Multifactor Authentication con notarizzazione su blockchain

Torino, 3 Dicembre 2020

Alessandro Vassallo (ISP)
Aristide Piazza (PwC)

Il Gruppo Intesa Sanpaolo

Leader italiano di dimensione europea

Il Gruppo Intesa Sanpaolo è uno dei **primi gruppi bancari in Europa,** con una capitalizzazione di mercato di 31,1 miliardi di euro, ed è impegnato a sostenere l'economia dei Paesi in cui opera, in particolare in Italia dove si impegna anche a diventare un riferimento in termini di sostenibilità e responsabilità sociale e culturale.

Intesa Sanpaolo è **leader in Italia in tutte le aree di business** (retail, corporate e wealth management).

Il Gruppo offre i propri servizi a **19 milioni di clienti attraverso una rete di oltre 4.700 filiali** ben distribuite su tutto il territorio nazionale con quote di mercato non inferiori al 12% nella maggior parte delle regioni italiane.

Intesa Sanpaolo **ha altresì una presenza internazionale strategica, con circa 1.000 sportelli e 7,2 milioni di clienti**, incluse le banche controllate operanti nel commercial banking in 12 Paesi in Europa centro-orientale e in Medio Oriente e Nord Africa e una rete internazionale specializzata nel supporto alla clientela corporate in 25 Paesi, in particolare nel Medio Oriente e Nord Africa, e in quelle aree in cui si registra il maggior dinamismo delle imprese italiane, come Stati Uniti, Brasile, Russia, India e Cina.

4.719 Filiali	19 mln Clienti
31 bln Capitalizzazione	~90 k Impiegati

Il team di cybersecurity di Intesa Sanpaolo

Un gruppo di professionisti con presidio internazionale

Gruppo Intesa Sanpaolo ~ 350

Capogruppo ~ 160	Legal Entities ~ 110	UBI Banca ~ 80

La strategia cyber di Intesa Sanpaolo

Un approccio basato su quattro pilastri, a fondamento della roadmap di Gruppo

Garantire che le attività fondamentali per la cybersecurity abbiano **livelli di presidio eccellenti**

Essere in grado di cogliere il più velocemente possibile i **segnali deboli di possibili situazioni d'attacco**

Awareness e cyber culture, formazione, pillole comunicative e esercitazioni come **fattori abilitanti per l'approccio Security by design**

Accrescere i livelli di cyber resilience e cyber readiness dell'intero Gruppo con un **presidio unico su tutte le realtà**

Fondamentali… il controllo accessi in era Covid

L'emergenza Covid-19 ha fatto registrare un incremento esponenziale degli accessi da remoto e parallelamente sulla scena internazionale un aumento dell'incidenza degli attacchi tramite i medesimi canali

120.000+

Persone interne e collaboratori

Il Gruppo Intesa conta un numero di collaboratori interni ed esterni in costante crescita, in Italia e nel mondo, e l'integrazione di UBI Banca ha dato e darà ulteriore spinta a questo trend.

85.000+

Accessi remoti giornalieri

La diffusione dello smart working come modalità di lavoro prevalente, ha aumentato del 1200% il numero di accessi giornalieri al sistema informativo, tramite i canali di accesso remoto, da parte delle persone interne e dei collaboratori, sparsi in tutto il mondo.

È divenuto necessario accelerare il processo di adozione della 2FA (iniziato nel 2017) per l'accesso ai sistemi critici e remoti, per…

Ridurre i rischi di intrusione o frode interna, derivanti da sottrazioni di credenziali di autenticazione.

Ottenere la compliance con vincoli normativi.

Migliorare i livelli di sicurezza, semplificando al massimo la user experience.

Avviare di un percorso di evoluzione verso il paradigma della Risk Based Authentication.

La soluzione di 2FA del Gruppo Intesa Sanpaolo

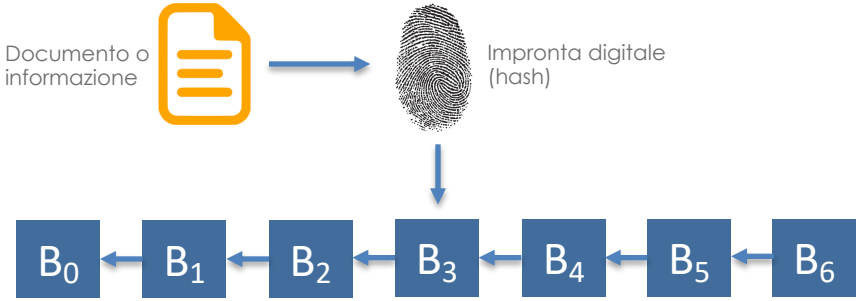
La soluzione introdotta dal Gruppo Intesa Sanpaolo è stata sviluppata internamente in collaborazione con PricewaterhouseCoopers consentendo un controllo completo della filiera, scalabilità di costi e completa personalizzazione

