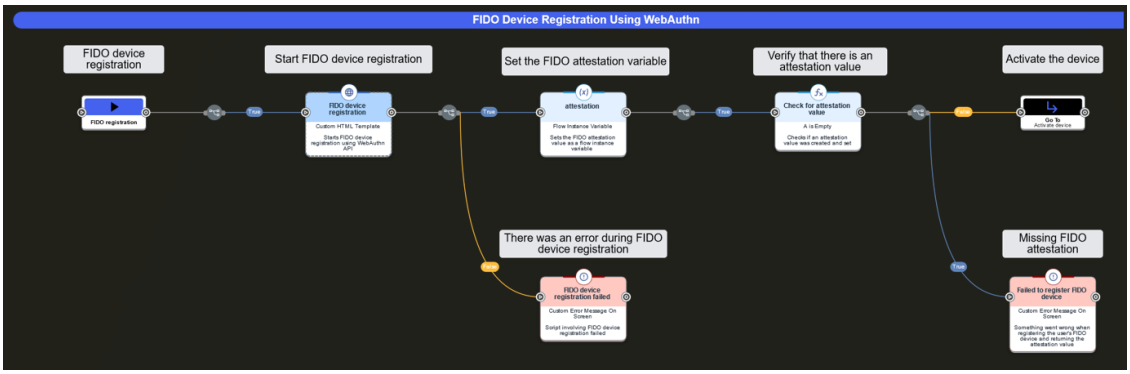

Figura 5.13. Attestazione FIDO

5.4. **Finalizzazione della Registrazione**: Una volta completato con successo l'associazione dell'utente all'autenticatore FIDO2, l'utente conclude il processo di registrazione e attivazione. Viene creato un nuovo profilo nel sistema, pronto per l'accesso passwordless(figura 5.14).

La biforcazione del flusso di registrazione in due sotto flussi permette agli utenti di personalizzare la propria esperienza di sicurezza, scegliendo tra la tradizionale sicurezza basata su password e l'innovativo approccio passwordless supportato dagli autenticatori FIDO2. Questa scelta non solo arricchisce l'esperienza utente ma rappresenta anche un passo avanti nella promozione di metodi di autenticazione più sicuri e user-friendly.

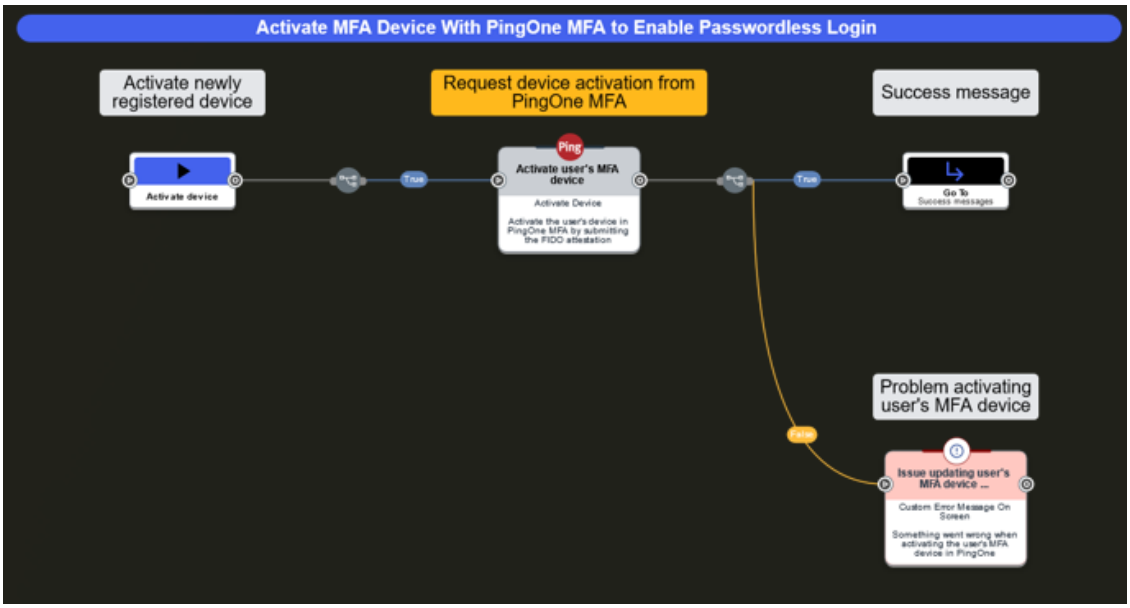

Figura 5.14. Attivazione del dispositivo e finalizzazione del processo di registrazione

5.3.1 Connettori

Come già accennato nei capitoli precedenti, i connettori giocano un ruolo fondamentale all'interno della piattaforma PingOne DaVinci, fungendo da elementi costitutivi per la creazione di flussi di autenticazione. Concentrandoci ora sul flusso di registrazione, ci addentriamo nell'esame specifico dei connettori che hanno reso possibile l'implementazione di questo percorso. I connettori PingOne, come quelli dedicati alla validazione dell'email o all'inserimento dell'utente nel sistema, offrendo funzionalità già integrate nella piattaforma, hanno semplificato notevolmente il processo. La loro configurazione ha richiesto unicamente l'immissione dei parametri corretti, spesso derivanti dagli output di altri connettori nel flusso. Nell'ottica di gestire in modo efficace i possibili errori durante il flusso di registrazione, è stato impiegato il connettore "Error Message". Questo strumento si è rivelato fondamentale per catturare e visualizzare gli errori che potrebbero verificarsi, offrendo agli utenti un feedback sul tipo di problema incontrato. La capacità di identificare e comunicare chiaramente gli errori migliora l'esperienza dell'utente, facilitando la risoluzione dei problemi e rendendo il processo di

autenticazione più fluido e intuitivo. Particolare attenzione è stata rivolta ai connettori HTTP, indispensabili per interagire con le API esterne e per personalizzare l'interfaccia utente. Questi connettori offrono la possibilità di integrare pagine HTML personalizzate, inclusi form e script, che possono essere adattati alle specifiche esigenze del flusso. Vediamo ora gli script presenti nei due connettori HTTP, quello per il controllo di compatibilità con WebAuthn(figura 5.15) e quello per creare una nuova credenziale per registrare il dispositivo usando WebAuthn(da figura 5.16 a 5.19). Questo è possibile grazie alla creazione automatica di un file JSON che riepiloga dettagliatamente la configurazione dei connettori, fornendo un utile riferimento per future revisioni o condivisioni delle logiche di flusso con il supporto tecnico.

```
const webAuthnCheck = () => {
  if (!window.PublicKeyCredential) {
    document.getElementById('webAuthnSupport').value = false;
    document.getElementById('webAuthnSupportSubmitBtn').click();
    return false;
  }

  document.getElementById('webAuthnSupport').value = true;
  document.getElementById('webAuthnSupportSubmitBtn').click();
  return true;
};

if (document.readyState === 'loading') {
  document.addEventListener('DOMContentLoaded', webAuthnCheck);
} else {
  const webAuthnSupportSubmitBtn = document.getElementById('webAuthnSupportSubmitBtn'
  if (webAuthnSupportSubmitBtn) {
    webAuthnSupportSubmitBtn.addEventListener('click', webAuthnCheck);
  }
  return webAuthnCheck();
}
```

Figura 5.15. Script per eseguire la verifica dell'API WebAuthn

```
const buildAttestationForPingOneMFA = (credential) => {
  const newCredentialInfo = {};
  const response = {};

  if (credential.id) {
    newCredentialInfo.id = credential.id;
  }
  if (credential.type) {
    newCredentialInfo.type = credential.type;
  }
  if (credential.rawId) {
    newCredentialInfo.rawId = toBase64Str(credential.rawId);
  }
  if (!credential.response) {
    throw "Missing 'response' attribute in credential response";
  }
  response.clientDataJSON = toBase64Str(credential.response.clientDataJSON);
  response.attestationObject = toBase64Str(credential.response.attestationObject);

  newCredentialInfo.response = response;
  return newCredentialInfo;
};
```

Figura 5.16. Funzione buildAttestationForPingOneMFA

Spiegazione del codice

Nel primo script(figura 5.15) è implementata la funzione **webAuthnCheck**, che controlla se l'API WebAuthn (window.PublicKeyCredential) è disponibile nel browser dell'utente. L'API WebAuthn permette di realizzare l'autenticazione sicura tramite credenziali crittografiche, sostituendo o integrando metodi di autenticazione tradizionali come password o SMS. Se l'API non è supportata (window.PublicKeyCredential è undefined), il valore di un campo input nascosto (webAuthnSupport) viene impostato su false, e si simula un click sul pulsante di invio (webAuthnSupportSubmitBtn) per avanzare nel flusso di autenticazione, nel connettore di errore. Se l'API è supportata, il valore viene impostato su true e si procede allo stesso modo, ma il

```
const buildPubKeyCredentialOptions = (options) => {
  const createCredentialsOptions = {};
  createCredentialsOptions.rp = options.rp;
  createCredentialsOptions.user = options.user;
  createCredentialsOptions.user.id = new Uint8Array(options.user.id);
  createCredentialsOptions.challenge = new Uint8Array(options.challenge);
  createCredentialsOptions.pubKeyCredParams = options.pubKeyCredParams;
  if (options.timeout) {
    createCredentialsOptions.timeout = options.timeout;
  }
  if (options.excludeCredentials) {
    createCredentialsOptions.excludeCredentials = credentialListConversion(options.exc
  }
  if (options.authenticatorSelection) {
    createCredentialsOptions.authenticatorSelection = options.authenticatorSelection;
  }
  createCredentialsOptions.authenticatorSelection.authenticatorAttachment = 'cross-pla
  if (options.attestation) {
    createCredentialsOptions.attestation = options.attestation;
  }
  if (options.extensions) {
    createCredentialsOptions.extensions = options.extensions;
  }
  return createCredentialsOptions;
};
```

Figura 5.17. Funzione buildPubKeyCredentialOptions

flusso proseguirà con la registrazione del dispositivo. Il codice frammentato implementa un sistema di registrazione utente utilizzando la tecnologia WebAuthn, che consente una registrazione sicura attraverso l'autenticazione basata su credenziali crittografiche. Ecco una panoramica di ciò che ogni parte fa:

- **buildAttestationForPingOneMFA**: Prepara l'oggetto di attestazione da una credenziale WebAuthn generata, includendo dettagli come l'ID della credenziale, il tipo e i dati di risposta codificati in base64, pronti per la registrazione con il servizio PingOne MFA(figura 5.16);
- **buildPubKeyCredentialOptions**: Configura le opzioni necessarie per

```
const registerNewPubKeyCredAndSubmitAttestation = async (options) => {
  options = parseJSONIfNeeded(options);
  const publicKeyCredentialCreationOptions = buildPubKeyCredentialOptions(options);
  try {
    const pubKeyCred = await navigator.credentials.create({publicKey: publicKeyCreder
    const attestedCred = buildAttestationForPingOneMFA(pubKeyCred);
    const attestationElement = document.getElementById('attestation');
    const attestationBtn = document.getElementById('submitAttestationButton');
    attestationElement.value = JSON.stringify(attestedCred);
    attestationBtn.click();
    return JSON.stringify(attestedCred);
  } catch (error) {
    throw new Error('Failed to use WebAuthn to create a new credential.', {cause: err
  }
};
```

Figura 5.18. Funzione registerNewPubKeyCredAndSubmitAttestation

```
const fidoRegistration = async (event) => {
  if (event) event.preventDefault();
  resetErrorMessageText();
  const publicKeyCredentialCreationOptions = '{{global.variables.publicKeyCredentialCr
  if (publicKeyCredentialCreationOptions) {
    try {
      return await registerNewPubKeyCredAndSubmitAttestation(publicKeyCredentialCreati
    } catch (error) {
      updateErrorMessageText(error);
      return false;
    }
  } else {
    updateErrorMessageText('Missing credential creation options');
  }
};
```

Figura 5.19. Funzione fidoRegistration

la creazione di una nuova credenziale WebAuthn, stabilendo parametri come il Relying Party, le informazioni utente, la sfida, i parametri della chiave pubblica, e altre configurazioni opzionali per la richiesta di

creazione della credenziale(figura 5.17);

- **registerNewPubKeyCredAndSubmitAttestation**: Gestisce il processo di creazione della nuova credenziale WebAuthn tramite l'API del browser e invia i dati di attestazione al server per la registrazione(figura 5.18);
- **fidoRegistration**: Agisce come punto di ingresso per avviare il flusso di registrazione, preparando le opzioni di creazione della credenziale, gestendo la registrazione effettiva e fornendo feedback all'utente attraverso l'interfaccia della pagina web(figura 5.19);

5.4 Flusso di Login

1. **Inserimento dell'Email e Verifica della Presenza dell'Email nel Database**: Il processo di login inizia con l'utente che inserisce il proprio indirizzo email in un form, per verificare che l'utente sia all'interno del sistema. Utilizzando un connettore di PingOne DaVinci, il sistema verifica se l'email inserita corrisponde a un account esistente nel database, altrimenti non si procederà con l'autenticazione;

