Il futuro dell'Identità Digitale e della Digital Integrity

Aruba Wallet, per una nuova infrastruttura europea di fiducia.



pulse

aruba.it



L’Europa si sta muovendo verso un modello unificato di identità digitale, in cui i wallet digitali diventano l’interfaccia di riferimento per il trust, la conformità normativa e le interazioni transfrontaliere.

In questo scenario, Aruba si propone come single point of trust, integrando identità digitale, servizi fiduciari qualificati e infrastrutture europee all’interno di un’architettura nativamente predisposta per l’ecosistema wallet.

In tale contesto, il wallet non rappresenta soltanto uno strumento operativo: diventa il **livello di controllo** attraverso cui la fiducia digitale viene verificata, governata e scalata su tutto l’ecosistema europeo.

Sommario

01 | **Introduzione: trend attuali e contesto di riferimento** 4

02 | **Minacce e opportunità** 7

03 | **Il posizionamento di Aruba** 10

04 | **Logica di portafoglio e architettura delle soluzioni** 12

05 | **Prospettive future dell'identità digitale** 17

CAPITOLO 01

Introduzione: trend attuali e contesto di riferimento

L'Europa sta entrando in una nuova fase di maturità digitale, in cui l'identità non è più un semplice meccanismo di accesso, ma si afferma come componente strutturale di fiducia, governance e controllo operativo.

Per le imprese, questa evoluzione genera al tempo stesso pressioni e opportunità. Il quadro regolatorio si fa più stringente, il rischio cyber cresce e i sistemi sono sempre più interconnessi. Parallelamente, un nuovo paradigma dell'identità offre la possibilità di ridurre resistenze, rafforzare la responsabilità e abilitare nuove modalità di interazione digitale.

Per oltre un decennio, la trasformazione digitale è stata guidata da esigenze di rapidità e scala. Le organizzazioni hanno adottato il cloud, automatizzato i processi e connesso sistemi in ambienti sempre più articolati.
L'identità digitale è evoluta in parallelo a questo cambiamento, ma non con una logica unificante. È rimasta frammentata, modellata su schemi nazionali, vincolata a singole piattaforme e spesso progettata per casi d'uso specifici, anziché con un programma sistemico. Questo approccio presenta chiaramente dei limiti.

Gli ambienti digitali contemporanei sono, per natura, distribuiti. Le aziende operano su infrastrutture ibride, piattaforme SaaS, API, dispositivi connessi e sistemi sempre più supportati dall'Intelligenza Artificiale. Il perimetro tradizionale si è dissolto e ogni interazione, umana o automatizzata, richiede processi di verifica continui e affidabili.

La fiducia digitale è, di fatto, sempre più complessa da sviluppare e mantenere: i deepfake compromettono l'autenticità, le frodi identitarie si amplificano attraverso l'automazione e gli ecosistemi digitali articolati riducono la tracciabilità delle responsabilità. Non si tratta di un fenomeno contingente, ma di una trasformazione strutturale. I sistemi devono dimostrare la propria integrità e, in questo contesto, l'identità digitale diventa il meccanismo attraverso cui le organizzazioni attestano chi sta operando, con quale livello di autorizzazione e all'interno di quali confini legali e operativi.

La regolamentazione europea riflette questa evoluzione. Framework normativi come eIDAS 2.0, NIS2, GDPR, DORA e AI Act stanno ridefinendo i criteri con cui i sistemi devono essere progettati. **La fiducia non può più essere un elemento aggiuntivo: deve essere incorporata nell'architettura tecnologica**, mentre la responsabilità deve risultare tracciabile per impostazione predefinita.

L'European Digital Identity Wallet rappresenta un elemento centrale di questa transizione. Entro la fine del 2026, ogni Stato membro dovrà mettere a disposizione un wallet digitale che consenta ai cittadini di conservare e collettare credenziali, condividere soltanto i dati necessari e firmare con pieno valore legale. Questo modello si estende anche alle organizzazioni attraverso i Digital Business Wallet, accessibili sia come piattaforme web sia come applicazioni dedicate. Tali soluzioni integrano l'identità nei processi aziendali mediante autorizzazioni, credenziali e notifiche con validità legale, le Qualified Electronic Registered Delivery Services (QeRDS).

