The Integrity Economy

Cybersecurity, trust services and the architecture of Digital Identity in Europe.

aruba.it

For much of the past two decades, digital transformation has been measured in terms of speed and scale.

Organisations raced to migrate infrastructure to the cloud, automate processes, and deploy new technologies faster than competitors. Efficiency became the dominant metric of progress, and acceleration the defining characteristic of the digital economy. That phase of transformation is now reaching its limits.

Across Europe, the question is no longer simply how quickly systems can evolve, but whether the digital structures behind them are reliable, governable and resilient over time. Speed alone does not create trust. In complex digital ecosystems, it can just as easily amplify fragility.

Several forces are converging to produce this shift.

Regulation is becoming structurally embedded in digital architecture. Frameworks such as **GDPR, NIS2, eIDAS 2.0** and the **AI Act** are redefining how organisations design systems, govern identities and manage risk. Beginning in 2026, NIS2 will introduce direct board-level accountability for cybersecurity governance, with financial penalties reaching up to two percent of global turnover for critical entities that fail to meet risk management obligations.

Compliance is no longer an afterthought applied to finished systems. It is increasingly a design requirement.

At the same time, the technological environment itself has changed. Corporate infrastructures are now distributed by default. Hybrid clouds, SaaS platforms, operational technology, APIs, remote workforces and autonomous systems have dissolved the traditional boundaries of the enterprise network. Every connection expands capability, but also expands exposure.

Trust within these ecosystems has become harder to establish. Deepfakes blur authenticity. Identity fraud scales through automation. Opaque AI systems raise new questions about accountability and traceability.
Organisations may continue to digitise their operations, yet stakeholders increasingly ask a more fundamental question: **can these systems be trusted?**

In response, the foundations of digital competition are beginning to shift.

In many global technology markets, trust is still treated as a brand attribute, something organisations signal rather than structurally engineer. **Europe is increasingly moving in a different direction**, embedding trust directly into the architecture of digital systems through regulatory frameworks, digital identity infrastructures and European technology platforms. In this emerging model, **trust becomes infrastructure rather than reputation**. Cybersecurity protects the environments in which identities and data operate; trust services validate digital actions, transactions and communications; and brand protection safeguards the public expression of organisations in the digital space. Together, these capabilities ensure data and identity integrity across every digital interaction, preserving authenticity, attribution and accountability over time.

Integrity thus becomes the operational trust layer of the digital economy, the condition that allows organisations to act, transact and evolve securely in a distributed world while preserving strategic control: the ability to decide, operate and innovate with verifiable identity and trusted infrastructure.

This transition points toward what may be described as an **Integrity Economy**.

In such an environment, competitive advantage derives not only from technological capability, but from the ability to demonstrate verifiable control over infrastructure, identities, data and risk exposure.

In practice, this **integrity emerges from the convergence of three capabilities**: **cybersecurity**, which protects systems; **trust services**, which validate digital actions; and **brand protection**, which safeguards the public identity of organisations in the digital sphere.