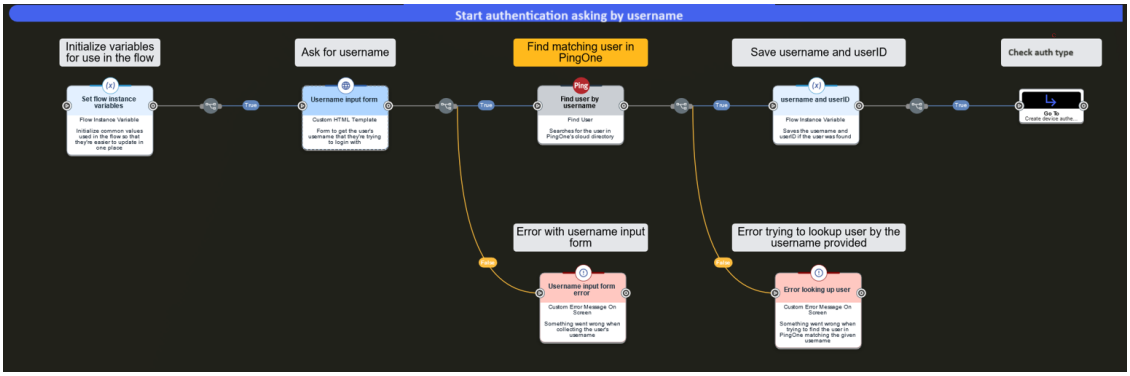

Figura 5.20. Prima parte del flusso di autenticazione

2. **Determinazione della Modalità di Autenticazione**: A questo punto, il sistema, attraverso il connettore DaVinci, identifica il metodo di autenticazione scelto dall'utente durante la registrazione (password o

passwordless), indirizzando verso uno dei due sotto flussi di autenticazione;

3. **Sottoflusso con Password**

   3.1. **Richiesta di Inserimento della Password**: Se l'utente ha scelto l'autenticazione con password durante la registrazione, viene richiesto di inserire la sua password tramite un form dedicato;

   3.2. **Verifica della Correttezza della Password**: Il sistema controlla che la password inserita corrisponda a quella associata all'email nel database(5.21);

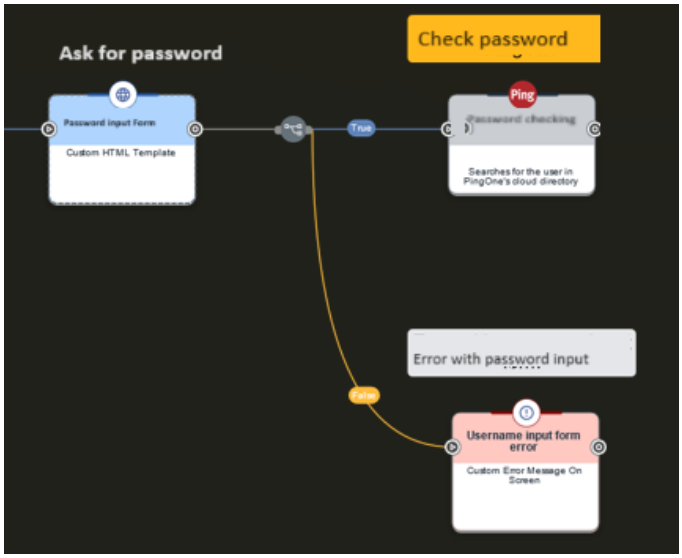

Figura 5.21. Controllo della password

   3.3. **Richiesta di Migrazione al Passwordless**: Una volta autenticato, viene presentato all'utente un pop-up che chiede se desidera passare all'autenticazione passwordless. In caso di risposta affermativa, si innesca il processo di transizione:

      3.3.1. **Verifica Compatibilità API WebAuthn**: Si esegue un controllo invisibile per verificare la compatibilità del browser con l'API WebAuthn;

      3.3.2. **Enrollment del Dispositivo**: L'utente procede con l'associazione di un dispositivo FIDO2;

3.3.3. **Aggiornamento Modalità di Autenticazione**: Il sistema aggiorna le informazioni dell'utente per riflettere la nuova modalità di autenticazione passwordless scelta.

4. **Sottoflusso Passwordless con Autenticatori FIDO2**

4.1. **Creazione dell'autenticazione del dispositivo**: Il processo inizia con la raccolta di informazioni dal dispositivo di autenticazione dell'utente. Questo include l'identificativo unico del dispositivo, noto come Device ID, e le credenziali a chiave pubblica. Questi valori sono salvati nel sistema e serviranno a identificare in modo univoco il dispositivo e a verificarne l'autenticità in fase di autenticazione(figura 5.22);

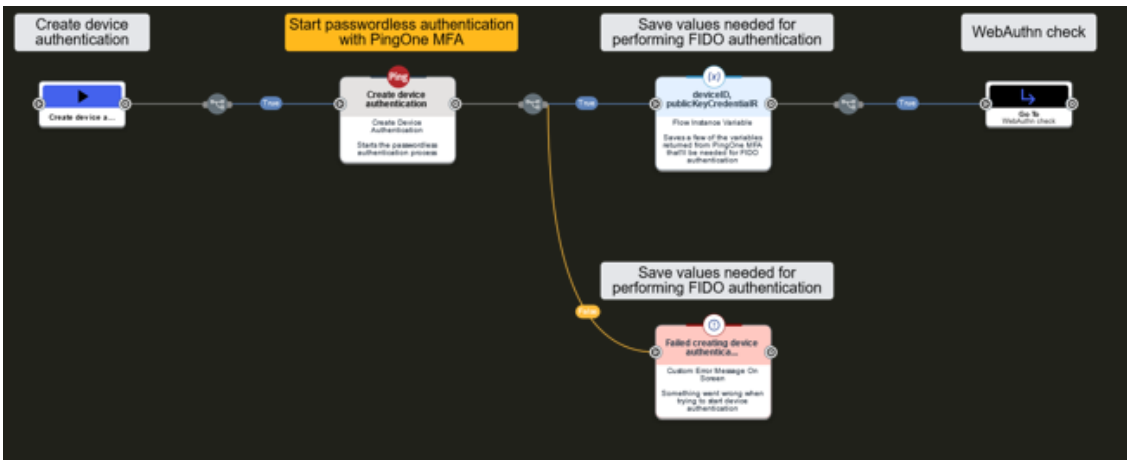

Figura 5.22. Prima parte del flusso di autenticazione FIDO2

4.2. **Verifica Compatibilità con l'API WebAuthn**: Per gli utenti che hanno optato per l'autenticazione passwordless, il sistema verifica la compatibilità del browser con l'API WebAuthn(figura 5.23);

4.3. **Challenge con l'Autenticatore**: Il sistema genera una challenge crittografica unica che sarà inviata al dispositivo di autenticazione per essere firmata (figura 5.24);

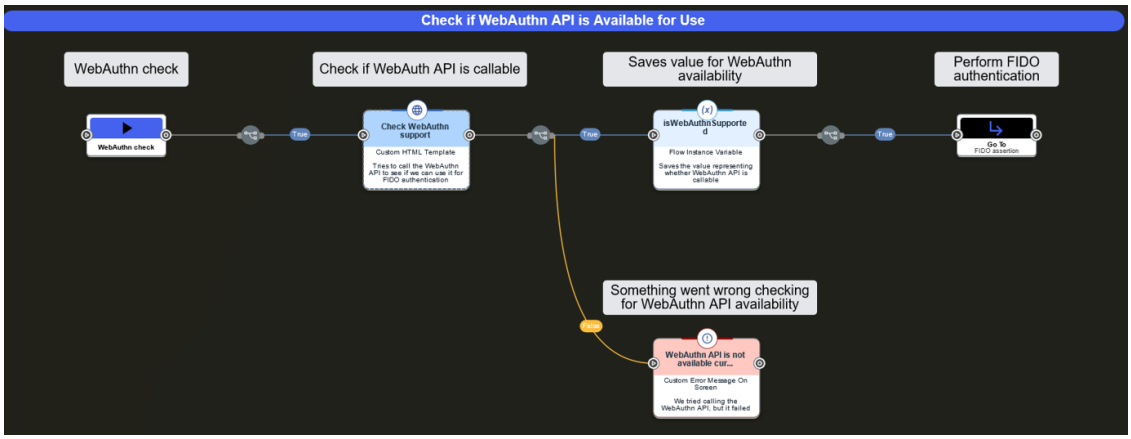

Figura 5.23. Controllo della disponibilità dell'API WebAuthn

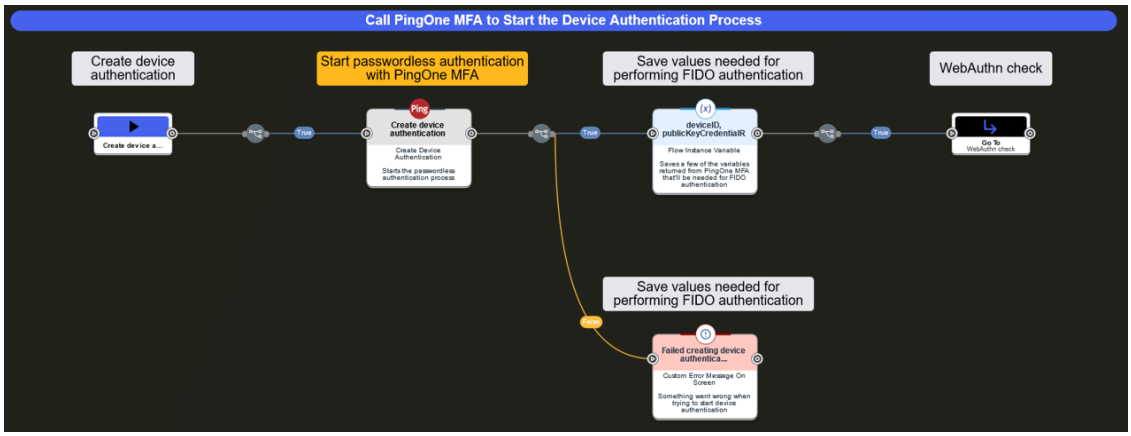

Figura 5.24. Generazione della challenge

4.4. **Validazione dell'asserzione**: L'asserzione firmata viene inviata indietro al servizio che ha emesso la challenge. Questo è il momento critico in cui l'asserzione viene confrontata con i dati conosciuti e attendibili dal servizio. Il servizio utilizza la chiave pubblica associata all'utente per verificare la firma sull'asserzione. Se la verifica ha esito positivo, dimostra che l'asserzione proviene dal dispositivo autorizzato e che la sessione di autenticazione è legittima(figura 5.25);

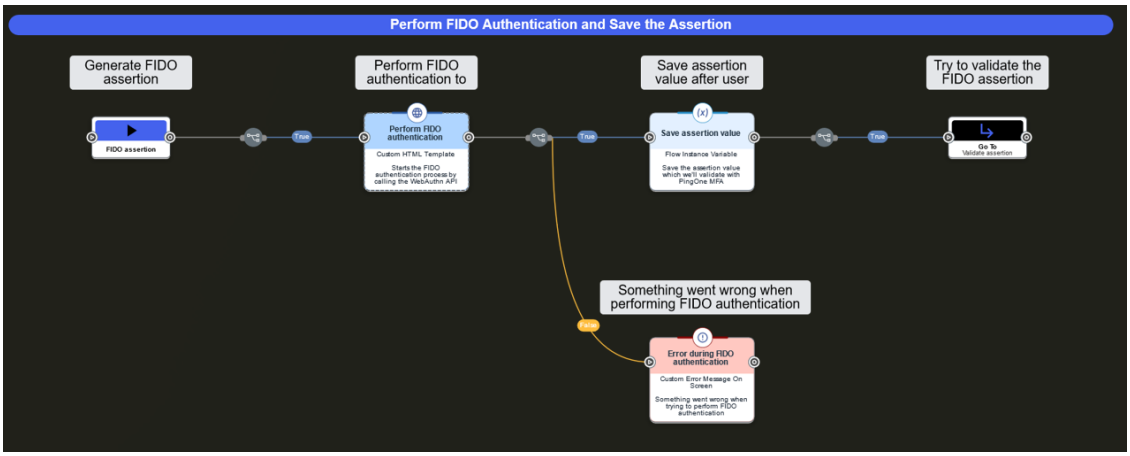

Figura 5.25. Validazione dell'asserzione

5. **Login Completato**: In assenza di errori durante il processo di autenticazione, l'utente ottiene l'accesso all'applicazione.

Questo approccio al processo di login offre agli utenti flessibilità e sicurezza, permettendo non solo di accedere all'applicazione tramite il metodo di autenticazione scelto in fase di registrazione ma anche di passare a un metodo più sicuro e conveniente come il passwordless. La transizione offerta post-login rappresenta un'opportunità per migliorare l'esperienza utente incrementando al contempo la sicurezza dell'account.

5.4.1 Connettori

Come già fatto in precedenza andiamo ad osservare quella che è la configurazione, e quindi lo script presente per eseguire l'autenticazione tramite FIDO2.(da figura 5.26 a 5.29).