Si afferma così un nuovo paradigma: l'identità digitale evolve da funzione tecnica a infrastruttura portante dell'ecosistema europeo, diventando la **dorsale su cui si fonda la fiducia in ogni transazione e in ogni interazione digitale**.



Wallet pubblici e wallet privati: uno standard comune, ruoli distinti

I wallet digitali pubblici, emessi sotto il controllo degli Stati membri in conformità con eIDAS 2.0, offrono ai cittadini uno strumento sicuro e interoperabile per la gestione dell'identità e delle credenziali digitali. Consentono autenticazione, condivisione selettiva di attributi verificati e firme digitali con pieno valore legale, sia nei servizi pubblici sia in quelli privati, garantendo al contempo il rigoroso rispetto dei principi di privacy e minimizzazione dei dati.

I wallet pubblici definiscono un livello di identità affidabile e interoperabile su scala europea, con un focus su identità ad alto livello di garanzia e casi d'uso prevalentemente legati alla PA, con un set di credenziali interoperabili circoscritte.

I wallet privati estendono lo stesso paradigma agli ambienti enterprise, supportando processi B2B, B2C e B2E.

Basati sulle medesime fondamenta tecnologiche e regolatorie, si integrano nelle applicazioni aziendali e nei flussi operativi, consentendo alle organizzazioni di gestire interazioni con clienti e dipendenti, autenticazione e accesso ai servizi all'interno dei propri ecosistemi digitali. Il valore distintivo dei wallet privati risiede nella capacità di rendere l'identità un elemento operativo nei processi di business concreti, ampliando l'insieme delle credenziali fino a includere tutti i dati necessari per specifiche transazioni. Possono inoltre incorporare funzionalità di identity proofing con livelli di garanzia calibrati sul contesto d'uso, migliorando l'esperienza utente e riducendo le resistenze in fase di adozione. Un ulteriore elemento strategico è la loro interoperabilità con i wallet pubblici.

L'opportunità strategica consiste nel superare la logica del wallet unico per adottare un modello di fiducia multilivello.
I wallet pubblici costituiscono il punto di riferimento per identità ad elevata garanzia e giuridicamente riconosciute, a supporto dei rapporti tra cittadini e PA e dei casi d'uso transfrontalieri.

Parallelamente, i wallet privati possono rendere operativi gli stessi standard nei percorsi enterprise, nelle relazioni con i clienti e nelle esperienze dei dipendenti, modulando i livelli di assurance in funzione del rischio associato a ciascuna transazione.

Questo approccio consente di preservare la riservatezza attraverso meccanismi di selective disclosure e principi di minimizzazione dei dati, favorendo al tempo stesso l'interoperabilità tra ecosistemi differenti, senza imporre a tutti i casi d'uso un unico profilo identitario definito dallo Stato, per una maggiore sicurezza e un crescente tasso di adozione.

Il risultato è un equilibrio più efficace tra sicurezza, conformità e diffusione operativa, capace di accelerare l'adozione dell'identità digitale nei processi reali di business.

CAPITOLO 02

Minacce e opportunità

L'identità basata su wallet non rappresenta più una scelta facoltativa: è una direttrice inevitabile, alimentata sia da pressioni esterne, normative e di cyber risk, sia dalle opportunità offerte da nuovi modelli operativi.

Le imprese si confrontano con rischi crescenti derivanti da architetture IAM frammentate e da un contesto regolatorio sempre più stringente.

Le infrastrutture di identità costruite nel tempo mostrano oggi aree di esposizione significative: provider multipli, sistemi IAM legacy e integrazioni personalizzate convivono senza una logica unitaria. In molti casi, inoltre, dati personali e informazioni sensibili restano archiviati in database centralizzati, anziché essere gestiti direttamente tramite wallet digitali, come consentirebbero i nuovi modelli decentralizzati.
Questo approccio genera costi e complessità, ma soprattutto riduce la visibilità complessiva. Quando l'identità si estende oltre i dipendenti e coinvolge partner, servizi digitali e processi automatizzati, tale frammentazione si trasforma in un rischio strutturale.

Le minacce evolvono con la stessa rapidità. I sistemi basati su password restano ancora ampiamente diffusi, nonostante vulnerabilità ormai note. Phishing, condivisione impropria di credenziali e attacchi automatizzati ne sfruttano sistematicamente i limiti.

Parallelamente, i modelli di identità centralizzati introducono single point of failure in ecosistemi che dipendono da interazioni digitali continue.

