The future of Digital Identity and Digital Integrity

Aruba Wallet, for a new European Trust Infrastructure.



pulse

aruba.it



Europe is moving toward a unified digital identity model where wallets become the standard interface for trust, compliance, and cross-border interaction.

Aruba positions itself as a single point of trust, combining identity, qualified trust services, and European infrastructure into an integrated, wallet-ready architecture.

In this context, **the wallet is not just a tool: it becomes the operational control layer** through which digital trust is verified, governed, and scaled across the European ecosystem.

Summary

01 | **Introduction: current trends and context** 4

02 | **Threats & opportunities** 7

03 | **Aruba's position** 9

04 | **Portfolio logic & details** 11

05 | **Future outlook on digital identity** 15

CHAPTER 01

Introduction: current trends and context

Europe is entering a new phase of digital maturity in which identity moves beyond a basic login mechanism and becomes a foundational layer of trust, governance, and operational control.

For enterprises, this shift creates both pressure and opportunity. Regulation is tightening, cyber risk is rising, and systems are becoming more interconnected. At the same time, a new identity model offers a way to reduce friction, strengthen accountability, and enable new forms of digital interaction.

For more than a decade, digital transformation was driven by speed and scale. Organisations moved to the cloud, automated processes, and connected systems across increasingly complex environments. Identity evolved alongside this transformation, but without a unifying logic. It remained fragmented, shaped by national schemes, tied to individual platforms, and often designed for specific use cases rather than for systemic trust. That model has reached its limits.

Digital environments today are inherently distributed. Enterprises operate across hybrid infrastructures, SaaS platforms, APIs, connected devices, and increasingly AI-driven systems. The traditional perimeter has dissolved, and every interaction (human or machine!) requires verification.

Trust is becoming harder to establish: deepfakes undermine authenticity, identity fraud scales through automation, and complex digital ecosystems dilute accountability. This is a structural shift. Systems must prove integrity and in this context Digital Identity becomes the mechanism through which organisations demonstrate who is acting, under which authority, and within which legal and operational boundaries.

European regulation reflects this shift. Frameworks such as eIDAS 2.0, NIS2, GDPR, DORA, and the AI Act are redefining how systems must be designed. **Trust must be engineered into architecture, and accountability must be traceable by design**.

The European Digital Identity Wallet is central to this transition. By the end of 2026, each Member State should provide a wallet enabling citizens to store credentials, share only necessary data, and sign with legal validity.

This model extends to organisations via Digital Business Wallets (which function both as a web platform or an app), which embed identity into business processes through authorizations, credentials, and notifications with legal validity (QeRDS).

This marks a shift where **identity becomes the European digital backbone for trust across every transaction and interaction**.



Public and Private Wallets: one standard, different roles

- **Public digital wallets**, issued under the control of Member States under eIDAS 2.0, provide individuals with a secure and interoperable way to manage identity and credentials.

  They enable authentication, selective sharing of verified attributes, and legally valid digital signatures across public and private services, while ensuring strict adherence to privacy and data minimisation principles.

  Public wallets establish a trusted and interoperable identity layer at European scale focusing on high level of assurance identity and mainly driven by Public Administration use cases, with a limited set of interoperable credentials.

- **Private wallets** extend the same model also to enterprise environments, in B2B, B2C and B2E processes.
  Built on the same technical and regulatory foundations, they integrate into company applications and processes, enabling organisations to manage customer and employee interactions, authentication, and service access within their own digital ecosystems. Private wallets make that identity operational within real business processes, extending the set of credentials to include all data necessary to specific transactions.
  They can include Identity proofing features with a fine-tuned level of assurance, to enhance UX and reduce friction in adoption, and can interoperate with public wallets.

The key opportunity is to move from a single-wallet logic to a layered trust model.

Public wallets can anchor high-assurance, legally recognized identity for citizen-to-public-administration and cross-border use cases, while private wallets can operationalize the same standards in enterprise, customer, and employee journeys, with assurance levels tuned to the risk of each transaction.
This preserves privacy through selective disclosure and data minimisation, while creating interoperability without forcing all use cases into the same state-defined profile, improving both security and adoption.