Spiegazione del codice

Questo codice completo implementa il processo di autenticazione utente utilizzando la tecnologia WebAuthn. Ecco una panoramica di ciò che ogni parte fa:

```
const buildPubKeyRequestOptions = (options) => {
  const publicKeyCredentialRequestOptions = {};
  publicKeyCredentialRequestOptions.challenge = new Uint8Array(atob(options.challenge)
  if (options.allowCredentials) {
    publicKeyCredentialRequestOptions.allowCredentials = options.allowCredentials.map(
      type: cred.type,
      id: new Uint8Array(atob(cred.id).split('').map(char => char.charCodeAt(0))),
      transports: cred.transports
    }));
  }
  if (options.timeout) publicKeyCredentialRequestOptions.timeout = options.timeout;
  return publicKeyCredentialRequestOptions;
};
```

Figura 5.26. Funzione buildPubKeyRequestOptions

```
const createPubliCKeyCredential = (assertion) => {
  return {
    id: assertion.id,
    type: assertion.type,
    rawId: toBase64Str(assertion.rawId),
    response: {
      clientDataJSON: toBase64Str(assertion.response.clientDataJSON),
      authenticatorData: toBase64Str(assertion.response.authenticatorData),
      signature: toBase64Str(assertion.response.signature),
      userHandle: toBase64Str(assertion.response.userHandle ? assertion.response.userH
    }
  };
};
```

Figura 5.27. Funzione createPubliCKeyCredential

- **buildPubKeyRequestOptions**: Prepara le opzioni necessarie per una richiesta di autenticazione con l'API WebAuthn. Questo include la conversione della sfida da una stringa base64 a un array di byte (Uint8Array), la preparazione dell'elenco delle credenziali consentite per l'autenticazione e la definizione del tempo massimo disponibile per completare

```
const getFIDOAssertion = async (options) => {
  options = parseJSONIfNeeded(options);
  const publicKeyCredentialRequestOptions = buildPubKeyRequestOptions(options);
  try {
    const assertion = await navigator.credentials.get({ publicKey: publicKeyCredentiall
    return JSON.stringify(createPubliCKeyCredential(assertion));
  } catch (error) {
    throw new Error('Failed to generate an assertion through FIDO authentication.', {c
  }
};
```

Figura 5.28. Funzione getFIDOAssertion

```
const fidoAuthn = async (event) => {
  if (event) event.preventDefault();
  const publicKeyCredentialRequestOptions = '{{global.variables.publicKeyCredentialReq
  try {
    const assertion = await getFIDOAssertion(publicKeyCredentialRequestOptions);
    document.getElementById('assertionValue').value = assertion;
    document.getElementById('assertionButton').click();
  } catch (error) {
    updateErrorMessageText(error.toString());
  }
};
```

Figura 5.29. Funzione fidoAuthn

l'operazione. L'obiettivo è di formulare una richiesta che soddisfi i criteri di sicurezza richiesti dall'API WebAuthn e dal server che verifica l'autenticazione(figura 5.26);

- **createPubliCKeyCredential**: Prende l'asserzione ottenuta e la trasforma in un formato standardizzato (PublicKeyCredential), che include tutti i dettagli necessari per la verifica lato server, come l'ID della credenziale, il tipo e i dati della risposta codificati in base64. Questo passaggio è fondamentale per assicurare che le informazioni inviate al server siano complete e conformi agli standard WebAuthn(figura 5.27);

- **getFIDOAssertion**: Utilizza le opzioni preparate per richiedere al browser dell'utente di eseguire l'autenticazione FIDO. Attraverso l'API WebAuthn, il browser interagisce con un autenticatore compatibile (come un dispositivo biometrico, una chiave di sicurezza hardware, o un PIN) per generare un'asserzione. Questa asserzione contiene una firma digitale creata dall'autenticatore che può essere verificata dal server per confermare l'identità dell'utente. La funzione gestisce questo processo e prepara l'asserzione per l'invio al server(figura 5.28);

- **fidoAuthn**: Agisce come funzione principale che coordina il flusso di autenticazione, iniziando con la preparazione e l'invio della richiesta di autenticazione e terminando con l'elaborazione dell'asserzione ricevuta. Se l'autenticazione riesce, i dettagli dell'asserzione vengono utilizzati per procedere con le successive fasi di autenticazione o accesso all'applicazione. In caso di fallimento, l'utente viene informato tramite messaggi di errore appropriati(figura 5.29);

5.5 Web Application

Entriamo ora nel vivo dell'applicazione pratica, dove i concetti di autenticazione si trasformano in interazioni concrete all'interno di un'app web. Il lavoro fatto fino a questo punto prende vita in una piattaforma che non solo protegge ma facilita ogni passo dell'utente. In questo capitolo, andiamo a scoprire come l'architettura dei flussi di autenticazione si concretizza in un ambiente web intuitivo, accessibile e sicuro. I prossimi paragrafi guideranno l'utente attraverso l'esperienza dell'app, dimostrando come la teoria dell'autenticazione avanzata prende forma nel mondo reale, influenzando e migliorando la routine digitale.

5.5.1 HomePage

Quando un utente accede alla schermata iniziale dell'applicazione(figura 5.30), si trova di fronte a un form di accesso/registrazione. Questo form richiede all'utente di inserire un *username*, che in questo contesto corrisponde alla sua email. Subito dopo l'inserimento, l'utente ha due opzioni disponibili tramite due distinti bottoni: uno per effettuare il login e l'altro per registrarsi. L'applicazione effettua un controllo preliminare sul formato dell'email per assicurarsi che sia valido. Successivamente, procede con la ricerca dell'email all'interno del database per verificare se un utente stia tentando di registrarsi con un'email già in uso o di accedere con un'email non associata a nessun iscritto. Rispettivamente sarà mostrato il messaggio di errore "Email già presente" o "Email non presente".

5.5.2 Registrazione

Dopo la validazione dell'email tramite codice OTP, il processo di registrazione si divide in due percorsi distinti a seconda della scelta dell'utente su come desidera autenticarsi: tramite password o tramite tecnologia FIDO2. Questa fase inizia con una schermata di selezione dove l'utente può decidere il metodo di autenticazione preferito(figura 5.31).

Con Password

Se l'utente sceglie la registrazione con password, viene reindirizzato a un form specifico(5.32). Qui, deve inserire una password e confermarla, assicurandosi che soddisfi tutte le policy di sicurezza preimpostate (come lunghezza minima, inclusione di caratteri speciali, ecc.). In caso di successo, l'utente completa la registrazione e può accedere al portale. Se la password non rispetta le policy, viene mostrato un messaggio di errore che specifica le regole non soddisfatte, permettendo all'utente di adeguarsi.

Senza Password

Nel percorso di registrazione che utilizza la tecnologia FIDO2, l'utente si imbatte in una fase decisamente orientata alla sicurezza avanzata. Dopo aver scelto di procedere senza l'utilizzo di una password tradizionale, appare

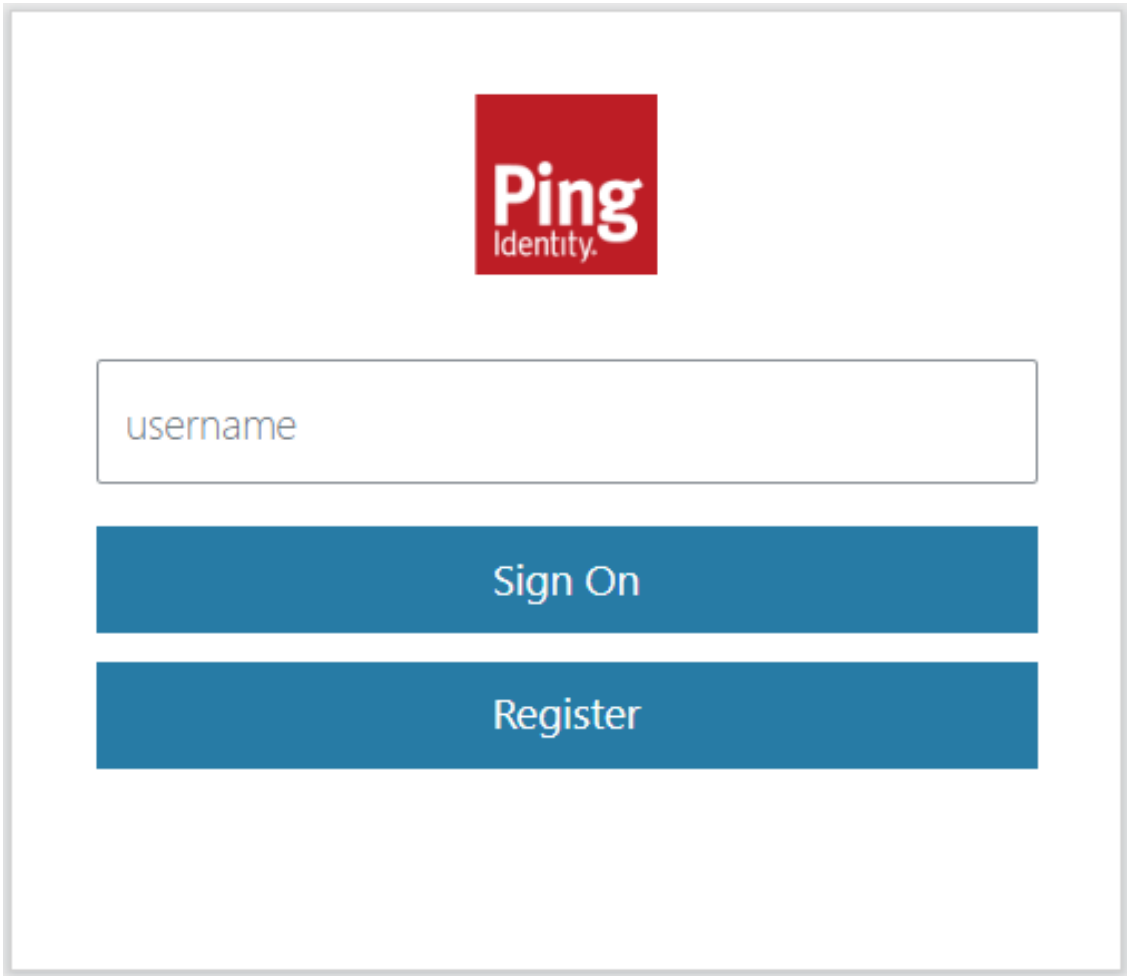

Figura 5.30. Schermata HomePage

la schermata per registrare il dispositivo FIDO(figura 5.33), e in seguito alla pressione dell'unico bottone presente, si apre la finestra "Sicurezza di Windows"(figura 5.34). Questo passaggio è cruciale perché introduce l'utente al concetto di *Passkey*, una chiave di sicurezza che rappresenta un modo più sicuro ed efficiente per accedere ai servizi online.

All'interno di questa finestra, l'utente ha la possibilità di selezionare tra diverse opzioni per la sua autenticazione FIDO2. Le scelte disponibili includono l'utilizzo di una chiave di sicurezza fisica o l'impiego del dispositivo Windows stesso, che, come menzionato, supporta lo standard WebAuthn. Quest'ultimo permette un'esperienza di autenticazione senza password, sfruttando

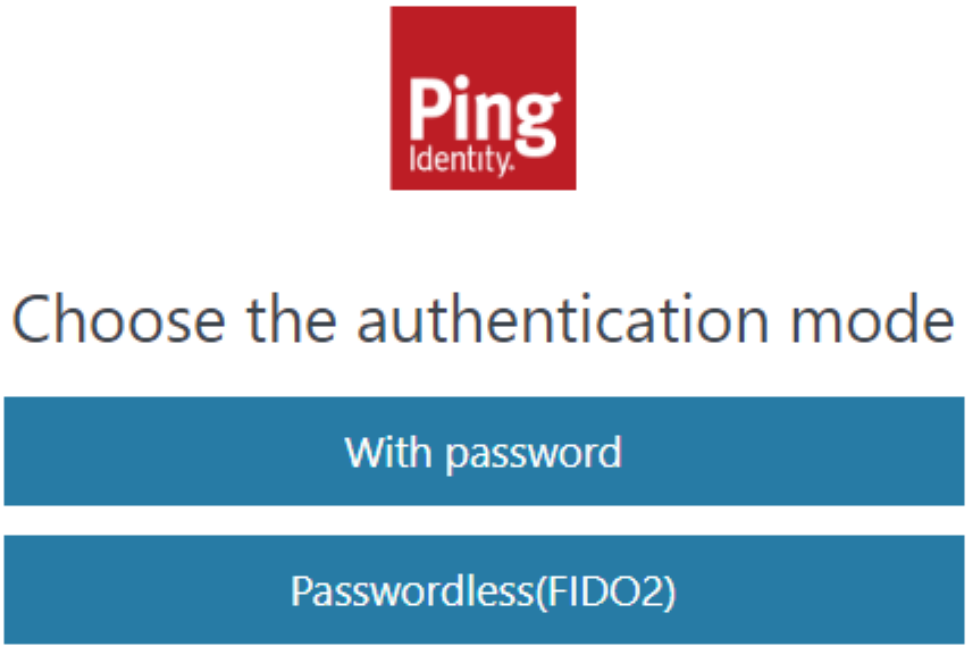

Figura 5.31. Schermata in cui l'utente è invitato a scegliere la modalità di autenticazione

caratteristiche biometriche o PIN configurati sul dispositivo dell'utente.