In parallelo, molte organizzazioni stanno progressivamente perdendo il controllo sulle deleghe operative.
API, workflow automatizzati e agenti di Intelligenza Artificiale agiscono su sistemi differenti senza framework identitari chiari, verificabili e sottoposti a audit.

In questo scenario, l'identità diventa una questione di accountability, compliance e governance, con implicazioni dirette a livello di board. La regolamentazione rafforza ulteriormente questo cambiamento. Framework come NIS2, eIDAS 2.0 e GDPR richiedono alle organizzazioni di dimostrare tracciabilità, elevati livelli di assurance dell'identità e processi auditabili.

L'identità digitale diventa quindi il mezzo attraverso cui le aziende attestano il proprio controllo e prevengono utilizzi impropri dei dati personali.

Accanto a queste pressioni, **le opportunità abilitate dal nuovo paradigma sono altrettanto rilevanti**.

Il wallet introduce infatti un modello completamente diverso di gestione dell'identità digitale. Al posto della condivisione di profili identitari completi, abilita meccanismi di selective disclosure: un utente può dimostrare un attributo specifico senza rendere visibili informazioni non necessarie.

Questo riduce in modo significativo l'esposizione dei dati e il rischio associato, aumentando al contempo il livello di fiducia nell'informazione scambiata. Il tutto avviene ogni volta che i dati vengono condivisi, sotto il controllo diretto dell'utente. Di conseguenza, il consenso al trattamento dei dati personali non è più un passaggio esterno al processo, ma diventa incorporato nell'architettura stessa del wallet.

L'aderenza al GDPR si trasforma così in una proprietà nativa del sistema, anziché in un adempimento procedurale. La riduzione della resistenza legata alla compliance nei processi di condivisione dei dati apre la strada a nuovi modelli di business precedentemente difficili da implementare.
Le credenziali diventano inoltre riutilizzabili tra servizi e confini nazionali, abilitando onboarding più semplici, processi di KYC e KYB più affidabili, flussi di firma digitale più solidi e l'erogazione di servizi cross-border senza la necessità di integrazioni ripetute.

In modo ancora più rilevante, le organizzazioni possono superare la logica di sistemi isolati e partecipare a un ecosistema europeo della fiducia digitale. Il focus si sposta progressivamente dall'accesso ai sistemi al controllo dell'identità e delle interazioni che li attraversano.

Da obbligo di compliance a blueprint architetturale.

eIDAS 2.0 e l'European Digital Identity Wallet

La revisione del Regolamento eIDAS 2.0 introduce l'European Digital Identity Wallet come componente di trust formalmente definita all'interno dell'ecosistema europeo. Impone a ciascuno Stato membro di rendere disponibile almeno un wallet digitale per cittadini e residenti e di garantirne il riconoscimento a livello transfrontaliero nell'UE.
Questo passaggio segna una trasformazione: l'identità digitale diventa un'interfaccia di fiducia regolamentata, soggetta a requisiti espliciti in termini di assurance, gestione del ciclo di vita delle credenziali e interoperabilità con i wallet pubblici.

Cosa cambia per le imprese

Nel perimetro di eIDAS 2.0, le organizzazioni che oggi utilizzano il wallet per finalità di identificazione, autenticazione e firma digitale, includendo l'obbligo di accettazione previsto dal quadro normativo entro il 2027, devono essere in grado di consumare dati di identità ad alta garanzia e servizi fiduciari qualificati in modo conforme, verificabile e non discriminatorio su scala cross-border.

Questo include l'utilizzo di servizi quali Qualified Electronic Signature (QES), Qualified Electronic Attribute Attestation (QEAA) e Qualified Electronic Registered Electronic Delivery Services (QeRDS), tutti integrati in processi auditabili e conformi ai requisiti normativi.

Intersezione con NIS2, DORA e normative di settore

La direttiva NIS2 amplia in modo significativo il perimetro delle cosiddette "entità essenziali e importanti", innalzando al contempo le aspettative in termini di identity & access management, sicurezza dei sistemi e tracciabilità degli incidenti.
In parallelo, il regolamento DORA introduce requisiti analoghi per il settore finanziario, con un focus specifico sulla resilienza operativa digitale e sulla gestione del rischio ICT, incluso quello legato ai fornitori terzi.
In termini operativi, questo significa che gli operatori di infrastrutture critiche devono essere in grado di dimostrare in modo inequivocabile chi ha fatto cosa, con quale livello di autorizzazione e in quale sistema, utilizzando meccanismi allineati a standard europei comuni, e non più basati su silos identitari proprietari o soluzioni frammentate.