CHAPTER 02

Threats & opportunities

Wallet-based identity isn't optional anymore and it is driven both by pressures (regulatory and cyber risks) and opportunities. Enterprises face mounting risks from fragmented IAM and tightening regulation. Identity architectures built over time face potential exposure: multiple identity providers, legacy IAM systems, custom integrations coexist without a unified logic and the fact that in this model personal and private data is stored on databases (and not on the wallets as could be the case). This creates cost and complexity, but more critically limits visibility. As identity extends beyond employees to partners, services, and automated processes, this fragmentation becomes a structural risk.

Threats evolve at the same pace. Password-based systems remain widespread despite their known weaknesses, while phishing, credential sharing, and automated attacks exploit them at scale. Centralised identity models introduce single points of failure in environments that depend on continuous digital interaction.

In parallel, organisations are losing control over delegated authority. APIs, workflows, and AI agents act across systems without clear, auditable identity frameworks. Identity becomes a matter of accountability, compliance, and governance at board level. Regulation reinforces this shift. Under frameworks such as NIS2, eIDAS 2.0 and GDPR, organisations must demonstrate traceability, strong identity assurance, and auditable processes. Identity becomes how organisations prove control and prevent misuse of personal data.

But alongside these pressures, **opportunities are equally significant**.

The wallet introduces a different paradigm. Instead of sharing full identity profiles, it enables selective disclosure. A user can prove a specific attribute without exposing unnecessary data, reducing risk while increasing confidence in the information exchanged. And this is done every time data is shared, strictly under user control. As a result, consent to personal data processing is embedded by design in the wallet's architecture, making GDPR adherence intrinsic rather than procedural. Compliance friction in data sharing is dramatically reduced, unlocking entirely new business models.

Credentials now work across services and borders. This enables simpler onboarding, more reliable KYC and KYB, stronger digital signing flows, and cross-border service delivery without repeated integrations. More importantly, organisations can move beyond isolated systems and participate in a broader European trust ecosystem. **The priority shifts from access to control**.

From compliance obligation to architectural blueprint

eIDAS 2.0 and the European Digital Identity Wallet

The revised eIDAS 2.0 Regulation introduces the European Digital Identity Wallet as a formally defined trust component, obliging every Member State to make at least one wallet available to citizens and residents and to ensure cross border recognition across the EU.

For enterprises, this changes identity from a local implementation choice into a regulated trust interface, with clear requirements on assurance levels, credential lifecycle, and interoperability with public wallets.

What this means for enterprises

Under eIDAS 2.0, organisations that rely today on the wallet for identification (and the 2027 deadline for acceptance obligation under the current framework), authentication, and signing must be able to consume high assurance identity data and qualified trust services (QES, QEAA, QeRDS) in a way that is auditable and non discriminatory across borders.
This pushes identity and signing workflows out of bespoke integrations and into standardised, wallet centric patterns that can be scrutinised by regulators and supervisors.

Intersection with NIS2, DORA, and sector rules

NIS2 expands the scope of “essential and important entities” and raises expectations on identity, access management, and incident traceability, while DORA does the same for ICT and third party risk in financial services.

In practice, this means critical operators must be able to demonstrate who did what, under which authority, in which system, and do so using mechanisms that align with EU level standards rather than proprietary identity silos.

Why architecture matters now

In this landscape, wallets and qualified trust services are no longer optional add ons. They become building blocks of compliant architectures:

- **Wallets**: standardised interfaces for high assurance identity and attributes, recognised across the EU;
- **Qualified trust services**: legally robust mechanisms for signatures, attestations, and evidence delivery that stand up in court and under supervision.

Enterprises that treat wallets and trust services as foundational architectural building blocks, rather than as point solutions, will assure a consistent, repeatable trust model across countries, business units, and digital channels and potentially turn compliance pressure into competitive differentiation.

CHAPTER 03

Aruba’s position

Aruba approaches the wallet as part of a broader architecture built around Digital Integrity that spans infrastructure, trust services, and enterprise integration.

The value of a wallet lies in the trust infrastructure behind it, rather than in the interface itself. Issuing credentials, verifying claims, enabling signatures, and ensuring legal validity all require a coordinated system.
Most providers address individual layers (certifications, authentication, etc.), while Aruba is building an offering that extends to the wallet ecosystem, with the aim of covering the entire digital trust lifecycle.