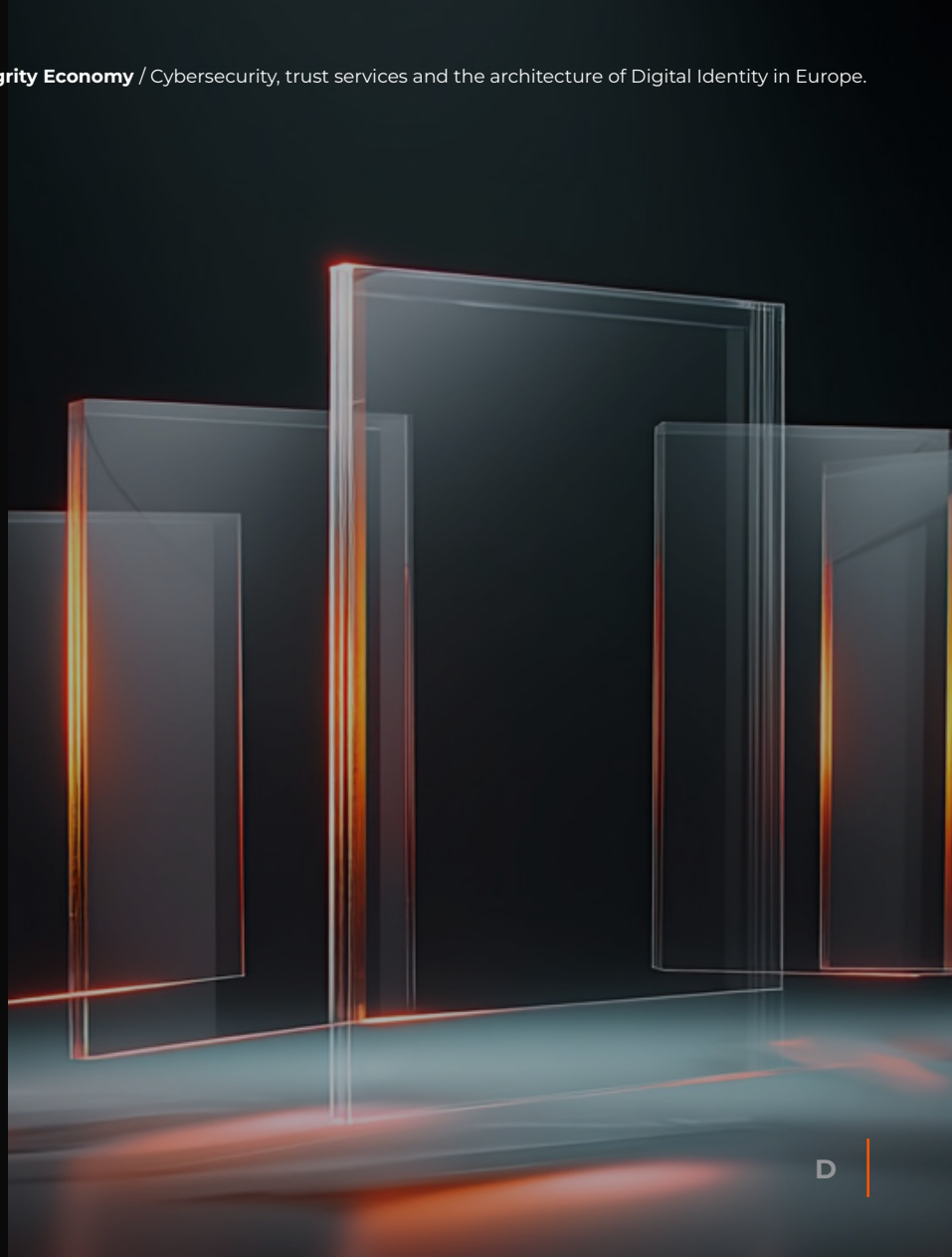
Ultimately, these mechanisms converge around a single objective: ensuring that digital identities, and the transactions, communications and decisions associated with them, remain authentic, attributable and verifiable over time.

For enterprises, this represents a profound shift in how digital transformation must be approached. It is no longer simply a sequence of technology upgrades.
It is a design discipline that connects data centre architecture to identity governance, cybersecurity operations to legal trust frameworks, and cloud execution domains to jurisdictional accountability.

Integrity, in this sense, becomes the condition that allows digital systems to scale without losing control.

The next phase of digital transformation will therefore not be defined by those who move fastest, but by those who build systems capable of sustaining trust over time. Velocity alone can produce innovation, but without structural integrity it also produces systemic risk.

Velocity without integrity creates fragility.
Integrity, by contrast, enables durable innovation.



Summary

01 | **Integrity in a Dispersive, Regulated World** 7

02 | **Operationalising Integrity** 9

03 | **Integrity from the Ground Up** 12

04 | **Compliance by design** 14

05 | **Identity as the Core of Integrity** 15

06 | **Secure strategic control at Scale** 18

07 | **APPENDIX A - Trust Services: Legal Validity by Design** 21

08 | **APPENDIX B - Brand Protection** 25

09 | **APPENDIX C - Cybersecurity** 29

EVIDENCE OF ARUBA'S INTEGRITY ECONOMY SCALE

Europe's leading trust infrastructure operator
Aruba, through its two Certification Authorities and QTSPs, Aruba PEC and Actalis, operates 1.6 billion electronic signatures a year, 9 million+ certified-email (PEC) mailboxes, 2 million+ managed digital identities, and over 1 million active SSL certificates.