La selezione e la registrazione di una Passkey segnano il completamento del processo di registrazione. L'utente è ora in grado di accedere al portale dell'applicazione web con un metodo altamente sicuro, riducendo i rischi associati alle password tradizionali e migliorando significativamente l'esperienza utente grazie alla comodità dell'autenticazione biometrica o del PIN.
.

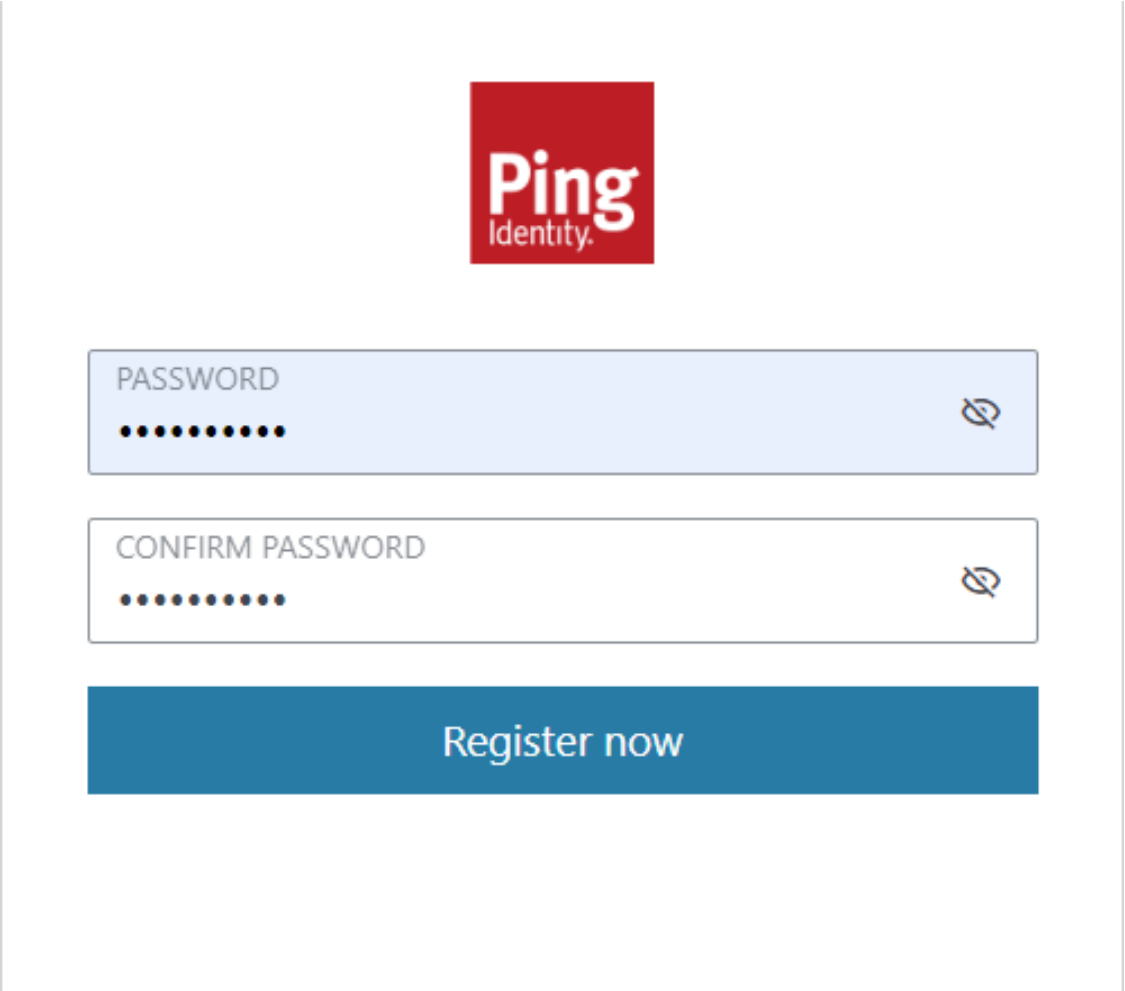

Figura 5.32. Schermata in cui l'utente è invitato a scegliere la modalità di autenticazione

5.5.3 Login

Quando un utente, dalla homepage, decide di accedere all'applicazione, il sistema automaticamente identifica la modalità di autenticazione selezionata durante la fase di registrazione. Questa funzionalità assicura un'esperienza utente fluida e personalizzata, guidando l'utente direttamente al metodo di login appropriato.

Figura 5.33. Schermata per registrare la Passkey

Con Password

Nel caso in cui l'utente abbia scelto la registrazione con password, viene presentata una schermata specifica (figura 5.35) dove è richiesto di inserire la propria password. In questa pagina, è inoltre disponibile un link "Forgot Password" che consente agli utenti di avviare il processo di reset della password, nel caso in cui questa sia stata dimenticata. Questa opzione migliora l'accessibilità e la gestione dell'account, permettendo agli utenti di recuperare l'accesso in modo sicuro e guidato.

Dopo l'inserimento corretto della password, compare un popup (figura 5.36) che propone all'utente l'opportunità di migrare verso un sistema di autenticazione senza password. Se l'utente accetta, il processo di migrazione inizia immediatamente: comporta la registrazione del dispositivo per l'autenticazione e l'aggiornamento delle impostazioni dell'account. Nei successivi accessi, al posto della password, verrà richiesto di utilizzare il nuovo metodo di autenticazione, rendendo l'esperienza più sicura e conveniente.

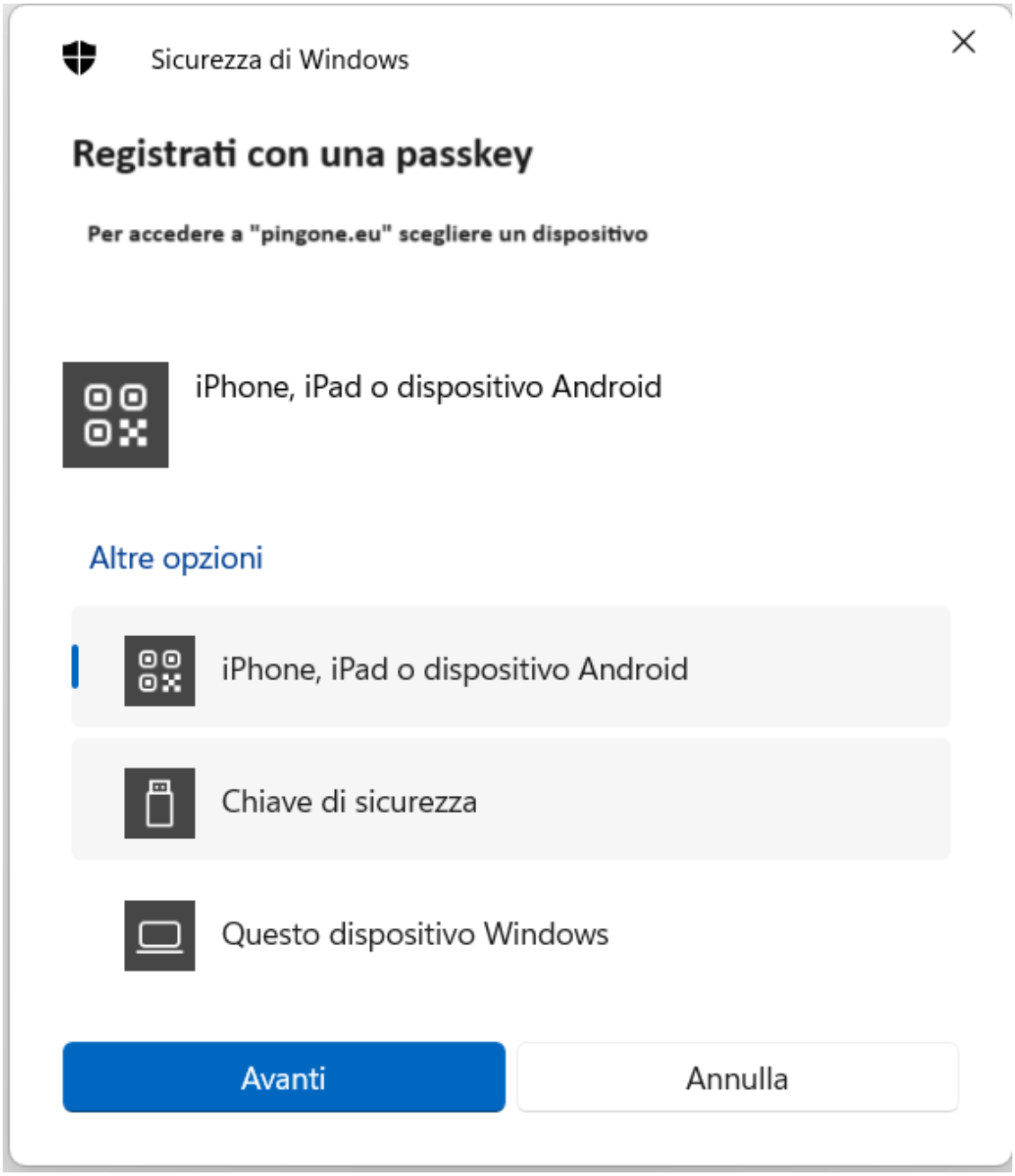

Figura 5.34. Schermata per scegliere la Passkey

Senza Password

Per gli utenti che hanno optato per un metodo di autenticazione senza password durante la fase di registrazione, il login avviene attraverso la finestra

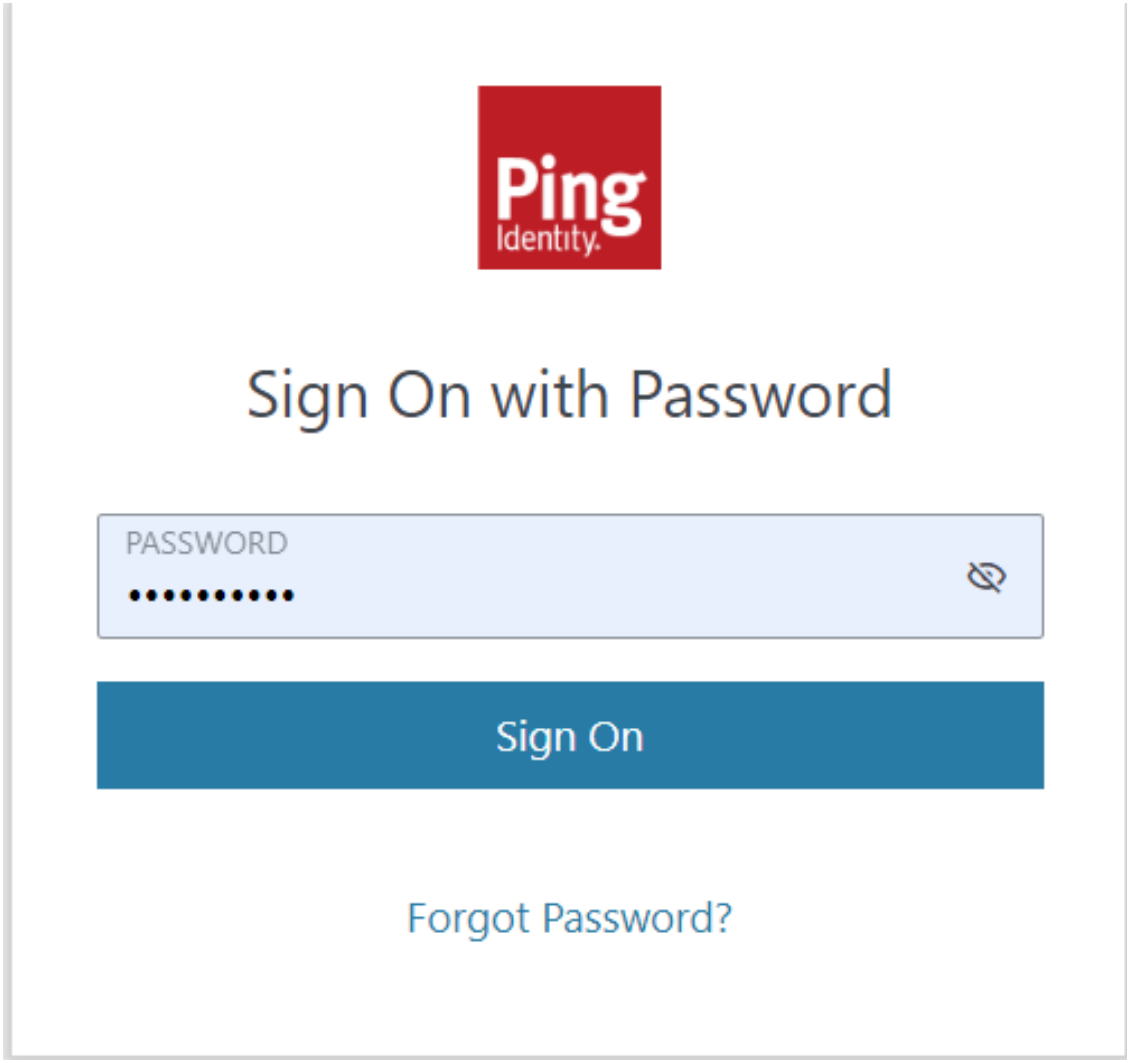

Figura 5.35. Schermata per inserire la password

di "Sicurezza Windows". In questa fase, viene chiesto all'utente di selezionare il dispositivo con la passkey salvata(figura 5.37). Questo metodo sfrutta lo standard FIDO2 per garantire un accesso sicuro e senza l'uso di password. Utilizzando dispositivi o caratteristiche biometriche approvate, l'utente può accedere al proprio account in maniera più diretta e protetta, eliminando la necessità di ricordare e digitare password complesse.

