SSG
SCAI SOLUTION GROUP

++

Identificazione biometrica e sicurezza: una combinazione vincente

SCAI Solution Group Series.

La scienza biometrica viene in soccorso della sicurezza informatica con sistemi di riconoscimento personalizzati.

Indirizzo

SCAI Solution Group SPA
Via Monte Nero, 73
20135 MILANO
Italia

Contatti

Telefono: 06 904050 04
Email: info@ssgroup.it
Website: www.ssgroup.it
P.IVA: 05348521005

Innoviamo per creare valore

Table of Content
Whitepaper

01.
Contesto di Mercato

01

Nell'era dell'Internet of Things (IoT) e del cloud computing, il concetto di sicurezza informatica è radicalmente cambiato.

Il metodo di accesso online con ID e Password (come unico modello di autenticazione possibile che si è consolidato nel tempo) oggi non è più considerato sicuro per via delle numerose **minacce informatiche** alle quali ogni sistema di accesso pubblico e privato è continuamente esposto.

Oggi, l'identificazione biometrica offre una risposta a questo problema con soluzioni basate sull'utilizzo dell'informatica per il riconoscimento di una persona, sulla base di una o più caratteristiche fisiologiche.

È proprio grazie alla biometria usata quotidianamente dai consumatori e insita nei dispositivi mobili che è possibile autenticare un utente senza dover esportare dati biometrici in modo certo.

02. Lo standard **ISO IEC 27000**

Lo **standard ISO IEC 27000** (*Information Security Management Systems (ISMS) Family of Standards*), definisce l'autenticazione come: "*Il processo tramite il quale viene confermata la veridicità di un attributo parziale o di un'informazione che sostiene di essere vera da parte di un'entità*".

Nello specifico, lo standard ISO IEC 27000 riunisce tutte le **norme internazionali** che hanno l'obiettivo di **proteggere le informazioni**, mantenute ed elaborate da un'organizzazione.

La registrazione e l'autenticazione diventano, quindi, il primo elemento che un utente si trova a dover affrontare nel momento in cui interagisce con il servizio.

Realizzare un **sistema di autenticazione** che sia **usabile** e allo stesso tempo sicuro è un problema complesso da affrontare, a causa della vastità di dispositivi e di servizi che possono essere affiancati a uno specifico applicativo.

L'autenticazione rappresenta un fattore molto determinante nel mondo dell'accesso ai servizi, per questo motivo è importante non trascurare il tema e dotarsi di sistemi di accesso sicuri e validati.

Ma come siamo arrivati fino al riconoscimento biometrico?

Ripercorriamo l'evoluzione dei sistemi di autenticazione, soffermandoci brevemente su ognuno di essi.

CONTINUA

1. Sistemi di autenticazione password-based

Come primo elemento di analisi, andiamo a considerare uno dei sistemi più conosciuti e discussi al mondo: le **password testuali ripetibili**.

Esse rappresentano una chiave d'accesso utilizzabile più volte, formata da caratteri alfanumerici. Solitamente si usa per accedere in modo esclusivo a una risorsa informatica.

Il sistema di autenticazione *password-based* risulta tra quelli più considerati e utilizzati. In parte, ciò dipende dal processo che inizialmente era ritenuto molto semplice dall'utente finale, ma poi si è rivelato un processo complesso nel momento in cui l'utente non ricorda o sbaglia la password. Inoltre questa può essere facilmente rubata od indovinata da un hacker (per esempio: se vengono memorizzate nel browser o salvate sul pc) e non è stata costruita in modo "robusto".

Da questo sistema password-based si è poi passati alla One Time Password, vediamo nello specifico di cosa si tratta.

2. One-Time Password

L'**OTP** agisce attraverso un meccanismo di password testuali la cui validità è legata al suo utilizzo. Dopo che sarà adoperata, infatti, essa non potrà più essere riutilizzata, rendendo quindi del tutto inefficace il replay della stessa password e *sniffing attack*.