Perché oggi l'architettura è un elemento centrale

In questo contesto regolatorio e tecnologico, i wallet e i servizi fiduciari qualificati non possono più essere considerati componenti accessorie. Diventano invece elementi strutturali delle architetture di compliance e sicurezza.

Wallet digitali

Rappresentano interfacce standardizzate per l'identità ad alta garanzia e per la gestione degli attributi digitali, riconosciute a livello europeo.

Servizi fiduciari qualificati

Costituiscono meccanismi giuridicamente vincolanti per firme elettroniche, attestazioni e gestione delle evidenze digitali, con piena validità probatoria in ambito legale e di supervisione regolatoria.

Le organizzazioni che adottano wallet e servizi fiduciari non come soluzioni puntuali, ma come elementi fondanti dell'architettura digitale, sono in grado di costruire un modello di fiducia coerente e replicabile tra Paesi, business unit e canali digitali.

In questo modo, la pressione regolatoria si trasforma da vincolo operativo a leva di differenziazione competitiva e di maturità digitale.

CAPITOLO 03

Il posizionamento di Aruba

Aruba interpreta il wallet come parte integrante di un'architettura più ampia incentrata sulla Digital Integrity, che integra infrastruttura, servizi fiduciari e capacità di integrazione enterprise in un unico modello coerente.
Il valore del wallet non risiede nell'interfaccia in sé, ma nell'infrastruttura di fiducia che lo abilita. Emissione delle credenziali, verifica delle attestazioni, abilitazione delle firme digitali e garanzia della validità legale sono funzioni che richiedono un sistema strutturato.

Molti provider presidiano singoli livelli della catena del valore, certificazioni, autenticazione o servizi di firma, mentre Aruba sta costruendo un'offerta estesa all'ecosistema wallet, con l'obiettivo di presidiare l'intero ciclo della fiducia digitale.

In qualità di Qualified Trust Service Provider, identity provider e operatore di cloud europeo, Aruba integra autenticazione, validità giuridica e controllo operativo all'interno di un framework unificato. Questo elemento è determinante, poiché **i wallet non operano in modo isolato**: l'emissione delle credenziali, la verifica delle attestazioni, la gestione delle

notifiche legali e i processi di firma digitale richiedono un'infrastruttura coerente che i fornitori frammentati non sono in grado di garantire in modo completo.

L'architettura prevede un Wallet Gateway, il componente destinato a connettere l'identità basata su wallet con i sistemi enterprise reali: piattaforme HR, portali clienti, workflow documentali e processi digitali core. Questo approccio consente alle organizzazioni di adottare il modello in modo progressivo, avviando l'integrazione dai casi d'uso prioritari e scalando successivamente sull'intero ecosistema applicativo. Il risultato è un modello di **governance by design**: invece di incastrare soluzioni di fornitori differenti, le organizzazioni dispongono di un single point of trust lungo l'intero ciclo di vita dell'identità digitale.

Aruba ha avviato il percorso per diventare Business/Private Wallet Provider, provider di attestazioni elettroniche di attributi qualificate e non qualificate (QEAA ed EAA) e fornitore di un Wallet Gateway. Queste componenti sono destinate a integrarsi con i servizi di firma elettronica e sigillo qualificati già offerti da Aruba, a supporto della formalizzazione contrattuale e documentale. L'obiettivo è costruire un modello integrato di fiducia digitale, fondato su infrastrutture cloud europee e orientato alla tracciabilità end-to-end dei processi.

Il coinvolgimento di Aruba nelle iniziative europee di interoperabilità rafforza questo posizionamento, contribuendo attivamente alla definizione delle modalità con cui l'ecosistema dell'identità digitale evolverà e opererà su scala europea nei prossimi anni.

L'infrastruttura del Trust

Perché il data center è la nuova frontiera del Trust.

La visione di Aruba parte da un principio chiave: la fiducia digitale è solida quanto lo è il data center che la ospita. In questa prospettiva, Aruba mette a disposizione uno "Sovereign Stack" verticalmente integrato, elemento distintivo rilevante anche a livello di governance.