Figura 5.36. Pop-up per la transizione al passwordless

5.5.4 Portale Utente

Una decisione strategica è stata l'integrazione del portale utente nell'applicazione(figura 5.38), un hub centrale dell'applicazione che consolida tutte le funzionalità self-service. Questa interfaccia è progettata per offrire agli utenti pieno controllo sulle proprie impostazioni di sicurezza e autenticazione, abilitando una gestione autonoma e sicura del proprio account. Il portale utente permette di eseguire una varietà di azioni self-service, tra cui il cambio della password, l'attivazione del multifactor authentication (MFA), e l'aggiunta di più dispositivi per l'autenticazione senza password. La possibilità di registrare più dispositivi è particolarmente rilevante, poiché affronta direttamente il problema della dipendenza da un unico dispositivo di sicurezza, migliorando la resilienza dell'accesso all'account. La necessità e l'importanza di queste funzionalità, insieme alla soluzione al problema della dipendenza da un unico

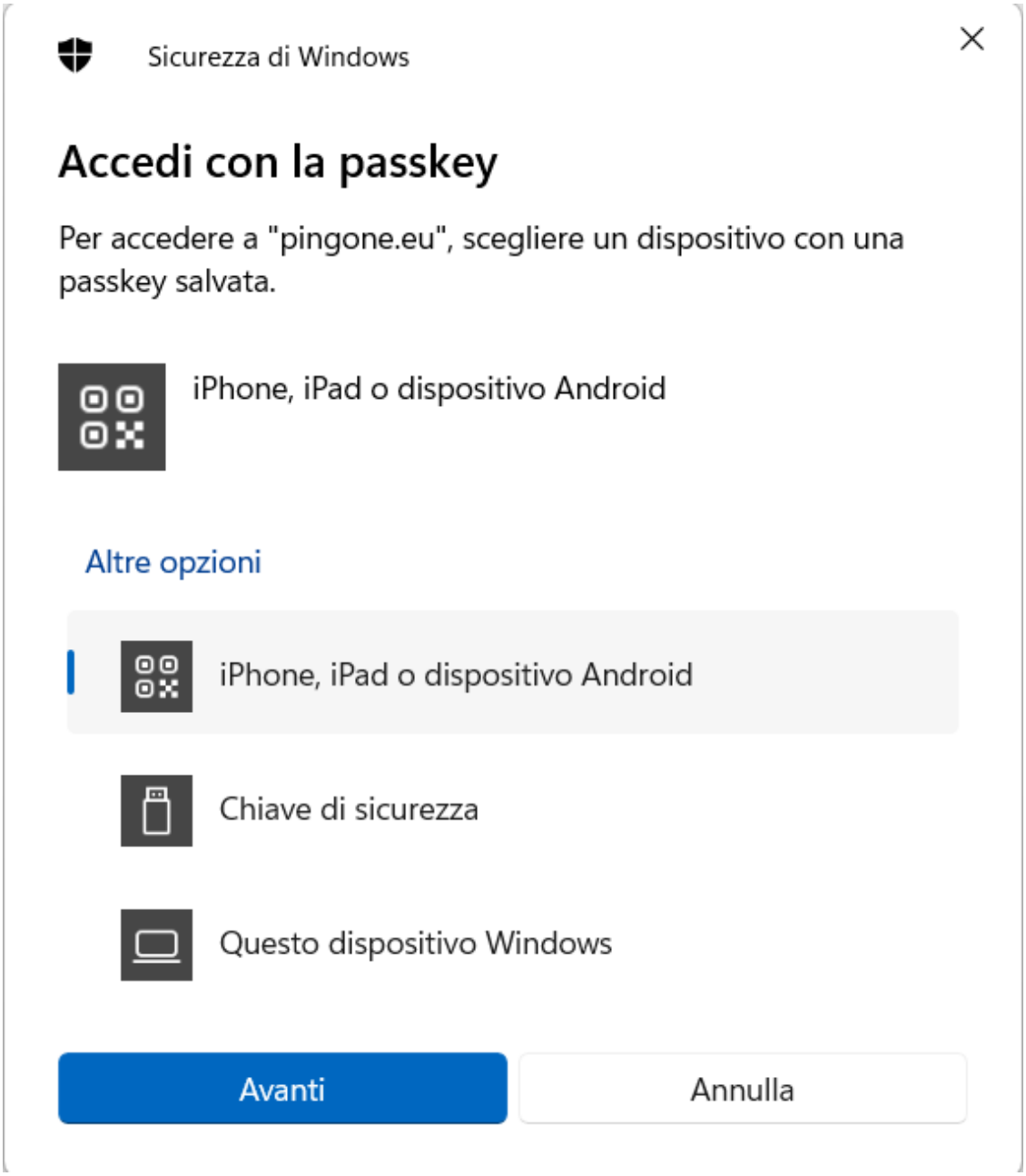

Figura 5.37. Schermata per selezionare il dispositivo per poter accedere

dispositivo, saranno discusse più dettagliatamente nel capitolo successivo.

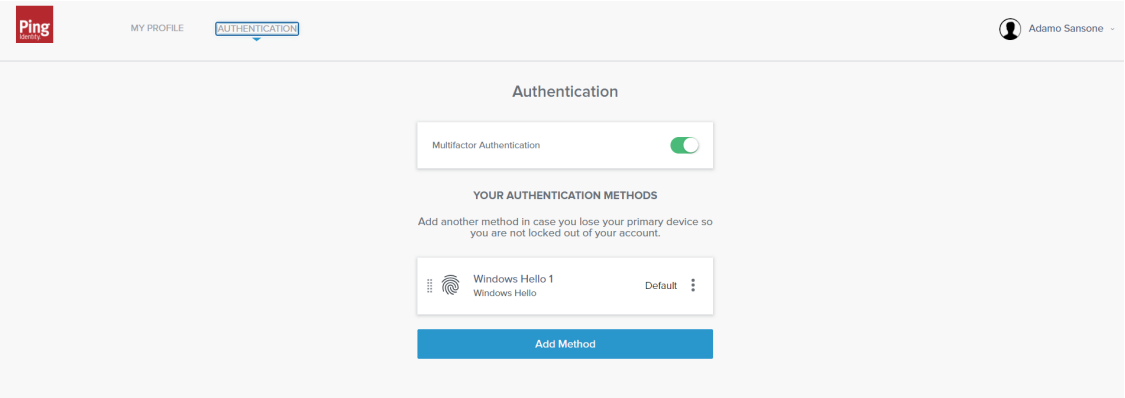

Figura 5.38. Schermata del portale utente per aggiungere un nuovo dispositivo

5.6 Rilevamento dei Rischi

All'interno dell'ambiente sono stati integrati i *predictors*, con il fine di valutare il rischio associato a determinate attività o comportamenti degli utenti e per prevedere possibili minacce o anomalie. Si tratta di strumenti o modelli che possono operare in modo automatico, basandosi su algoritmi di machine learning e intelligenza artificiale o essere configurati manualmente, definendo regole personalizzare o criteri specifici. In particolare, all'interno dei nostri due flussi sono stati inseriti i seguenti predittori(5.39):

- **Velocita IP**: Gli account compromessi possono essere associati a molti indirizzi IP diversi. Se un utente tenta di accedere al proprio account da 4 indirizzi IP diversi in un breve intervallo di tempo, il modello rileva un'anomalia;
- **Dispositivo Sospetto**: Verifica la presenza di impostazioni sospette o discrepanze per rilevare emulatori, macchine virtuali, applicazioni di mirroring o dispositivi manomessi, analizzando vari dati, il sistema operativo, il tipo e la versione del browser, le informazioni sull'hardware e le impostazioni sul dispositivo;
- **Anomalia della Geovelocità**: Controlla che l'intervallo di tempo tra due posizioni di accesso, non sia inferiore al tempo necessario per spostarsi tra i due punti.

- **Anomalia della Posizione dell'Utente**: Definendo un raggio attorno alla posizione dei tentativi di accesso riusciti in precedenza, rileva anomalie se una nuova sessione di login viene aperta da una posizione maggiore del raggio definito nelle impostazioni. Questo per ridurre il rischio di approvazione involontarie di notifiche push e attacchi di acquisizione di account (ATO).

- **Rilevamento di Rete Anonima**: Analizza i dati dell'indirizzo IP dal dispositivo di un utente per rilevare l'utilizzo di una rete anonima, come VPN sconosciute, per mascherare il proprio indirizzo IP.

- **Reputazione dell'IP**: Partendo sempre dall'indirizzo IP, viene effettuata una ricerca per verificare che non sia coinvolto in attività dannose, come attacchi DDoS(*Destributed Denial Of Service*) o attività di spam.

- **Rilevamento dei Bot**: Gli attacchi bot stanno diventando sempre più diffusi e gli autori malintenzionati utilizzano un'ampia varietà di vettori di attacco, dal credential stuffing e dagli attacchi di forza bruta allo spraying di password e agli account falsi. Questo modello rileva comportamenti non umani, strutture automatizzate e registratori analizzando mouse, tastiera, sensori tattili e mobili e attributi del dispositivo.

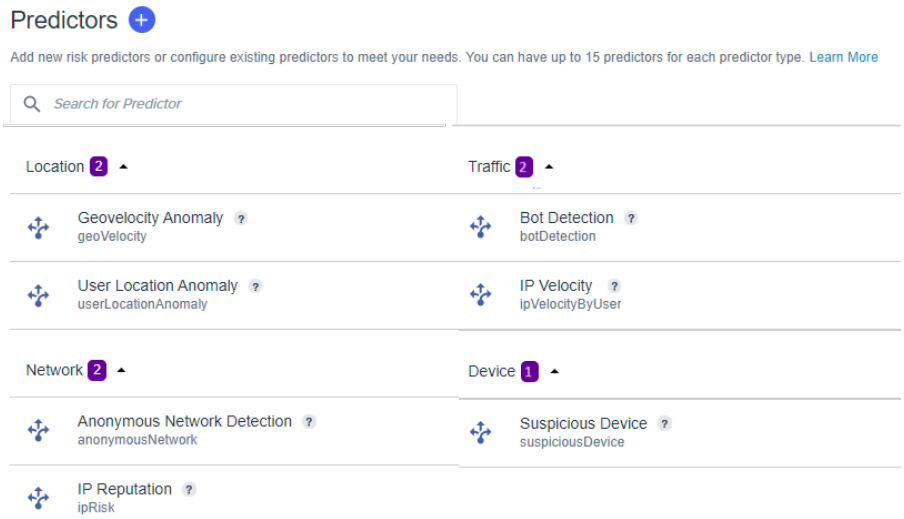

Figura 5.39. Lista dei predittori

Utilizzando questi punti dati, il modello di apprendimento automatico caratterizza l'attività anomala come a rischio basso, medio o alto e richiede all'utente l'azione di autenticazione appropriata. Infatti, è stato possibile definire un valore, associato al livello di rischio corrispondente. Nel caso in cui non ci sono informazioni sufficienti per calcolarlo è stato impostato un valore di fallback. Per quanto riguarda la configurazione dei modelli, in particolare per il rilevamento di rete e anonima e della reputazione dell' IP, si è fatto accesso a siti [13] o gitHub esterni [14], per poter ricavare le "blacklist" degli indirizzi IP, e inserirli in formato CIDR. Invece, nel campo Elenco consentiti, sono stati immessi gli indirizzi IP per i quali le considerazioni sulla rete anonima devono essere ignorate. L'output fornisce un livello di rischio finale, e in base a queste anomalie e alla corrispondente priorità, potrebbe essere richiesto, se è presente, un ulteriore metodo di autenticazione per verificare l'identità dell'utente o, in casi estremi, potrebbe essere necessario bloccare temporaneamente l'account per prevenire possibili violazioni della sicurezza e danni ai dati sensibili.