Affinché il sistema funzioni, è necessario che client e server siano perfettamente sincronizzati tra loro, altrimenti non sarà possibile autenticarsi.
L'avvento di internet ha aumentato la consapevolezza dei suoi utilizzatori, i quali hanno compreso che non c'era nessuna garanzia, né sicurezza in merito alle informazioni scambiate.

Con il diffondersi della rete Internet, come mezzo di comunicazione oltre che di informazione, è aumentata anche la coscienza da parte dei suoi utilizzatori sul fatto che i meccanismi da questa usati per il trasporto delle informazioni da un sito all'altro, non garantiscono la benché minima garanzia sulla confidenzialità e integrità delle stesse.

Da qui nasce, quindi, l'esigenza di creare un nuovo sistema di autenticazione che semplifichi l'accesso anche per l'utente.

Le esigenze delle persone oggi sono radicalmente cambiate, perché la vita in generale è diversa. Oggi i cellulari sono diventati oggetti insostituibili, perché con essi svolgiamo più azioni contemporaneamente, da qui il sistema del **SMS Authentication**.

3. SMS Authentication

Il cellulare è divenuto ormai uno strumento di uso comune. L'idea di utilizzarlo come mezzo di ricezione di un **sms**, che potesse servire per l'autenticazione, ha semplificato di molto il metodo di accesso.
Tuttavia questa modalità non è riuscita ad ovviare al problema di sicurezza. Da qui è nato poi il sistema **Multi Factor Authentication**.

4. Multi Factor Authentication

A fronte dell'iniziale utilità, tutti i precedenti sistemi di autenticazione si sono rivelati fallaci nel lungo periodo. Nonostante questo, sono comunque riusciti a portare a un'innovazione importante, che è alla base del sistema **Multi Factor Authentication**.

In risposta alle lacune dei precedenti sistemi di autenticazione, infatti, è stato sviluppato un sistema con nuove funzionalità, in grado di:

SEMPLIFICARE LA USER EXPERIENCE

MANTENERE ELEVATO IL GRADO DI SICUREZZA

La **Multi Factor Authentication (MFA)**, o autenticazione a più fattori, è quella tecnologia che permette di riconoscere, attraverso più di due metodi di autenticazione, la persona che effettua l'accesso a un sistema o a un'applicazione.

Il sistema è pensato per offrire un'autenticazione senza l'utilizzo di uno username, password, One Time Password (OTP) o qualsiasi forma di segreto condiviso.

Prima che la MFA prendesse il sopravvento, potevamo limitarci all'autenticazione a 2 fattori, ovvero alla combinazione tra qualcosa che conosci (la tua password) e qualcosa che hai (un token, una app, ecc).
L'MFA aggiunge un **ulteriore livello di protezione** al processo di autenticazione. Durante l'accesso ad account o app, gli utenti eseguono verifiche dell'identità aggiuntive, come la scansione dell'impronta digitale o l'immissione di un codice, il tutto attraverso l'utilizzo del proprio smartphone e senza una vera e propria password.

In questo modo, non ci sono password che possono trapelare o essere rubate. Tutte le tecniche per ottenere le credenziali e bypassare il sistema, come *credenziali stuffing*, *rainbow table*, *keylogging* e *replay attack*, risultano perciò inutili.

Il sistema di autenticazione a più fattori ha permesso a **SSG** di ragionare su di una soluzione specifica, in grado di soddisfare i criteri di sicurezza necessari, oggi, per rispondere alle esigenze del mercato informatico.

>>>

03. L'offerta di SSG **per una sicurezza all'accesso avanzata**

40 password al giorno

Mediamente, in un giorno scriviamo oltre 40 password. Spesso capita che non ci ricordiamo alcune di queste e i sistemi al terzo tentativo, per esempio, ci blocchino l'accesso.

Alla fine siamo costretti ad innescare tutto il sistema automatico (e a volte manuale) per il reset della password. Questo processo al lavoro coinvolge, quindi, non solo l'utente finale, ma anche un gruppo che gestisce le utenze per accessi, magari, su sistemi critici.