Backbone of Italy's national digital trust
Aruba's trust infrastructure underpins 62.4 million Italian health cards and 2.7 million domains under management, operating as registry for .cloud and a major operator within .it, .eu and other European ccTLD ecosystems.

Founding European-compliance posture
Aruba is a Gaia-X Board Member and active node of the Digital Clearing House, and a 1st (founding) member of CISPE adhering to its Code of Conduct, embedding European data protection and federated-cloud compliance into its operating fabric.

1.6BN
ELECTRONIC SIGNATURES MANAGED EACH YEAR

+9M
CERTIFIED EMAIL (PEC) MAILBOXES

+2M
DIGITAL IDENTITIES MANAGED

+1M
ACTIVE SSL CERTIFICATES

62.4M
ITALIAN HEALTH CARDS MANAGED

2.7M
MANAGED DOMAINS

evidence box

CHAPTER 01

Integrity in a Dispersive, Regulated World

The digital environment in which organisations operate today bears little resemblance to the centralized IT architectures of the past.

Corporate systems are now inherently distributed, spanning hybrid cloud infrastructures, SaaS platforms, operational technology, remote workforces and increasingly automated processes. What was once a contained network perimeter has become a constantly shifting ecosystem of interconnected services.

This dispersion expands capability, but it also transforms the nature of risk.

Every additional integration, an API, a SaaS dependency, a connected device, or an automated workflow, creates new pathways through which disruption can propagate. At the same time, automation and AI compress decision cycles, allowing systems to act faster and at greater scale than traditional governance mechanisms were designed to oversee. The result is an environment where operational complexity and systemic exposure grow simultaneously.

In such conditions, risk management can no longer be treated as an administrative function or a periodic compliance exercise. It becomes a structural requirement for organisational resilience.

European regulation is increasingly reflecting this reality. The NIS2 Directive formalises a governance model in which cybersecurity and operational continuity are no longer confined to technical teams. Organisations must demonstrate comprehensive risk management practices that extend across supply chains, third-party providers, and critical digital dependencies. Boards are expected to exercise direct oversight, and failure to implement adequate safeguards may carry significant financial penalties.

Compliance, therefore, cannot remain an after-the-fact verification process. It must be embedded within the design and operation of digital systems themselves.

Yet many organisations struggle to operationalise this shift. Without a clear definition of what integrity means within their own digital environment, across infrastructure, data, identities and external dependencies, security investments tend to become reactive. Controls are added in response to incidents or regulatory pressure rather than integrated into a coherent architectural model.

This reactive pattern is increasingly difficult to sustain. Industry surveys consistently highlight a persistent shortage of cybersecurity expertise, with talent gaps affecting a substantial share of European enterprises. Under these conditions, fragmented security strategies impose both financial and operational strain.

What becomes necessary instead is a transition from isolated security controls to coherent design frameworks capable of governing distributed digital environments.

In such a landscape, **integrity becomes more than a principle of good governance. It functions as the structural property that determines whether digital systems remain manageable as they scale in complexity**.

Organisations that embed integrity into the architecture of their infrastructure, identities and operational processes develop the capacity to absorb shocks, adapt to regulatory change and maintain control over increasingly complex ecosystems. Those that do not often find themselves trapped in cycles of reactive remediation.

The distinction between the two increasingly defines the difference between durable resilience and persistent vulnerability.

CHAPTER 02

Operationalising Integrity

If integrity is to become a meaningful property of digital systems rather than a strategic aspiration, it must be translated into operational practice.

In many organisations, however, the reality of security architecture reflects the fragmented evolution of the digital environment itself. Infrastructure may be hosted across multiple cloud providers, cybersecurity tools sourced from specialised vendors, identity platforms managed separately, and governance frameworks layered on top to reconcile the resulting complexity. Each component may function effectively in isolation, yet the overall system often lacks a clear centre of responsibility.
When incidents occur, accountability can become difficult to trace. Responsibility is dispersed across providers, platforms and operational domains, while organisations remain ultimately accountable for the consequences.