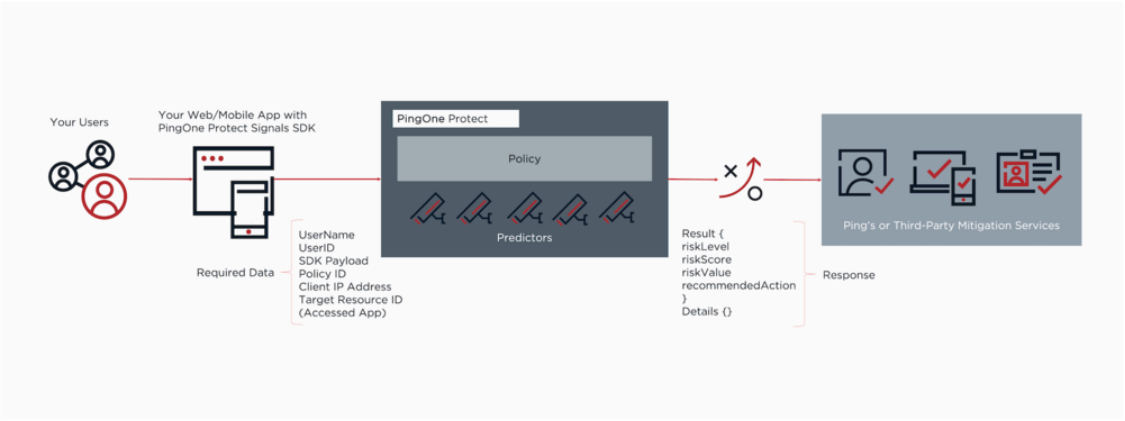

Figura 5.40. Modello di protezione

5.7 Test e Sfide del Laboratorio

Questo capitolo descrive le sperimentazioni condotte nel laboratorio. Testando il progetto, è stato possibile visualizzare ed analizzare i pacchetti inviati e

ricevuti dall'applicazione web. Per fare ciò, è stato utilizzato il software Wireshark [15]. Anche se ogni pacchetto è cifrato, a causa dell'utilizzo di TLS, questo test è comunque stato utile per associare i messaggi ai loro mittenti e destinatari, al fine di generare mappe logiche tra i componenti. Applicando il filtro dell'indirizzo IP, così come quello riguardante il protocollo dei pacchetti, impostato come TLS è stato possibile pulire il test ed avere le informazioni desiderate. I messaggi TLS, come Client Hello, Server hello e Change Cipher Spec sono utilizzati per il processo di handshake. Inoltre, il monitoraggio degli esiti, delle chiamate API e delle variabili in tempo reale si è rivelato utile nel tracciamento sia del flusso di processo e sia nel flusso di dati.

5.7.1 Registrazione

In questa fase, si osserva la comunicazione tra l'applicazione web e il server FIDO2. Inizialmente, la piattaforma invia al server dell'applicazione web messaggi contenenti le informazioni inserite dall'utente nel modulo di registrazione. Si utilizza la versione TLS 1.2 per la comunicazione tra i due server. Dopo l'esecuzione dell'handshake, avviene lo scambio di diversi messaggi di dati applicativi tra i due attori per eseguire il compito di registrazione. Al termine di questa fase, alcuni messaggi vengono inviati dall'applicazione web al dispositivo dell'utente, rappresentando la risposta del punto di accesso. Nella piattaforma, il browser esegue l'API WebAuthn per creare le credenziali, chiedendo all'utente di utilizzare un autenticatore. Al termine di questo processo, il browser invia i dati come risposta al server dell'applicazione web, che può quindi utilizzare tali informazioni per effettuare la chiamata al sever FIDO. Durante questa fase, avviene lo scambio di numerosi messaggi tra i due server. Quando il server dell'applicazione web riceve la risposta completa, invia il risultato al browser(5.18).

5.7.2 Login

Quando l'utente desidera effettuare il login. Qui, come già spiegato, inserisce il proprio nome utente e viene chiamato il server dell'applicazione web. Il primo tipo di messaggi scambiati è di tipo TLS 1.3 tra il browser e il Relying Party. In particolare, il cliente invia le informazioni sul nome utente al server, che ora può procedere a effettuare la chiamata di autenticazione, utilizzando

192.168.1.18	3.124.182.214	TLSv1.2	758	Client Hello (SNI=authenticator.pingone.eu)
3.124.182.214	192.168.1.18	TLSv1.2	1506	Server Hello
3.124.182.214	192.168.1.18	TLSv1.2	1092	Certificate, Certificate Status, Server Key Exchange, Server Hello Done
192.168.1.18	3.124.182.214	TLSv1.2	180	Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message
192.168.1.18	3.124.182.214	TLSv1.2	153	Application Data
192.168.1.18	3.124.182.214	TLSv1.2	1155	Application Data
192.168.1.18	3.124.182.214	TLSv1.2	1542	Application Data
3.124.182.214	192.168.1.18	TLSv1.2	312	New Session Ticket, Change Cipher Spec, Encrypted Handshake Message
3.124.182.214	192.168.1.18	TLSv1.2	107	Application Data
192.168.1.18	3.124.182.214	TLSv1.2	92	Application Data
3.124.182.214	192.168.1.18	TLSv1.2	109	Application Data
3.124.182.214	192.168.1.18	TCP	1506	443 → 63340 [ACK] Seq=4309 Ack=3557 Win=33536 Len=1452 [TCP segment of a reassembled PDU]
3.124.182.214	192.168.1.18	TLSv1.2	304	Application Data
192.168.1.18	162.247.243.29	TLSv1.2	960	Application Data
192.168.1.18	76.223.31.44	TLSv1.2	96	Application Data
192.168.1.18	162.247.243.29	TLSv1.3	780	Client Hello (SNI=bam.nr-data.net)
162.247.243.29	192.168.1.18	TLSv1.3	513	Server Hello, Change Cipher Spec, Application Data, Application Data, Application Data
192.168.1.18	162.247.243.29	TLSv1.3	118	Change Cipher Spec, Application Data
192.168.1.18	162.247.243.29	TLSv1.3	4891	Application Data

Figura 5.41. Cattura su Wireshark della registrazione

URL Di Richiesta:	https://authenticator.pingone.eu/registration/pingid/devices/enrollment
Metodo Di Richiesta:	POST
Codice Di Stato:	200 OK
Indirizzo Remoto:	3.124.182.214:443
Norme Sui Referrer:	strict-origin-when-cross-origin

Figura 5.42. API di registrazione

la versione 1.2 di TLS. Quando il RP riceve la risposta dal server FIDO2, contenente la sfida da risolvere, inoltra questo risultato alla piattaforma. Dopo lo scambio di questi messaggi, all'utente viene richiesto di fornire la soluzione della sfida utilizzando il suo autenticatore: questo passaggio viene eseguito grazie alle API WebAuthn. Successivamente, la risposta dell'autenticatore viene inviata dal cliente al server dell'applicazione web. Quindi, viene chiamata l'API di autenticazione del Server FIDO e vengono scambiati alcuni messaggi. Successivamente, il risultato calcolato Server FIDO viene inviato dal server dell'applicazione web al cliente: in caso di successo, l'utente viene reindirizzato all'interfaccia della Risorsa e, di conseguenza, vengono scambiati alcuni messaggi per consentire la visualizzazione e il funzionamento di questa pagina(5.43).

192.168.1.18	3.124.182.214	TLSv1.2	758	Client Hello (SNI=authenticator.pingone.eu)
3.124.182.214	192.168.1.18	TLSv1.2	1506	Server Hello
3.124.182.214	192.168.1.18	TLSv1.2	1092	Certificate, Certificate Status, Server Key Exchange, Server Hello Done
192.168.1.18	3.124.182.214	TLSv1.2	180	Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message
192.168.1.18	3.124.182.214	TLSv1.2	153	Application Data
192.168.1.18	3.124.182.214	TLSv1.2	1155	Application Data
192.168.1.18	3.124.182.214	TLSv1.2	1542	Application Data
3.124.182.214	192.168.1.18	TLSv1.2	312	New Session Ticket, Change Cipher Spec, Encrypted Handshake Message
3.124.182.214	192.168.1.18	TLSv1.2	107	Application Data
192.168.1.18	3.124.182.214	TLSv1.2	92	Application Data
3.124.182.214	192.168.1.18	TLSv1.2	109	Application Data
3.124.182.214	192.168.1.18	TCP	1506	443 → 63340 [ACK] Seq=4309 Ack=3557 Win=33536 Len=1452 [TCP segment of a reassembled PDU]
3.124.182.214	192.168.1.18	TLSv1.2	304	Application Data
192.168.1.18	162.247.243.29	TLSv1.2	960	Application Data
192.168.1.18	76.223.31.44	TLSv1.2	96	Application Data
192.168.1.18	162.247.243.29	TLSv1.3	780	Client Hello (SNI=bam.nr-data.net)
162.247.243.29	192.168.1.18	TLSv1.3	513	Server Hello, Change Cipher Spec, Application Data, Application Data, Application Data
192.168.1.18	162.247.243.29	TLSv1.3	118	Change Cipher Spec, Application Data
192.168.1.18	162.247.243.29	TLSv1.3	4891	Application Data

Figura 5.43. Cattura su Wireshark del login

URL Di Richiesta:	https://authenticator.pingone.eu/pingid/assets/js/utils/webauthn/webauthn-v22.223.js
Metodo Di Richiesta:	GET
Codice Di Stato:	200 OK
Indirizzo Remoto:	3.120.213.26:443
Norme Sui Referrer:	strict-origin-when-cross-origin

Figura 5.44. API di autenticazione

5.7.3 *Predictors*

L'obiettivo principale di questo processo è valutare l'efficacia del sistema nel rilevare comportamenti anomali e potenzialmente dannosi. Per fare ciò, ho eseguito, dove possibile, una serie di test progettati per attivare specifici predittori, di cui se n'è parlato in precedenza, e osservare come il sistema risponde a tali scenari simulati.

- Test di Velocità IP: Accesso da un numero, maggiore alla soglia impostata, di indirizzi IP diversi in un breve lasso di tempo;

- Test di Dispositivo Sospetto: utilizzo di una chiavetta YubiKey non compatibile;

- Test di Anomalia della Geovelocità: Accesso da posizioni geografiche distanti in tempi brevi;

- Test di Rilevamento di Rete Anonima: Utilizzo di servizi VPN per mascherare l'indirizzo IP e verificare se il sistema rileva l'utilizzo di reti anonime.

In tutti i casi, è stato effettivamente riscontrato che il sistema è stato in grado di rilevare e segnalare le anomalie previste, confermando così l'efficacia dei predittori nel rilevare comportamenti sospetti e potenzialmente dannosi. Un esempio è mostrato nella figura 5.45, e in base allo *score*, il sistema ha richiesto nella fase di autenticazione, un ulteriore fattore (rischio medio) o bloccato l'account(rischio alto).

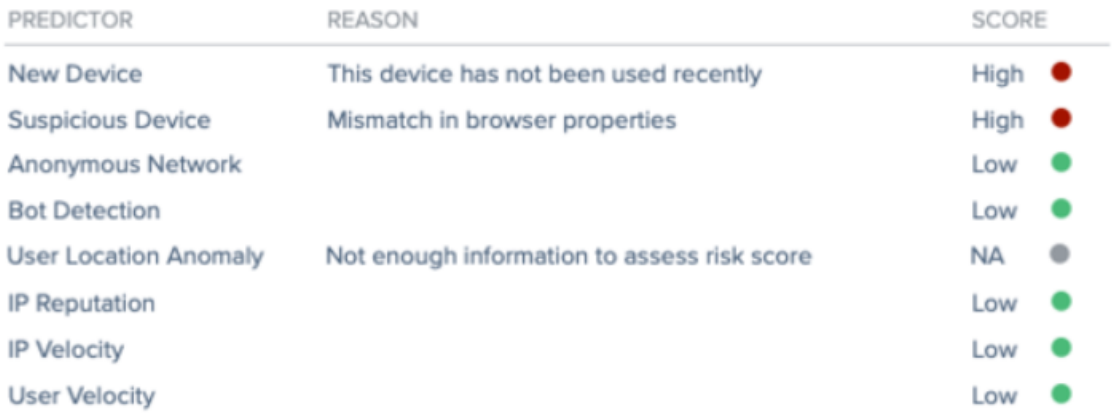

Figura 5.45. Esempio dell'output dei predittori

5.7.4 Sfide

Durante le sperimentazioni, è emerso un aspetto critico dell'autenticazione senza password: la dipendenza da un unico dispositivo. Se da un lato l'autenticazione FIDO offre un livello avanzato di sicurezza e comodità, riducendo il rischio di phishing e di attacchi basati su password rubate, dall'altro lato solleva preoccupazioni riguardo alla perdita o al malfunzionamento del dispositivo stesso. Senza un metodo alternativo di autenticazione, gli utenti potrebbero trovarsi impossibilitati ad accedere ai propri account. Questa situazione ha evidenziato che, nonostante i suoi indubbi vantaggi, l'autenticazione FIDO non dovrebbe essere considerata una soluzione miracolosa

per la sicurezza digitale. Piuttosto, essa rappresenta un componente di un ecosistema di sicurezza più ampio che dovrebbe includere misure di sicurezza complementari, come l'autenticazione a due fattori (2FA). L'integrazione di uno o più autenticatori, offre uno strato aggiuntivo di protezione, assicurando che, anche nel caso in cui un dispositivo di autenticazione vada perso o sia compromesso, l'accesso all'account rimanga protetto da un ulteriore livello di verifica.
La strategia per affrontare la migrazione verso l'autenticazione avanzata ha richiesto un approccio attentamente pianificato. Riconoscendo le potenziali sfide nell'adozione di questa tecnologia, ho scelto di implementare un approccio "soft", offrendo la possibilità di decidere il metodo di autenticazione, consentendo così agli utenti di familiarizzare gradualmente con il nuovo sistema e di comprendere i suoi benefici.