As a Qualified Trust Service Provider, identity provider, and European cloud operator, Aruba combines authentication, legal validity, and operational control within a single framework.

This matters because **wallets don't work in isolation**. Issuing credentials, verifying claims, ensuring legal notifications and digital signatures, all demand coordinated infrastructure that fragmented vendors can't deliver. The architecture includes plans for a Wallet Gateway designed to connect wallet-based identity with real enterprise systems: HR platforms, customer portals, document workflows, and core digital processes. Enterprises can integrate incrementally, starting where they decide to.

This approach defines **governance by desig**n. Instead of stitching together multiple vendors, organisations get a single point of trust across the identity lifecycle.

Aruba has begun the process of becoming a Business/Private Wallet Provider, a provider of qualified and non-qualified electronic attestations of attributes (QEAA and EAA), and a Wallet Gateway provider. These components are intended to integrate with the qualified electronic signature and seal services already offered by Aruba, supporting the formalisation of contracts and documents. The aim is to build an integrated digital trust model based on European cloud infrastructure and designed to support end-to-end process traceability.

Aruba's involvement in European interoperability initiatives further reinforces this position. It contributes to shaping how the ecosystem will function at scale and how it will evolve in the future.

The Infrastructure of Trust

Why the Data Center is the New Trust Frontier

The integrity of a wallet is inextricably linked to the foundations it sits on.

Aruba believes that trust is only as strong as the data center that hosts it. Aruba provides a vertically integrated "Sovereign Stack." This is a critical distinction for the board-level agenda:

- **Jurisdictional Integrity**: by owning the European cloud infrastructure, Aruba ensures that identity data, qualified attributes, and cryptographic keys remain within a 100% European legal and physical perimeter;
- **The Hardware Root of Trust**: strategic control requires more than just code; it requires a transparent chain of custody from the server rack to the end-user's mobile device. Aruba governs this entire lifecycle, eliminating the "infrastructure gap" where security often fractures;
- **Resilience as a Service**: in the face of intensifying geopolitical shifts and regulatory scrutiny (NIS2, DORA), "sovereignty" is no longer a buzzword, it is a functional requirement for continuous operation.

By collapsing the distance between the Cloud, the Identity Provider, and the Qualified Trust Service, Aruba moves beyond providing a tool. It provides the European Control Plane for the modern enterprise.

CHAPTER 04

Portfolio logic & details

The evolution of Aruba's portfolio aims to make wallet-based identity part of organisations' everyday operational processes. At its base are the essentials: digital identities, qualified certificates, electronic signatures, legally binding notifications and timestamping. These ensure every digital action is authentic, traceable, and legally valid.

On top sits the integration layer. The Wallet Gateway is intended to connect identity and credentials to enterprise systems and facilitate their integration with services such as certified electronic mail (PEC), compliant document management, and identity-based access control. This creates a unified system, not a toolkit. This turns Identity into infrastructure.

The same identity can onboard an employee, sign a contract, access systems, verify credentials, or control physical access. These are the use cases Aruba aims to enable by evolving its architecture and integrating wallet components with services that are already available.

For organisations, the expected benefits include reduced fraud risk, simpler identity management, and an improved user experience through mobile-based, passwordless interactions. Integrating identity, traceability, and trust services into processes can also help demonstrate compliance with applicable requirements. Identity shifts from a technical constraint to an operational backbone.

The shift to a wallet-centric model also has immediate operational implications. Moving toward passwordless (zero-password infrastructure) authentication reduces exposure to threats such as phishing and credential theft, while mobile-based signatures remove the need for physical tokens and associated logistics.

In the context of the Business Wallet, this extends to legally valid communication through Qualified Electronic Registered Delivery Services (QeRDS), enabling secure and traceable exchanges between organisations and public administrations.
In practice, **identity processes become both simpler and more secure**. Over time, this reduces operational friction and embeds compliance directly into workflows. Identity evolves from cost centre to operational efficiency and compliance by design. Aruba is evolving its architecture to support this transition.