Regulatory developments across Europe are increasingly challenging this model. Frameworks such as NIS2 place growing emphasis on demonstrable end-to-end governance, requiring organisations to understand and manage risk across their entire digital ecosystem.

Boards must maintain visibility over supply chain exposure, auditors expect traceability across hybrid infrastructures, and incident reporting obligations apply regardless of whether failures originate internally or through outsourced services.
Under these conditions, integrity cannot remain a declarative principle. It must be embedded in the way systems are designed, operated and governed.

Two broad approaches to operationalising integrity are beginning to emerge.

The first treats integrity primarily as a perimeter challenge. Organisations add security controls, expand monitoring capabilities and introduce additional compliance procedures in an effort to compensate for architectural fragmentation. While these measures can improve visibility, they often remain layered on top of existing complexity and rely heavily on the coordination of multiple external providers.

The second approach addresses the problem at a more structural level. Instead of compensating for fragmentation, it seeks to reduce it by aligning infrastructure ownership, operational security, connectivity and trust frameworks within a coherent architecture. In this model, integrity is not added as an external control layer; it becomes a property of the system itself.

Aruba's operating model has developed along these lines. **Long before concepts such as digital sovereignty became prominent in European technology policy, Aruba invested in the direct development and management of its own infrastructure**.

Data center facilities, European cloud environments and internal security operations were built to support mission-critical services operating at national scale.

Features such as energy resilience, logical segregation, auditability and identity governance were introduced not as marketing differentiators, but as operational requirements for maintaining continuity and trust.

Over time, these operational disciplines evolved into an integrated Trust & Security portfolio.

The distinction between this approach and more loosely assembled ecosystems is structural. Security practices developed to protect critical infrastructure under direct operational responsibility, including Security Operations Center procedures, vulnerability management cycles, audit frameworks, identity lifecycle governance and tested continuity models, derive from continuous operational exposure. They reflect systems that must function reliably under real conditions rather than architectures assembled primarily through contractual integration.

This vertical coherence alters the way risk is distributed.

When infrastructure, cloud environments, cybersecurity operations, connectivity and trust services operate within a unified accountability chain, governance becomes more transparent. Architectural control aligns with operational responsibility, and the ownership of risk is less likely to be dispersed across multiple external layers.

For organisations operating in regulated sectors, this coherence carries practical implications. Instead of independently assembling complex compliance architectures under conditions of regulatory pressure and cybersecurity talent shortages, enterprises can rely on operational models that have already been developed within stringent governance environments.

In this sense, integrity becomes a transferable operational discipline.

Such an approach does not eliminate complexity entirely, but it introduces architectural reference points that reduce fragmentation and clarify jurisdictional boundaries.

Within a dispersive digital economy, the question organisations increasingly face is not simply whether individual systems are secure. It is whether integrity is embedded structurally across the full digital stack, from the physical infrastructure on which services run to the identities through which actions are authorised.

Operationalising integrity therefore requires more than the addition of security tools. It demands the alignment of infrastructure ownership, identity governance, cybersecurity operations and legal trust frameworks within a coherent design logic.

When these elements operate together, integrity ceases to function merely as a compliance objective. It becomes an organising principle for the digital operating model itself.

CHAPTER 03

Integrity from the Ground Up

Digital integrity cannot be achieved through superficial security layers added to existing systems.

In complex digital environments, trust must be built into the architecture itself, beginning with the physical foundations on which digital infrastructure operates.

At the most fundamental level lies the physical substrate. Data centre design, energy redundancy, environmental safeguards and geographic location determine the baseline resilience of digital operations. Availability is not an abstract service-level objective; it is the outcome of engineered continuity in power, cooling and infrastructure control. Questions of jurisdiction and data sovereignty also begin here, where physical infrastructure determines the legal environment in which digital systems ultimately reside.