Se poi non viene utilizzata all'interno della società una *policy* per una costruzione corretta della password (lunghezza, complessità, periodo del cambio password forzato, ecc), i rischi di un accesso fraudolento si moltiplicano e non solo: si incorre anche al pericolo di non essere *compliant* ad alcuni requisiti/standard/regolamentazioni a livello nazionale o mondiale.

Tutte queste problematiche vengono risolte con la **soluzione offerta da Transmit Security**, dove l'accesso viene eseguito in maniera "fluida".

La soluzione è pronta per l'uso, scalabile e semplice da implementare, perché non richiede modifiche infrastrutturali. Ma, soprattutto, una tecnologia che garantisce:

- Un'esperienza utente ottimale;
- Una forte autenticazione tramite la biometria.

Transmit Security (https://www.transmitsecurity.com/) è stata fondata nel 2014 con l'obiettivo di cambiare l'approccio di sicurezza dell'identità. Ha continuamente sviluppato e trovato modi nuovi e innovativi per soddisfare le esigenze dei clienti, tenendo d'occhio la continua evoluzione del mondo cyber.

È presente in uffici di tutto il mondo - come ad esempio a Boston, Londra, Berlino, Tel Aviv, Tokyo, Hong Kong, Madrid, San Paolo e Città del Messico - e collabora con alcune delle più grandi e innovative aziende globali e aziende Fortune 500, per mantenere il loro stack di identità sicuro e scalabile.

La **soluzione di autenticazione MFA** offerta da **Transmit Security** introduce il concetto **"passwordless authentication"**, un elemento essenziale per snellire le procedure di accesso e semplificare al massimo la user experience dell'utente.

Quest'ultimo riscontra spesso difficoltà nel gestire e memorizzare le proprie password per accedere ai tanti sistemi che consentono, giornalmente, di effettuare pagamenti, leggere le email, accedere al conto bancario o all'intranet aziendale, ecc.

Oltre a questi servizi informatici di quotidiano utilizzo, si aggiungono anche gli accessi a tutti i software e applicativi a cui un dipendente deve poter fare accesso in modo sicuro in azienda per il suo lavoro. La soluzione di SSG risponde in maniera efficace a tutte queste esigenze.

Di seguito riportiamo alcuni importanti Use Cases in diversi settori per comprendere meglio applicabilità e vantaggi di questa tecnologia.

Use Cases: mondo bancario

Seppur le banche siano state le prime ad innalzare il livello di sicurezza al loro interno, l'accesso ai loro sistemi offerti alla clientela è stato sempre un nodo cruciale. Troppo spesso, infatti, si è letto di attacchi hacker non solo ai conti dei propri clienti, ma anche mirati all'intera infrastruttura.

Il tutto portato a termine essenzialmente attraverso il bypass dell'autenticazione, utilizzando metodi inizialmente basati su *brute force attack*, cioè dei veri e propri tentativi di utilizzo di password randomiche, attraverso degli strumenti automatici che utilizzano parole del dizionario.

Evolvendo la loro infrastruttura al proprio interno e utilizzando anche dei corsi mirati ai propri dipendenti, le banche hanno innalzato il livello di sicurezza.
Non si può dire però che lo stesso approccio abbia funzionato con la clientela, che spesso utilizza password molto semplici proprio per la difficoltà nel ricordare.

La soluzione Transmit aiuta il cliente ad un accesso rapido, attraverso il **face recognition** o il **finger print recognition** mediante il proprio cellulare. Il **riconoscimento biometrico** aiuta non soltanto la banca, ma anche l'utente nel far sì che utilizzi i propri servizi più frequentemente per le operazioni di pagamento.

Use Cases: Real Estate

Utilizzare un numero importante di agenti per un'azienda immobiliare mette a rischio le informazioni della propria clientela. I dati dei clienti sono contenuti all'interno di sistemi che possono essere fisici o in cloud.

"I dati personali sono tutte le informazioni relative a una persona vivente identificata o identificabile. Anche le varie informazioni che, raccolte insieme, possono portare all'identificazione di una determinata persona, costituiscono i dati personali."