Integrità giurisdizionale: attraverso il controllo diretto dell'infrastruttura cloud europea, Aruba garantisce che dati identitari, attributi qualificati e chiavi crittografiche rimangano all'interno di un perimetro giuridico e fisico interamente europeo.

Hardware root of trust: l'identità digitale e la capacità di agire nel mondo digitale richiedono una catena di fiducia verificabile e trasparente, che parte dal singolo rack di data center fino ad arrivare al dispositivo dell'utente. Aruba governa l'intero ciclo infrastrutturale, eliminando il cosiddetto "gap infrastrutturale", ovvero quei punti di discontinuità in cui la sicurezza e la fiducia tendono più frequentemente a frammentarsi nei modelli distribuiti.

Resilienza come capacità operativa: in un contesto caratterizzato da crescente instabilità geopolitica e da un rafforzamento della pressione regolatoria (tra cui NIS2 e DORA), la sovranità digitale è un requisito funzionale per garantire continuità operativa.

Attraverso l'integrazione tra cloud, identity provider e servizi fiduciari qualificati, Aruba supera la logica di componenti separati e offre un control plane europeo per l'impresa digitale moderna.

CAPITOLO 04

Logica di portafoglio e architettura delle soluzioni

L'evoluzione del portafoglio Aruba punta a rendere l'identità basata su wallet una componente dei processi operativi quotidiani delle organizzazioni. Alla base si collocano gli elementi fondamentali dell'identità digitale: identità digitali, certificati qualificati, firme elettroniche, notifiche con valore legale e servizi di timestamping. Questi componenti garantiscono che ogni azione digitale sia autentica, tracciabile e giuridicamente valida.

Sopra questo livello si sviluppa lo strato di integrazione. Il Wallet Gateway è destinato a connettere identità e credenziali ai sistemi enterprise e a favorirne l'integrazione con servizi quali la posta elettronica certificata (PEC), la gestione documentale conforme e i controlli di accesso basati sull'identità. Il risultato non è un insieme di strumenti eterogenei, ma un sistema coerente in cui l'identità diventa infrastruttura. La stessa identità digitale può essere utilizzata per onboarding di un dipendente, firma di un contratto, accesso a sistemi applicativi, verifica di credenziali o controllo degli accessi fisici.

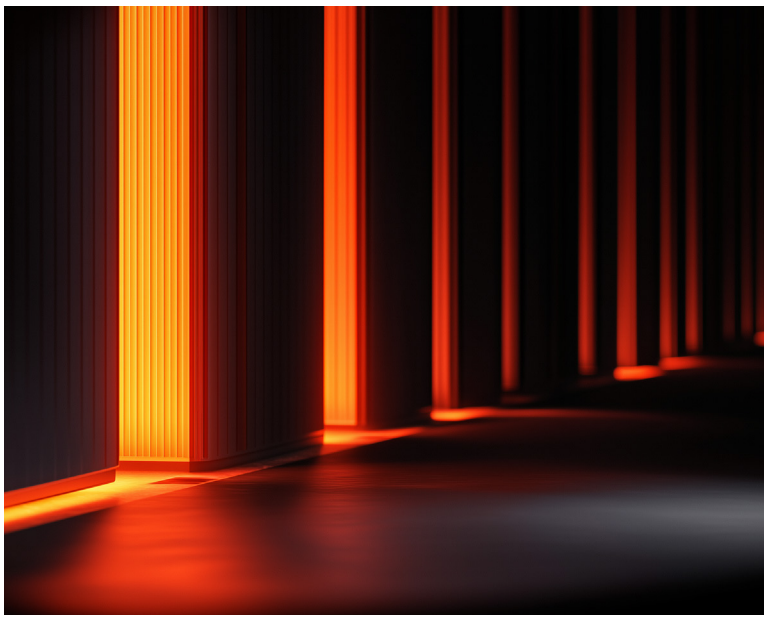
Questi sono i casi d'uso che Aruba punta ad abilitare attraverso l'evoluzione della propria architettura e l'integrazione delle componenti wallet con i servizi già disponibili.

Per le organizzazioni, i benefici attesi comprendono la riduzione del rischio di frode, una gestione più semplice dell'identità e una migliore esperienza utente, grazie a interazioni mobile-based e passwordless. L'integrazione di identità, tracciabilità e servizi fiduciari nei processi può inoltre supportare la dimostrazione della conformità ai requisiti applicabili. L'identità si sposta così da vincolo tecnico a colonna portante operativa dell'organizzazione.