Built on top of this foundation is the execution domain, where data and applications operate.

European cloud environments operating under European jurisdiction provide the conditions for controlled workload execution, enabling logical separation, auditable operations and governance across hybrid or multi-cloud architectures. In this context, **sovereignty is not merely a contractual promise but an architectural property shaped by infrastructure ownership, operational control and regulatory alignment**.

Beyond the execution layer lies the dynamic security perimeter. Modern digital environments are continuously exposed to evolving threats across networks, applications and external digital assets.
Managed cybersecurity capabilities, including continuous detection and response, vulnerability management, attack surface monitoring and protection of digital presence, help sustain operational continuity in this environment of constant exposure.

Increasingly, this perimeter also extends to the protection of digital identity and brand presence. Domains, DNS configurations and online identity assets have become critical components of organisational trust.
Fraudulent domains, impersonation campaigns and manipulated digital assets can undermine credibility within hours, making proactive monitoring and rapid response essential to maintaining the integrity of an organisation's digital presence.

At the highest layer sits formal trust infrastructure. Qualified trust services, including digital signatures, electronic seals, timestamps, public key infrastructures and identity frameworks aligned with eIDAS 2.0, translate technical security mechanisms into legally recognised digital actions. These services bind transactions, documents and communications to accountable identities within recognised jurisdictional frameworks.

The emergence of European digital identity wallets, including both citizen and organisational wallets, illustrates how this trust layer is evolving. Rather than serving only as authentication tools, these mechanisms increasingly function as operational instruments through which individuals and organisations manage identity, authorisation and delegated authority within verifiable ecosystems.

Taken together, these layers form an interdependent system. **Physical resilience supports sovereign execution environments; European infrastructure simplifies regulatory compliance; cybersecurity capabilities sustain operational continuity; and trust services establish the legal validity of digital actions**.

Integrity, in this sense, is not a single capability but a systemic property of the entire digital stack. It emerges when infrastructure, security, identity and legal trust mechanisms are designed to operate coherently from the physical foundation to the highest layers of digital interaction.

CHAPTER 04

Compliance by design

For many organisations, compliance remains largely episodic. It tends to appear as an audit-driven process that reveals structural weaknesses only when regulatory scrutiny intensifies. While this approach may have been workable in more stable technological environments, it is becoming increasingly difficult to sustain.

In digital ecosystems shaped by automation, AI systems and complex regulatory frameworks, compliance cannot be treated as a final verification step added after systems are built. Instead, it must be integrated into the design of digital architecture from the outset. Achieving this requires a shift toward compliance by design, in which governance, identity management and cybersecurity controls are embedded structurally across the full technology stack.

In practice, this means that many elements traditionally associated with compliance become foundational components of system architecture.

Logging mechanisms, separation of roles, strong identity management, integrated trust services, business continuity planning and auditable operational workflows are designed into systems rather than layered on afterwards.

Within such an architecture, regulatory requirements arising from frameworks such as NIS2, GDPR, DORA, eIDAS 2.0 and the AI Act are not treated as external constraints. Instead, they are reflected directly in how digital systems function, how access is governed and how operational evidence is generated.

As a result, governance shifts from an occasional audit activity to a continuous operational discipline.

The implications of this transition are not only regulatory but also economic. When compliance is embedded structurally within digital systems, organisations reduce the long-term costs associated with reactive remediation, fragmented tooling and repeated architectural redesign. At the same time, they are able to innovate within clearly defined governance boundaries, accelerating the adoption of new technologies while maintaining control over risk exposure.

Perhaps more importantly, **compliance begins to take on a cultural dimension**.

When security leaders, data protection officers, technology teams and business leadership operate within shared architectural principles, governance becomes aligned with organisational strategy rather than positioned as a constraint upon it. Compliance is no longer perceived solely as a defensive obligation, but as a mechanism through which organisations maintain operational clarity and accountability.

In mature digital ecosystems, governance therefore ceases to function as a source of friction. It becomes part of the design logic that allows complex systems to operate reliably at scale.

CHAPTER 05

Identity as the Core of Integrity

Digital integrity ultimately converges on the question of identity.