- **App e sistema proprietari** sviluppati in-house
- Autenticazione basata su **firma digitale** tramite autorizzazione di notifiche push
- User experience **frictionless**, in analogia con quella pensata per i Clienti.
- **Unica soluzione** per tutti i workflow di autenticazione ai sistemi critici ed ai canali remoti
- **Marcatura temporale** degli eventi di autorizzazione su **blockchain** (in corso)

Marcatura temporale su blockchain

Come usare una blockchain per la marcatura temporale?

Una blockchain è formata da una sequenza ordinata di blocchi, creati ad intervalli regolari, non modificabili, ciascuno dei quali contiene un timestamp (data/ora in cui è stato creato)



Il risultato è che tutte le informazioni contenute all'interno di un blocco sono automaticamente marcate temporalmente

Marcatura temporale: TSA vs Blockchain

Principali differenze tra i due approcci alla marcatura temporale

Timestamping PKI-based (TSA)

- **Necessita di una terza parte**, la Timestamping Authority (TSA) che, utilizzando un certificato digitale, firma una marca temporale contenente l'impronta digitale del documento e la data/ora corrente.
- Il meccanismo basato su firma digitale implica la necessità di custodire chiavi private (rischio).
- **Esiste un framework legale** che inquadra questo processo.

Timestamping su blockchain

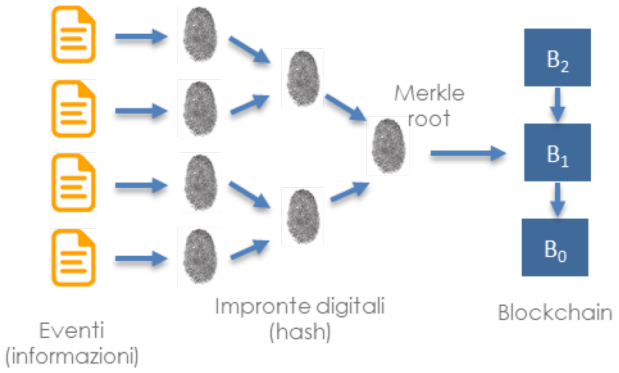
- **Non necessita** di una terza parte
- Non essendo basato su firma digitale, non è esposto a rischi di compromissione delle chiavi private.
- Il framework legale che inquadra questo processo è in corso di definizione (L. 11 febbraio 2019, n. 12).

*La notarizzazione su blockchain è uno dei casi d'uso sviluppati sulla **European Blockchain Services Infrastructure** (EBSI)*

Un approccio al problema della scalabilità

I limiti di scalabilità vengono superati aggregando più eventi (informazioni) e notarizzando, ad intervalli di tempo regolari, l'impronta digitale risultante da ciascuna aggregazione (merkle root).

- E' possibile effettuare un **numero arbitrariamente grande** di marcature temporali anche in un intervallo di tempo ridotto.
- A valle della scrittura in blockchain, viene rilasciata una ricevuta contenente tutti i passaggi di hashing effettuati partendo dall'informazione iniziale fino ad arrivare alla transazione scritta nel blocco.
- La ricevuta, insieme all'informazione originale, permettono di dimostrare l'esistenza dell'informazione alla data di creazione del blocco.



Conclusioni

1. L'introduzione di un secondo fattore di autenticazione per gli accessi da remoto ed ai sistemi critici comporta un cambio di paradigma completo con un forte impatto sugli utenti interni e sui collaboratori esterni. Per questo motivo occorre prestare particolare attenzione a:
   - Effettuare intense e puntuali campagne di comunicazione verso tutte le strutture coinvolte in modo da gestire al meglio la naturale resistenza al cambiamento.
   - Istruire nuovi processi per la gestione dell'abilitazione del secondo fattore, della disabilitazione e della deroga per poter affrontare i casi di eccezione temporanea o prolungate.
   - Intervenire sui modelli contrattuali con i fornitori per includere le necessarie clausole riguardanti le nuove modalità di accesso.
2. L'utilizzo di una blockchain per effettuare la marcatura temporale di eventi di autorizzazione (anche su grandi volumi) fornisce un importante contributo per migliorare la sicurezza applicativa e gestire possibili futuri requisiti di compliance e normativi eventualmente anche in altri contesti.