Tali informazioni potrebbero essere rivendute e messe sul mercato da parte di malintenzionati, per questo motivo SSG ha pensato a un'alternativa che realmente sia in grado di garantire sicurezza.

La **soluzione Transmit** offre l'accesso sicuro ai dati da parte degli agenti ed evita una possibile "**fuoriuscita di dati**".

Use Cases: reti di vendita

Con le app presenti sui cellulari, le reti di vendita raccolgono moltissime informazioni dei propri clienti e permettono anche l'utilizzo dell'e-commerce attraverso piattaforme che richiedono, essenzialmente, solo l'utenza e password dei clienti stessi.

Viene concentrata la sicurezza sulle transazioni di acquisto, ma spesso non viene applicata la stessa attenzione nel momento della richiesta di accesso. Gli stessi clienti, spesso, sono scoraggiati per i tentativi di accesso che non vanno a buon fine a causa di password errate.

Questa situazione frustrante per i clienti causa minor guadagno per le reti di vendita, piccole, medie o grandi.

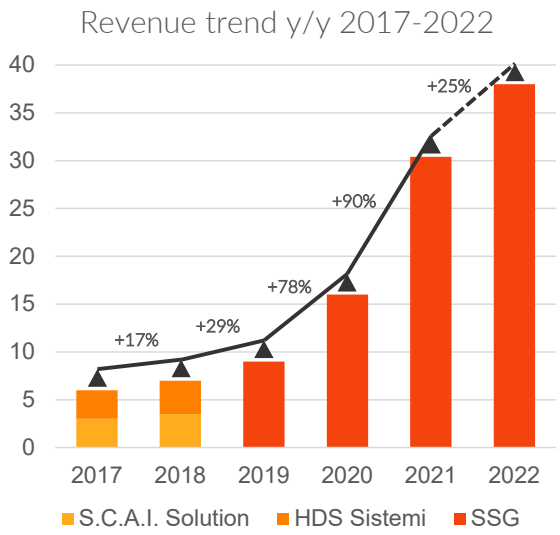
Anche in questo caso, la **soluzione Transmit** aiuta e supporta le aziende alla **fidelizzazione del cliente e agli acquisti** tramite l'e-commerce, che in Italia nel 2020 ammontava a 48,25 miliardi di euro.

SCAI Solution Group
Chi siamo

System Integrator (leader in Italia) che offre consulenza, soluzioni e servizi alle imprese che intendono attuare l'innovazione di processo investendo in tecnologie innovative abilitanti.

Nasce dall'unione delle società S.C.A.I. Solution e HDS Sistemi, che vantano un'esperienza consolidata nel mercato ICT.

La proposizione di SSG si sviluppa attorno a tre verticali di offerta nelle aree **Digital, Cyber Security** e **Datacenter per ICT**. I principali mercati di riferimento sono *Finance*, *Telco*, *Central & Local PA* e *Poste*.



ROMA
Sede legale, operativa e amministrativa

MILANO
Direzione e sede operativa

TORINO
Sede commerciale

40+ personale altamente qualificato in ogni settore di attività

15+ consulenti e sales
10+ architetti e specialisti IT
10+ management e practice leader

VISION

» Affermarsi come interlocutore di riferimento del mercato italiano cui rivolgersi per **soluzioni e servizi a valore aggiunto**, innovazione ed infrastrutture fruibili e abilitanti del business delle aziende.

» Diventare un **player influente e di rilievo** sul mercato italiano in grado di guidare il mercato verso un **cambiamento culturale ed infrastrutturale** attraverso l'applicazione degli standard qualitativi più elevati.

» Distinguersi dalla concorrenza per l'**esperienza del management, del reparto tecnico e della forza commerciale**.

MISSION

» Accompagnare i Clienti nell'**innovazione di processo** grazie alle competenze, alla conoscenza del mercato ed agli investimenti su risorse umane altamente qualificate.