Every digital system, whether cloud-native, automated or AI-driven, relies on the ability to attribute actions to identifiable actors operating under defined authority. Without reliable mechanisms for attribution, accountability becomes difficult to establish and governance frameworks lose their effectiveness. Identity therefore functions as the mechanism through which responsibility, authority and traceability are enforced within digital environments.

For human actors, employees, customers and citizens, identity governance requires comprehensive lifecycle management. Secure onboarding procedures, strong authentication mechanisms, granular authorisation controls, traceability of actions and timely revocation of privileges all contribute to maintaining trustworthy digital interactions.

In this sense, identity management extends well beyond authentication. It represents a governance framework that defines how individuals interact with systems and with one another.

At the same time, modern digital architectures introduce a growing number of **non-human identities**. Applications, APIs, services, tenants and cloud workloads all require mechanisms through which they can authenticate and interact securely.

Certificates, cryptographic keys and role-based access policies must therefore reflect the actual responsibilities and operational boundaries within which these entities operate. In distributed systems, service-to-service authentication becomes just as important as traditional user authentication.

The emergence of **machine identities** further expands this landscape. Devices, sensors, containers, automated workflows and increasingly AI-driven agents now perform actions autonomously and at scale. Each of these entities requires a verifiable identity through which its activity can be authenticated, authorised and monitored.
Without structured public key infrastructures and robust lifecycle management, the number of automated interactions can grow faster than the governance mechanisms designed to control them.

Within this evolving environment, AI agents present a particularly important case. Rather than constituting new legal actors, these systems operate as delegated extensions of existing identities and responsibilities.

Their authority derives from explicit delegation mechanisms, including identity wallets, cryptographic attestations and defined policy frameworks, through which organisations specify what actions an automated agent may perform and under what conditions.

This perspective ensures that automation remains anchored in accountable governance structures. Autonomy may increase operational efficiency, but it must remain framed within verifiable authority.

European identity frameworks play an important role in reinforcing this alignment between technical authentication and legal accountability. Qualified trust services and identity mechanisms defined under **eIDAS 2.0**, including digital signatures, electronic seals, timestamps and emerging wallet-based identity models, bind digital actions to identifiable actors within recognised jurisdictional frameworks.

As AI systems increasingly participate in operational and decision-making processes, identity governance becomes a central pillar of digital accountability. Automation that operates without clear identity structures risks generating opacity rather than efficiency.

Organisations that develop coherent identity frameworks preserve their ability to govern complex digital ecosystems. Those that neglect this dimension often find that technological capability grows faster than their capacity to maintain oversight.
A robust identity fabric therefore becomes essential to sustaining strategic control, the ability of organisations to adopt new technologies, scale automated processes and integrate AI systems while retaining control over authority and responsibility.

When identity governance is embedded structurally, innovation remains governable rather than opaque.

As digital ecosystems evolve, several disciplines traditionally treated as separate domains, cybersecurity operations, trust services and brand protection, increasingly converge around a common objective: preserving the integrity of digital identity and the actions performed through it.

Cybersecurity protects the systems and infrastructures through which identities operate. Trust services bind transactions, communications and documents to legally valid identities, preserving intent, authenticity and time. Brand protection safeguards the public expression of organisational identity across domains, communications and digital assets.

Together, these capabilities form complementary layers of Digital Integrity, ensuring that identities, transactions and communications remain **authentic**, **attributable** and **verifiable** across complex digital environments.

CHAPTER 06

Secure strategic control at Scale

The objective of mature digital transformation is not the accumulation of technologies. It is the development of strategic control: the capacity for organisations to choose, compose and govern infrastructure, data, AI systems and identities within clear architectural and jurisdictional boundaries.

In increasingly complex digital ecosystems, the ability to maintain such control is becoming a defining strategic capability.

Systems that scale rapidly but remain opaque or externally dependent may deliver short-term efficiency, yet they often weaken an organisation's capacity to manage risk, comply with evolving regulation and adapt its technological trajectory over time.