La transizione verso un modello centrato sul wallet comporta effetti operativi diretti. L'adozione di autenticazione passwordless (o zero-password infrastructure) riduce in modo significativo l'esposizione a minacce come phishing e furto di credenziali. Allo stesso tempo, le firme digitali da mobile eliminano la necessità di dispositivi fisici dedicati e la relativa complessità logistica.

Nel contesto del Business Wallet, questo paradigma si estende alla comunicazione con valore legale tramite i Qualified Electronic Registered Delivery Services (QeRDS), abilitando scambi sicuri e tracciabili tra organizzazioni e Pubblica Amministrazione.

In pratica, i processi identitari diventano al tempo stesso più semplici e più sicuri. Nel tempo, questo riduce la frizione operativa e integra la compliance direttamente nei workflow aziendali. **L'identità evolve così da centro di costo a leva di efficienza operativa e compliance by design**. Aruba sta evolvendo la propria architettura per accompagnare questa transizione.



Leadership di Aruba nei pilot europei sull'Identità Digitale

Aruba esprime una leadership consolidata nell'ecosistema del European Digital Identity Wallet (EUDI Wallet) attraverso un ruolo attivo in due principali Large-Scale Pilots (LSP), posizionandosi come attore chiave nella definizione dei modelli operativi di riferimento.

Nel contesto del POTENTIAL LSP, Aruba ha contribuito alla definizione di implementazioni di riferimento per l'integrazione tra EUDI Wallet e firme elettroniche qualificate (QES), in coerenza con eIDAS e con il Reference Architecture Framework (ARF).
L'azienda ha realizzato una soluzione end-to-end completa, che copre l'intero ciclo della fiducia digitale: dal wallet provider, all'orchestrazione dei relying party, fino ai servizi fiduciari qualificati e all'infrastruttura cloud sicura.
Questo approccio ha permesso di validare scenari di interoperabilità cross-border in ambiente quasi produttivo, con particolare attenzione a sicurezza, scalabilità e conformità normativa. Su queste basi si innesta la partecipazione di Aruba al WeBuild LSP, un consorzio che coinvolge oltre **180 organizzazioni in 30 Paesi**.

In questo contesto, il Wallet Gateway di Aruba abilita scenari di business cross-border complessi, tra cui automazione dei processi di KYC/KYB, gestione di adempimenti fiscali esteri e rappresentanza legale digitale delle imprese.

Nel loro insieme, questi programmi posizionano Aruba come **partner strategico per Pubbliche Amministrazioni e imprese**, contribuendo a ridurre la complessità di integrazione e ad accelerare l'adozione del Digital Single Market, in anticipo rispetto alle scadenze regolatorie previste per il 2026.

Quando il wallet diventa operativo

USE CASE



Workforce e digital workplace

Il wallet trasforma i processi HR e di gestione del workplace in flussi digitali end-to-end: dall'onboarding alla firma dei contratti, fino all'accesso alle applicazioni aziendali e alle infrastrutture fisiche.
I dipendenti possono autenticarsi tramite meccanismi strong e passwordless, condividere credenziali verificate (ruoli, formazione, certificazioni) e utilizzare lo stesso wallet sia per firme digitali sia per l'accesso fisico tramite NFC, all'interno di un ciclo di vita del dipendente gestito in modo centralizzato.

USE CASE



Comunicazioni business con valore legale

Nel contesto del Business Wallet, i servizi di Qualified Electronic Registered Delivery Services (QeRDS) e le firme qualificate convergono in un unico canale centrato sull'identità.

Le organizzazioni possono inviare e ricevere comunicazioni con pieno valore legale, automatizzare processi di credit collection e orchestrare journey di comunicazione multicanale in cui identificazione, notifica e firma contrattuale avvengono all'interno di un'esperienza coerente e continua.

USE CASE



Processi regolati nei settori finance e healthcare

Nel settore finanziario, i processi di KYC/KYB e AML basati su wallet semplificano onboarding e due diligence continua, mantenendo alti livelli di assurance e piena auditabilità. In ambito healthcare e life sciences, lo stesso stack di fiducia supporta flussi digitali per sperimentazioni cliniche, archiviazione certificata di referti e imaging diagnostico, e scambio sicuro di dati sensibili con autorità regolatorie e partner. Il risultato è una riduzione significativa dell'uso della carta, una contrazione dei tempi di processo e un rafforzamento strutturale della compliance.