Capitolo 6

Gestione delle Identità e degli Accessi(IAM) nella Migrazione al Passwordless

6.1 Ruolo di IAM

L'Identity and Access Management (IAM) rappresenta una colonna portante nell'ambito dell'Information Technology (IT), svolgendo un ruolo cruciale in ogni strategia di sicurezza informatica. Comprendendo una vasta gamma di tecnologie, l'IAM si articola principalmente in tre aree tecnologiche essenziali:

- **Gestione del Ciclo di Vita degli Utenti e Governance degli Accessi**:Questo aspetto dell'IAM si occupa dell'intera gestione dell'identità di un individuo all'interno di un'organizzazione, dall'ingresso (come nuovo dipendente) fino all'uscita. Include la creazione di account utente, la gestione dei cambiamenti di ruolo o dipartimento, e l'eliminazione degli account quando non più necessari. Attraverso processi noti come JML (Joiner, Mover, Leaver), la gestione del ciclo di vita degli utenti facilita e automatizza queste operazioni;

- **Gestione degli Accessi e Federazione (Access Management & Federation)**:Questa disciplina si concentra sulla gestione dell'accesso ai sistemi in tempo reale. Una volta che un utente possiede un account, è necessario gestirne l'accesso. Ciò comporta processi di autenticazione per verificare che le credenziali fornite, come nome utente e password, siano corrette;
- **Gestione degli Accessi Privilegiati (Privileged Access Management - PAM)**:PAM è un'area tecnica specifica dell'IAM che si occupa della gestione degli utenti con privilegi elevati, come gli amministratori di sistema. Questi utenti hanno accessi critici e richiedono una gestione dedicata per mitigare i rischi associati ai loro elevati livelli di accesso

Architettura

L'architettura dell'IAM si divide in quattro colonne verticali (Amministrazione, Auditing, Autenticazione e Autorizzazione - le quattro "A" di IAM) e tre strati orizzontali, riflettendo le diverse aree di competenza necessarie per una gestione efficace delle identità e degli accessi. La trasformazione digitale sta incidendo profondamente su tutte le aziende, modificando radicalmente il panorama IT. Con il passaggio a modelli basati sul cloud e as-a-service, le organizzazioni stanno offrendo servizi digitali tramite applicazioni e integrandosi con un'ampia gamma di dispositivi. Questo cambiamento nei modelli di business, nelle relazioni con i clienti e nella natura delle partnership commerciali pone le identità digitali al centro delle strategie aziendali. La capacità di gestire e controllare efficacemente l'accesso a tutti i servizi è essenziale per il successo delle iniziative di trasformazione digitale.

6.2 Configurazione di IAM per l'Autenticazione Passwordless

La configurazione dell'Identity and Access Management (IAM) per supportare l'autenticazione passwordless richiede una serie di passaggi strategici e modifiche tecniche per rendere possibile la migrazione. Ecco una panoramica dettagliata dei cambiamenti necessari:

Valutazione dell'Infrastruttura Esistente

- **Analisi dei Sistemi Attuali**: Esaminare le piattaforme, le applicazioni e i sistemi IAM attuali per determinare la loro compatibilità con l'autenticazione passwordless e identificare eventuali limitazioni;
- **Inventario delle Risorse**: Elencare tutte le risorse a cui gli utenti accedono (applicazioni interne, cloud, database, ecc.) per assicurarti che la migrazione passwordless le copra tutte.

Scelta delle Tecnologie Passwordless

- **Selezione dei Metodi di Autenticazione**: Scegliere tra varie opzioni passwordless come biometria, token di sicurezza hardware (ad es., YubiKey), notifiche push, codici QR, ecc;
- **Compatibilità e Standard**: Assicurarsi che le soluzioni scelte siano compatibili con gli standard di settore come FIDO2/WebAuthn per facilitare l'integrazione.

Aggiornamento o Integrazione dell'IAM

- **Piattaforma IAM Flessibile**: Se necessario, aggiornare o sostituire il sistema IAM esistente con una soluzione che supporti nativamente l'autenticazione passwordless o che possa essere facilmente integrata con soluzioni di terze parti;
- **API e SDK**: Utilizzare API e SDK per integrare il supporto passwordless nelle applicazioni e nei servizi esistenti, garantendo una transizione fluida per gli utenti finali.

Implementazione di Politiche di Sicurezza Aggiornate

- **Politiche di Autenticazione**: Definire politiche di autenticazione chiare che includano metodi passwordless, specificando quando e come devono essere usati;
- **Gestione dei Dispositivi**: Implementare politiche per la gestione dei dispositivi utilizzati per l'autenticazione passwordless, inclusa la registrazione, la deregistrazione e la gestione dei dispositivi compromessi.

Formazione e Sensibilizzazione degli Utenti

- **Comunicazione del Cambiamento**: Informare gli utenti sul passaggio all'autenticazione passwordless, i benefici e come la transizione influenzerà il loro modo di accedere ai sistemi.

Test e Validazione

- **Ambiente di Test**: Prima del lancio completo, implementare un ambiente di test per verificare la configurazione passwordless, assicurandosi che tutti i flussi di autenticazione funzionino come previsto.

Monitoraggio e Manutenzione Continui

- **Strumenti di Monitoraggio**: Utilizzare strumenti di monitoraggio e di reporting per tracciare l'uso dei metodi di autenticazione passwordless, rilevare tentativi di accesso sospetti e valutare l'efficacia delle politiche di sicurezza;
- **Aggiornamenti e Patch**: Mantenere aggiornate le soluzioni di autenticazione e l'infrastruttura IAM per proteggere contro nuove vulnerabilità e minacce.

Gestione del Cambiamento e Supporto agli Utenti

- **Supporto IT Proattivo**: Stabilire un team di supporto IT dedicato per assistere gli utenti durante la transizione, rispondendo a domande e risolvendo problemi relativi all'autenticazione passwordless;
- **Feedback degli Utenti**: Creare canali attraverso i quali gli utenti possono facilmente fornire feedback o segnalare problemi, facilitando l'identificazione e la risoluzione rapida delle preoccupazioni degli utenti.

Sicurezza e Conformità

- **Valutazione dei Rischi**: Eseguire regolari valutazioni dei rischi per identificare e mitigare le potenziali minacce alla sicurezza derivanti dall'adozione di metodi passwordless;
- **Conformità Normativa**: Assicurarsi che la soluzione passwordless scelta rispetti le normative locali e internazionali sulla privacy e la sicurezza dei dati.

Scalabilità e Flessibilità

- **Scalabilità dell'Infrastruttura**: Progettare l'infrastruttura IAM per essere scalabile, in modo da supportare l'aumento del numero di utenti e la crescente varietà di metodi di autenticazione passwordless nel tempo;
- **Flessibilità di Implementazione**: Preparare l'infrastruttura per adattarsi a nuove tecnologie di autenticazione che potrebbero emergere, garantendo che il sistema possa evolvere senza necessità di sostituzioni costose.

Integrazione con Altri Sistemi di Sicurezza

- **Sistemi di Threat Intelligence**: Integrare l'autenticazione passwordless con sistemi di threat intelligence per una risposta più rapida e informata alle minacce alla sicurezza.

La migrazione verso un sistema di autenticazione passwordless è un processo complesso che richiede una pianificazione accurata, un'implementazione meticolosa e un impegno continuo per il monitoraggio e il miglioramento. Affrontare queste sfide non solo migliorerà la sicurezza complessiva dell'organizzazione ma offrirà anche un'esperienza utente più fluida e senza attriti. Collaborando strettamente con i fornitori di tecnologia, i team di sicurezza, gli sviluppatori di applicazioni e gli utenti finali, le organizzazioni possono navigare con successo la transizione verso un ambiente più sicuro, efficiente e moderno senza l'uso di password.

6.3 Impatto delle Modifiche IAM sull'Esperienza Utente

L'adozione dell'autenticazione passwordless attraverso l'Identity and Access Management (IAM) influisce notevolmente sull'esperienza utente, introducendo cambiamenti significativi nella modalità di accesso ai servizi e applicazioni. Possiamo osservare una serie di effetti sia positivi che potenzialmente sfidanti e limitanti:

- **Sicurezza Rinforzata**: L'adozione di un approccio IAM passwordless con FIDO2 migliora notevolmente la sicurezza degli utenti. Le

credenziali statiche come le password sono vulnerabili a furti e attacchi di phishing. FIDO2, invece, utilizza metodi basati su crittografia asimmetrica e autenticazione biometrica, che sono molto più difficili da compromettere;

- **Esperienza Utente Semplificata**: L'esperienza utente beneficia enormemente dell'eliminazione delle password. Gli utenti non devono più ricordare complesse combinazioni di caratteri, riducendo la frustrazione e semplificando l'accesso. L'autenticazione diventa un processo rapido, spesso richiedendo solo un'impronta digitale o un riconoscimento facciale;

- **Riduzione dei Costi di Gestione**: Dal punto di vista dell'utente, l'adozione di un sistema passwordless riduce significativamente il tempo speso per la gestione delle password, inclusa la necessità di cambiare periodicamente le credenziali o di recuperare password dimenticate;

- **Disponibilità e Compatibilità dei Dispositivi**: Non tutti i dispositivi utilizzati dagli utenti possono supportare la tecnologia necessaria per l'autenticazione passwordless, come lettori di impronte digitali o telecamere per il riconoscimento facciale. Questo può limitare la possibilità di implementare pienamente un sistema passwordless in ambienti con una vasta gamma di hardware;

- **Gestione dell'Identità in Caso di Perdita o Furto**: Una delle preoccupazioni principali dell'autenticazione passwordless riguarda la gestione dell'accesso in caso di perdita o furto del dispositivo di autenticazione. Senza procedure chiare e sicure per il recupero dell'account, gli utenti potrebbero trovarsi esclusi dai propri servizi;

- **Educazione e Sensibilizzazione**: Affinché l'autenticazione passwordless sia accettata e adottata in modo sicuro, è essenziale un'ampia campagna di educazione e sensibilizzazione per gli utenti. Comprendere i benefici e le procedure corrette è fondamentale per garantire che la transizione migliori l'esperienza utente senza introdurre nuovi rischi;

6.4 Impatto delle Modifiche IAM sull'Azienda

La transizione verso il passwordless influisce soprattutto sull'ecosistema aziendale, portando con sé, vantaggi ma anche sfide e limitazioni che le organizzazioni devono affrontare e gestire. Dall'ottimizzazione dei processi alla necessità di investimenti in formazione e tecnologia, analizzeremo come queste modifiche IAM plasmano il futuro delle pratiche aziendali in termini di sicurezza digitale e gestione degli accessi:

- **Rafforzamento della Sicurezza Aziendale**: L'adozione del passwordless da parte degli utenti implica l'aumento della sicurezza per tutta l'azienda. Inoltre, contribuisce al miglioramento della conformità alle normative sulla privacy e sicurezza dei dati attraverso l'impiego di metodi di autenticazione basati su standard più sicuri;
- **Efficienza Operativa**: La migrazione verso sistemi di autenticazione senza password semplifica notevolmente le operazioni IT, eliminando gran parte delle richieste di assistenza legate al reset delle password. Questo alleggerimento del carico di lavoro consente al personale IT di dedicarsi a compiti più strategici e di valore, ottimizzando l'uso delle risorse aziendali;
- **Sfide nell'Implementazione**: Nonostante i benefici, l'implementazione del passwordless presenta sfide, inclusi gli investimenti iniziali necessari per l'aggiornamento dell'infrastruttura IT e l'acquisto di dispositivi compatibili con FIDO2. La transizione può incontrare resistenze interne dovute alla curva di apprendimento e alla necessità di adeguare le abitudini dei dipendenti ai nuovi sistemi di autenticazione;
- **Limitazioni Operative e di Sicurezza**: La dipendenza da dispositivi specifici per l'autenticazione introduce potenziali vulnerabilità, come il rischio associato alla perdita o al furto di tali dispositivi. Questo aspetto richiede l'elaborazione di piani alternativi efficaci per garantire l'accesso continuato ai servizi in caso di emergenza. Inoltre, la necessità di assicurare la custodia sicura dei dispositivi di autenticazione solleva questioni aggiuntive in termini di gestione della sicurezza fisica e informativa.

Capitolo 7

Ostacoli e Strategie

La transizione verso sistemi di autenticazione passwordless si è affermata come una priorità per le aziende che mirano a rafforzare la sicurezza e migliorare l'esperienza utente. Nonostante i benefici di questa evoluzione siano stati ampiamente discussi e riconosciuti nei capitoli precedenti, la migrazione verso il passwordless non è esente da sfide. Queste non si limitano solo a ostacoli tecnologici ma abbracciano una gamma più ampia di questioni, comprese le resistenze culturali e organizzative al cambiamento.
Senza un approccio globale e studiato, le resistenze al cambiamento e le barriere tecniche possono significativamente rallentare o compromettere il successo dell'implementazione del passwordless. In questo contesto, esploriamo la complessità di questo percorso, delineando gli ostacoli comuni e proponendo soluzioni strategiche per facilitare una migrazione efficace e accettata.