» Offrire **consulenza strategica** e competenze tecniche consolidate per assicurare crescita, efficienza e contenimento dei costi.

» Operare anche attraverso **collaborazioni con partner tecnologici** selezionati fra i migliori del mercato.

SCAI Solution Group
La nostra offering

Le competenze verticali delle Business Unit in cui la nostra organizzazione è specializzata ci consentono di esprimere un valore sul mercato concreto e misurabile.

DIGITAL

Servizi e tecnologie digitali volti sia all'**efficientamento dei processi aziendali** "standard" che di quelli più innovativi, **estendendone la "reach"** attraverso la loro **remotizzazione**.
Grazie ai più recenti e innovativi approcci di **customer engagement**, è possibile esaltare **l'efficacia dei processi** attraverso un'**interazione fra utenti/clienti e sales assistants.**
La soluzioni spaziano dalla Firma Digitale Remota alla Video Conference Avanzata, dalla gestione dei processi di Onboarding della clientela alla digitalizzazione degli asset aziendali.

ICT

La **gestione dei carichi** sui Data Center, la garanzia di un'efficente infrastruttura di **Disaster Recovery** e la sua relazione con i corretti livelli di **Business Continuity**. L'ottimizzazione delle soluzioni in relazione alle politiche di **Information Lifecycle Management**, progetti di integrazione e sviluppo applicativo per offrire un elevato livello di **qualità e continuità del servizio** anche per le attività più critiche.
Questo fa di SSG un partner privilegiato per pianificare le scelte chiave per l'**evoluzione tattica e strategica dei centri informatici** dei nostri clienti.

CYBER SECURITY

La Sicurezza Integrata per potenziare la difesa del Valore.

- Protezione del dato Aziendale
- Difesa dell'Identità e dell'Immagine
- Sicurezza del Perimetro della Rete
- Controllo dell'accesso ai Sistemi
- Continuità del Business
- Monitoraggio degli Eventi
- Prevenzione degli Incidenti

SSG offre **assessment di sicurezza** professionali, disegna **progetti integrati** e fornisce le **migliori soluzioni tecnologiche a protezione** degli asset aziendali.

Professional Services

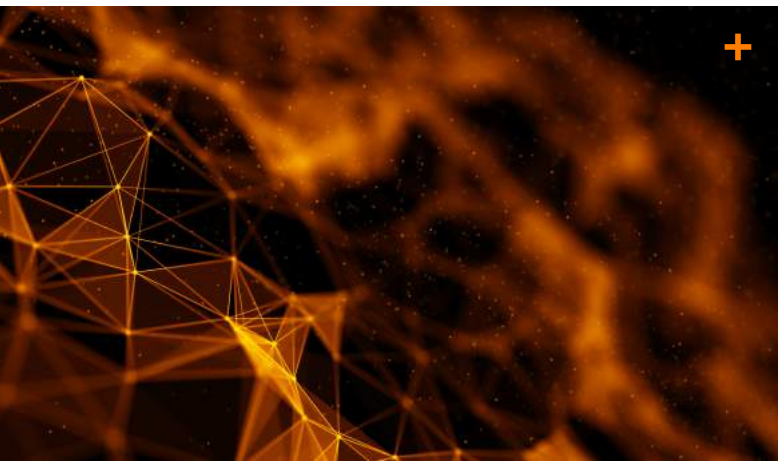
Dalla piccola media impresa sino alle più importanti realtà bancarie, telco e energy, **i Professional Services SSG hanno le competenze necessarie per tramutare un progetto in realtà**. Grazie alle competenze e alle soluzioni proprie delle tre BU, siamo in grado di offrire una visione di livello superiore e implementare servizi verticali, massimizzando il contributo che l'integrazione di ogni singola practice di SSG può fornire.

Approccio metodologico					Standard ISO		
PMI	AGILE	SIX SIGMA	SCRUM	KANBAN	9001	20000	27001

SCAI Solution Group SpA

Innoviamo per creare valore.

SCAI Solution Group



Identificazione biometrica e sicurezza: una combinazione vincente

www.ssgroup.it