CAPITOLO 05

Prospettive future dell'identità digitale

Il wallet non rappresenta soltanto l'evoluzione dell'identità digitale nel presente, ma segna il punto di svolta in cui l'identità diventa un vero e proprio livello di controllo trasversale per tutti i sistemi digitali.
Con l'espansione degli ecosistemi digitali, ogni azione, umana o automatizzata, dovrà essere associata a un'identità verificabile e a un livello di autorità chiaramente definito, indipendentemente dal fatto che si tratti di un dipendente, di un processo organizzativo, di un dispositivo connesso o di un agente di Intelligenza Artificiale.

La fiducia evolve verso un modello dinamico e continuo. I sistemi non si limiteranno a verificare l'identità al momento del login, ma la rivalideranno costantemente sulla base del contesto, dei segnali di rischio e dell'evoluzione delle condizioni operative.

Una credenziale wallet valida per un accesso ordinario potrà richiedere passaggi di verifica aggiuntivi in presenza di transazioni ad alto valore o comportamenti anomali.
Questo cambiamento spinge le imprese da architetture a silos verso ecosistemi interoperabili, in cui le organizzazioni interagiscono direttamente attraverso identità digitali verificate, riducendo la necessità di affidarsi a piattaforme intermediarie. Contratti cross-border, integrazioni con partner e verifiche lungo la supply chain potranno essere eseguiti in modalità peer-to-peer, supportati da evidenze crittografiche verificabili.

In questo modello, il wallet assume il ruolo di interfaccia operativa della fiducia. Consente alle organizzazioni di verificare invece di raccogliere dati e di applicare regole in modo esplicito, riducendo la dipendenza da forme di fiducia implicita e non strutturata.

Guardando avanti, tre direttrici evolutive definiranno questo scenario:

La machine identity governance raggiungerà gli stessi standard dell'identità umana. Con l'aumento del ruolo degli agenti di Intelligenza Artificiale nei processi di procurement, customer service o decisioni finanziarie, questi sistemi dovranno disporre di credenziali organizzative verificabili, con permessi espliciti e audit trail completi, analogamente a quanto previsto per gli utenti umani.

La resilienza crittografica dovrà evolvere per rispondere alle minacce quantistiche. L'adozione di schemi di firma post-quantum e modelli ibridi di gestione delle chiavi diventerà essenziale per proteggere credenziali a lunga durata, come quelle associate ai wallet, garantendone l'affidabilità nel tempo e la tenuta su orizzonti pluridecennali.

La verifica della fiducia in tempo reale sostituirà i controlli periodici. Segnali continui come integrità del dispositivo, contesto di localizzazione, biometria comportamentale e indicatori di rischio permetteranno di adattare dinamicamente i livelli di assurance, introducendo un modello di sicurezza adattiva realmente scalabile in funzione del rischio.

L'Europa sta costruendo in modo sistematico l'identità come infrastruttura abilitante. Per le imprese, questo rappresenta un cambiamento strutturale nel modo in cui i sistemi vengono progettati, le interazioni vengono orchestrate e la fiducia viene definita e governata. Le organizzazioni che adotteranno per prime questo paradigma contribuiranno a definire le regole dell'interazione digitale nel prossimo decennio.



About Aruba

Aruba, fondata nel 1994, è il Cloud Champion italiano e uno dei principali provider europei di infrastrutture e piattaforme digitali basate su asset proprietari. L'azienda progetta e gestisce l'intero stack tecnologico: dalla progettazione e costruzione di data center alle piattaforme cloud, dai servizi di trust e security alla connettività e alle soluzioni software che supportano strategie digitali e applicazioni basate su AI.

Con capitale interamente italiano, Aruba conta 16 milioni di utenti attivi sulle proprie piattaforme provenienti da oltre 100 nazioni e gestisce una infrastruttura distribuita su 8 data center in Europa, che ospita oltre 2,7 milioni di domini, 10 milioni di caselle e-mail, 9 milioni di caselle PEC e migliaia di infrastrutture IT di clienti.

Copyright © Aruba. All rights reserved.
Disclaimer: This content is provided for general information purposes and is not intended to be used in place of consultation with our professional advisors.

aruba.it