7.1 Sfide per gli Utenti

Questo capitolo si dedica all'analisi degli ostacoli che gli utenti possono incontrare nel passaggio verso sistemi di autenticazione passwordless, affrontando sfide sia psicologiche che pratiche.

Resistenza al Cambiamento

La naturale resistenza al cambiamento rappresenta un ostacolo significativo. Utenti abituati alle password tradizionali possono mostrarsi scettici o preoccupati di fronte a nuovi metodi di autenticazione, temendo complicazioni o

minacce alla sicurezza personale.

Dubbi sulla Sicurezza

Nonostante i vantaggi in termini di sicurezza offerti dal passwordless, persistono dubbi e incertezze, particolarmente riguardo l'impiego di dati biometrici e la loro protezione.

Percezione di Complessità

L'introduzione di tecnologie innovative può apparire come un ostacolo per gli utenti meno tecnologici, che potrebbero considerare il passwordless più difficile da comprendere e utilizzare rispetto all'ingresso di una password.

Questioni di Accessibilità e Inclusività

È fondamentale assicurare che il passwordless sia accessibile a tutti gli utenti, inclusi coloro con esigenze particolari. La preoccupazione è che certi metodi passwordless non siano adatti o fruibili da tutti.

Preoccupazione per la Perdita dei Dispositivi

La dipendenza da dispositivi fisici per l'autenticazione introduce la preoccupazione di perdere l'accesso ai servizi qualora tali dispositivi vengano smarriti o dimenticati.

7.2 Sfide per le Aziende

In questo segmento, esaminiamo invece le sfide che le aziende affrontano nell'adozione di sistemi di autenticazione senza password, evidenziando le complessità organizzative e tecniche. L'implementazione del passwordless, pur portando vantaggi in termini di sicurezza e gestione degli accessi, solleva questioni riguardanti l'impatto sulle infrastrutture IT, sui processi aziendali e sul coinvolgimento del personale.

Investimenti Iniziali e Costi di Implementazione

La transizione al passwordless richiede un significativo investimento finanziario iniziale. Le aziende devono considerare i costi associati all'acquisto di nuove tecnologie, come token hardware FIDO2 o sistemi di riconoscimento biometrico, e alla revisione o sostituzione delle infrastrutture IT esistenti per supportare l'autenticazione senza password. A ciò si aggiungono i costi per la formazione del personale IT e degli utenti finali sui nuovi metodi di autenticazione.

Complessità Tecnologica e Integrazione dei Sistemi

Incorporare soluzioni passwordless in un ambiente IT esistente può presentare complessità tecniche notevoli. Le aziende devono affrontare le sfide relative alla compatibilità dei nuovi sistemi con le infrastrutture e le applicazioni già in uso, assicurando che l'introduzione del passwordless non interrompa i processi aziendali critici. Questo può richiedere un'attenta pianificazione e, talvolta, lo sviluppo di soluzioni personalizzate.

Gestione del Cambiamento Organizzativo

L'adozione del passwordless non è solo una questione tecnica ma richiede anche un cambiamento organizzativo. Le aziende devono gestire la resistenza interna al cambiamento, educando i dipendenti sui vantaggi dell'autenticazione senza password e rassicurandoli sulla sicurezza e l'efficacia dei nuovi sistemi. Questo aspetto può richiedere campagne di comunicazione interne, sessioni di formazione e supporto continuo durante la fase di transizione.

Preoccupazioni sulla Sicurezza e la Privacy

Nonostante il passwordless offra miglioramenti significativi in termini di sicurezza rispetto alle password tradizionali, le aziende possono incontrare preoccupazioni interne riguardo la sicurezza dei dati, in particolare per quanto riguarda la gestione e la protezione delle informazioni biometriche e dei token di autenticazione. È fondamentale che le soluzioni adottate siano conformi alle normative sulla privacy e sulla protezione dei dati, come il GDPR nell'Unione Europea.

Preoccupazione per la Perdita dei Dispositivi

La dipendenza da dispositivi fisici per l'autenticazione introduce la preoccupazione di perdere l'accesso ai servizi qualora tali dispositivi vengano smarriti o dimenticati.

7.3 Strategie per una Migrazione Efficace

L'informazione è il primo passo cruciale nel promuovere l'adozione del passwordless. Un approccio multi sfaccettato può aiutare a raggiungere e coinvolgere l'intera base di utenti:

- **Organizzazione di Seminari e Workshop Interattivi**: Questi eventi servono non solo a presentare il concetto e i benefici dell'autenticazione passwordless ma anche a dimostrarne l'applicazione pratica. Attraverso sessioni interattive, gli utenti possono sperimentare direttamente la facilità e la sicurezza del passwordless, risolvendo i loro dubbi in tempo reale;
- **Sviluppo di Materiale Informativo Approfondito**: Creare e distribuire guide dettagliate, domande frequenti (FAQ) approfondite e video tutorial che coprono vari aspetti del passwordless, dalla configurazione alla quotidiana operatività. Questi materiali dovrebbero essere progettati per essere intuitivi, accessibili da dispositivi mobili e facilmente comprensibili, senza presupporre una precedente conoscenza tecnica
- **Campagne di Comunicazione Continua**: Utilizzare i canali di comunicazione interna, come email, intranet e social aziendali, per mantenere l'autenticazione passwordless un argomento di discussione corrente. Le comunicazioni regolari possono includere aggiornamenti sul processo di implementazione, suggerimenti per una migliore sicurezza digitale e storie di successo di altri utenti o dipartimenti;
- **Condividere Successi e Testimonianze**: Raccontare storie di successo e condividere testimonianze di utenti che hanno già adottato con entusiasmo il passwordless può servire da potente incentivo per altri. Vedere i colleghi adottare e trarre vantaggio dal nuovo sistema può motivare l'intera organizzazione a seguire l'esempio.

Prima di poter convincere gli utenti all'adozione dell'autenticazione passwordless, è essenziale che le aziende stesse integrino e adottino queste soluzioni all'interno dei loro sistemi. Tuttavia, la decisione di passare al passwordless varia significativamente a seconda delle necessità specifiche di ogni organizzazione. Per alcune, l'investimento in questa tecnologia rappresenta un passo strategico verso un aumento della sicurezza e dell'efficienza operativa, mentre per altre, i cui requisiti di sicurezza possono essere soddisfatti con misure meno avanzate, l'adozione potrebbe non giustificare i costi iniziali.
In questo contesto, l'affidarsi a fornitori di terze parti specializzati, quali Ping Identity, si presenta come un'opzione strategica. Questo approccio consente alle aziende di beneficiare dell'expertise e delle infrastrutture avanzate senza dover sostenere l'intero onere finanziario e operativo di un'implementazione interna da zero. I costi associati a queste soluzioni esterne, pur essendo significativi, vengono bilanciati dai vantaggi nel lungo periodo, in termini di sicurezza migliorata, efficienza operativa, riduzione dei rischi e concentrazione sul core business, delineando un chiaro percorso verso un solido ritorno sull'investimento e rendendo l'adozione del passwordless una scelta strategica vantaggiosa.

Capitolo 8

Conclusione

Nei capitoli precedenti è stato esplorato in maniera dettagliata il percorso che ha guidato il lavoro di tesi, iniziando dalla definizione del problema, ovvero il problema dell'utilizzo delle password, per giungere alla progettazione e implementazione di una soluzione passwordless su DaVinci. Da questo percorso è emerso chiaramente come la migrazione verso soluzioni passwordless comporti notevoli benefici, migliorando la sicurezza e l'usabilità per gli utenti finali.

8.1 Punti di Forza

L'uso della piattaforma Ping DaVinci per l'implementazione del passwordless rivela una serie di vantaggi distintivi:

1. **Approccio Low-Code**: La piattaforma offre un ambiente di sviluppo low-code che semplifica notevolmente i processi di implementazione, permettendo agli sviluppatori di concentrarsi sulla logica piuttosto che sul codice, riducendo i tempi di sviluppo;

2. **Documentazione Chiara e Use Cases**: DaVinci mette a disposizione una documentazione ben strutturata e numerosi casi d'uso che guidano gli sviluppatori attraverso vari scenari di implementazione, facilitando l'apprendimento e l'adozione della tecnologia;

3. **Facilità di Personalizzazione**: Grazie alla vasta gamma di personalizzazioni, permette alle aziende di adattare i flussi di autenticazione alle proprie esigenze specifiche senza compromettere la sicurezza o l'esperienza utente.

4. **Adattabilità**: Grazie alla sua flessibilità, DaVinci può essere integrata con diverse applicazioni, rendendola una soluzione versatile per l'implementazione dell'autenticazione passwordless in vari contesti aziendali.

8.2 Limiti e Considerazioni

Nonostante i numerosi punti di forza, l'adozione di DaVinci per l'autenticazione passwordless presenta alcune sfide:

- **Complessità Sottovalutate**: Poiché DaVinci sia specificamente progettato per facilitare l'implementazione di soluzioni IAM, alcune sfide operative non sono state immediatamente evidenti. La natura pronta all'uso del prodotto e la sua efficacia nel rispondere alle esigenze di autenticazione IAM hanno inizialmente mascherare questioni tecniche o limitazioni funzionali.

- **Mancanza di Statistiche sui Flussi**: Un'importante mancanza nell'ambito dell'implementazione è stata la mancata esecuzione di test sui flussi di autenticazione con un gruppo rappresentativo di utenti. Questo approccio avrebbe permesso di analizzare le scelte che gli utenti avrebbero effettuato durante il processo di autenticazione, consentendo di raccogliere feedback dettagliati sulla loro esperienza. L'assenza di questa analisi statistica ha limitato la comprensione approfondita delle preferenze degli utenti e delle eventuali difficoltà riscontrate durante l'autenticazione.

8.3 Sviluppi Futuri

Partendo dalle limitazioni di questo studio, qui di seguito vengono elencate alcune delle tematiche che potrebbero essere affrontate in lavori futuri:

- **Raccolta di Insight e Feedback Utente**: Far testare i flussi al fine di raccogliere feedback preziosi sulla loro esperienza e sulle scelte effettuate durante il processo di autenticazione. In aggiunta, sarebbe utile condurre questionari mirati per valutare il livello di consapevolezza degli utenti sulla sicurezza informatica, i problemi legati all'uso delle password e le loro conoscenze sull'autenticazione senza password. Questi dati avrebbero fornito preziosi insight sulle esigenze degli utenti e sulle loro preferenze, offrendo una base solida per la definizione di strategie più precise e mirate, in grado di soddisfare al meglio le esigenze e le aspettative degli utenti.
- **Sviluppo Autonomo di Soluzioni Passwordless**: Esaminare la fattibilità e le potenziali sfide associate all'implementazione di soluzioni passwordless sviluppate internamente, senza l'ausilio di piattaforme esterne. Questo implica valutare attentamente le risorse, le competenze e le capacità interne dell'azienda per creare e gestire efficacemente un sistema di autenticazione passwordless.

Bibliografia

[1] R. W. Shirey, “Internet Security Glossary, Version 2”, RFC-4949, 2007, DOI: 10.17487/RFC4949

[2] C. Paulsen, R. Byers, “Glossary of Key Information Security Terms”, NIST Interagency or Internal Report (NISTIR) 7298, 2019, DOI: 10.6028/NIST.IR.7298r3

[3] P. A. Grassi, J. L. Fenton E. M. Newton, R. A. Perlner, A. R. Regenscheid, W. E. Burr, J. P. Richer “Digital Identity Guidelines Authentication and Lifecycle Management”, NIST Special Publication 800-63B, 2017, DOI: 10.6028/NIST.SP.800-63b

[4] M. Nieles, K.Dempsey, V. Y. Pillitteri “An Introduction to Information Security”, NIST Special Publication 800-12, 2017, DOI: 10.6028/NIST.SP.800-12r1

[5] “SMB data breach statistics”, Verizon, 2020 [Online]. Available: `https://www.verizon.com/business/resources/reports/dbir/2020/smb-data-breaches-deep-dive/`

[6] H. Poll, “The United States of P@ssw0rd&”, Google, 2019 [Online]. Available: `https://storage.googleapis.com/gweb-uniblog-publish-prod/documents/PasswordCheckup-HarrisPoll-InfographicFINAL.pdf`

[7] “81% of company data breaches due to poor passwords”, TraceSecurity, 2018 [Online]. Available: `https://www.tracesecurity.com/blog/articles/weak-passwords-cause-data-breaches`

[8] “FIDO2” [Online]. Available: `https://fidoalliance.org/fido2`

[9] “FIDO Alliance” [Online]. Available: `https://fidoalliance.org`

[10] “World Wide Web Consortium” [Online]. Available: `https://www.w3.org`

[11] “Ping Identity Portale” [Online]. Available: https://www.pingidentity.com/en.html

[12] “Documentazione PingOne DaVinci ” [Online]. Available: https://docs.pingidentity.com/r/en-us/davinci/davinci_landing_page

[13] “MYIP.MS” [Online]. Available: https://myip.ms/info/whois/192.168.1.1#a

[14] “Documentazione gitHub” [Online]. Available: https://github.com/Conticop/bad-asn-list

[15] “Wireshark” [Online]. Available: https://www.wireshark.org/