Aruba's Leadership Across European Digital Identity Pilots

Aruba demonstrates comprehensive EUDI Wallet expertise through dual leadership in major Large-Scale Pilots (LSPs). In the POTENTIAL LSP, Aruba defined reference implementations for EUDI Wallet-QES integrations per eIDAS/ ARF, delivering the only complete end-to-end solution, spanning wallet provider, relying party orchestration, qualified trust services, and secure cloud infrastructure. This enabled validated cross-border interoperability and production-grade scenarios focusing on security, scalability, and compliance.

Building on this foundation, Aruba's participation in the WeBuild LSP (**180+ organizations across 30 countries**) validates complex cross-border business scenarios through its Wallet Gateway, including automated KYC/KYB, foreign tax filings, and digital legal representation for companies.

These pilots collectively position Aruba as the **strategic partner for public administrations and enterprises**, reducing integration complexity while accelerating Digital Single Market adoption ahead of the 2026 mandate.

Where the wallet becomes operational



USE CASE

Workforce and workplace

The wallet turns HR and workplace processes into end to end digital flows: from onboarding and contract signing to access to corporate applications and facilities. Employees can authenticate with strong, passwordless mechanisms, share verified credentials (roles, training, certifications), and use the same wallet for both digital signatures and NFC based physical access, governed centrally over the full employee lifecycle.



USE CASE

Business communications with legal value

In a Business Wallet context, qualified electronic registered delivery (QeRDS) and qualified signatures move into a single, identity centred channel. Organisations can send and receive legally valid notifications, automate credit and collections workflows, and orchestrate multi channel communication journeys where identification, notification, and contract signing happen in one coherent experience.



USE CASE

Regulated processes in finance and healthcare

In finance, wallet based KYC/KYB and AML checks streamline onboarding and ongoing due diligence, while preserving high assurance and auditability. In healthcare and life sciences, the same trust stack can support digital clinical trial workflows, certified archiving of diagnostic reports and imaging, and secure exchange of sensitive data with regulators and partners, reducing paper, shortening cycle times, and strengthening compliance.



CHAPTER 05

Future outlook on digital identity

The wallet is not only the evolution of Digital Identity today but also marks the point where identity becomes a control layer for all digital systems.
As environments expand, every action (human or machine!) must be linked to a verifiable identity and a defined authority, whether it's a human employee, organisational process, connected device, or AI agent.

Trust will become dynamic and continuous. Systems won't just check identity at login, they'll re-verify it constantly based on context, risk signals, and changing conditions.
A wallet credential that worked for routine access might demand extra steps for high-value transactions or unusual patterns.

This shifts enterprises from platform silos to interoperable ecosystems. Organisations will interact directly through verified digital identities, bypassing the need to trust intermediary platforms.

Cross-border contracts, partner integrations, supply chain verification will all be executed peer-to-peer with cryptographic proof.

In this model, the wallet acts as the operational interface. It enables organisations to verify rather than collect, and to enforce rules rather than rely on implicit trust.

Looking ahead, three developments will shape this landscape:

- **Machine identity governance will match human standards**. As AI agents handle procurement, customer service, or financial decisions, they'll carry verifiable organisational credentials with defined permissions and audit trails, just like human employees.

- **Cryptographic resilience must evolve against quantum threats**. Post-quantum signatures and hybrid key schemes will protect long-lived credentials like those in wallets, ensuring they remain trustworthy for decades.

- **Real-time trust verification will replace periodic checks**. Continuous signals, device integrity, location context, behavioural biometrics, will adjust assurance levels dynamically, creating adaptive security that scales with risk.

Europe is methodically building identity as infrastructure. For enterprises, this represents a structural shift in how systems are designed, interactions are managed, and trust is established. The organisations that move first will define the rules of digital interaction for the next decade.

In this scenario, **the wallet becomes the control layer of digital trust where digital Integrity becomes reality**.

aruba.it



About Aruba

Aruba, founded in 1994, is Italy's Cloud Champion and one of Europe's leading providers of digital infrastructures and platforms based on proprietary assets. The company designs and manages the entire technology stack: from the design and construction of data centers to cloud platforms, from trust and cybersecurity services to connectivity and software solutions that support digital strategies and AI-based applications.

With entirely Italian capital, Aruba serves 16 million users from over 100 countries and operates an infrastructure distributed across 8 data centers, hosting thousands of customers' IT infrastructures.

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