Across Europe, emerging initiatives around federated cloud ecosystems and digital sovereignty frameworks illustrate that scale and governance need not be mutually exclusive. Large-scale digital environments can remain interoperable, compliant and resilient without requiring organisations to relinquish control over their infrastructure, identities or data.

When integrity is engineered into the underlying architecture, performance and sovereignty can coexist.

Looking ahead, several structural developments are likely to shape the evolution of digital integrity.

One concerns **cryptographic resilience**. The emergence of quantum computing capabilities is expected to challenge existing encryption models, making long-term cryptographic preparedness an issue of strategic planning rather than a purely technical upgrade. Organisations that begin preparing for post-quantum cryptographic environments today will be better positioned to preserve the durability of their digital trust frameworks.

A second vector involves the **rapid expansion of machine identities**. AI agents, automated workflows and autonomous systems increasingly perform operational tasks across digital infrastructures. Governing these systems requires clear delegation models, lifecycle management and verifiable authority structures capable of ensuring that automated activity remains attributable and accountable.

A third shift relates to the **management of continuous security posture across hybrid and multi-cloud environments**.
As infrastructures become more distributed, resilience can no longer rely on periodic assessments alone. Security oversight must evolve into a continuous process that monitors exposure, adapts to emerging threats and maintains operational integrity across interconnected systems.
Organisations that embed integrity structurally from the outset maintain a degree of technological optionality. They preserve the ability to evolve architectures, integrate new technologies and adopt AI-driven capabilities without accumulating hidden structural risk.

By contrast, systems in which security remains an external overlay often appear to accelerate innovation while gradually increasing fragility.

In this context, security should not be understood merely as a defensive control layer. Properly integrated, it functions as the mechanism through which organisations protect the conditions that allow digital innovation to occur.

From physical infrastructure and cloud execution environments to cybersecurity operations, brand protection and legal trust validation, these mechanisms ultimately converge around the protection of digital identity itself, ensuring that actions performed in the digital world remain authentic, attributable and durable over time.

As Europe's digital ecosystem continues to mature, **trust is increasingly shifting from a reputational attribute to a structural component of infrastructure**.
Organisations capable of engineering this integrity into their systems will be best positioned to sustain innovation while maintaining control over the environments in which they operate.

aruba.it

APPENDIX / A

Trust Services: Legal Validity by Design

appendix

Within the Digital Integrity framework described in this paper, Trust Services provide the legal validation layer that binds digital actions to accountable identities.

Legal Validity by Design

Trust Services form the apex of Digital Integrity. They transform technical actions into legally binding, verifiable reality. In a regulatory environment shaped by eIDAS 2.0, NIS2, GDPR, the AI Act, and national digital frameworks, authenticity and non-repudiation are no longer procedural details, they are structural requirements.

Integrity requires that identity, intent, time and delivery can all be demonstrated and verified.

As a Qualified Trust Service Provider and one of Europe's leading Certification Authorities, with Actalis as the first EU CA, Aruba operates at continental scale.

More than 1.6 billion digital signatures per year and over 10 million certified email (PEC) mailboxes reflect not only market adoption, but systemic relevance.
Trust at this scale is not a feature. It is infrastructure. Trust Services are the legal validation layer of the full digital stack.

Operational Tools for the Integrity Economy
Within the Integrity Economy, Qualified Trust Services are not compliance accessories; they are operational instruments.
Actalis, as a Qualified Trust Service Provider under eIDAS 2.0, and Aruba PEC together form a legally recognized trust infrastructure that guarantees authenticity, integrity, and non-repudiation across digital interactions.

Digital signatures, qualified certificates (QWAC and QSEALc), SSL/TLS encryption, and certified electronic delivery (PEC) provide the immutability and traceability increasingly required under NIS2 governance obligations. In regulated environments, the ability to demonstrate that a transaction is authentic, time-stamped, and unaltered is no longer optional, it is enforceable.

From Technical Security to Legal Certainty
Digital systems can be secure without being legally binding. Trust Services close this gap. Aruba's certified platform integrates digital signatures, timestamps, electronic delivery, digital identity, e-archiving, and compliant e-invoicing into a unified architecture.

Hosted on European infrastructure and embedded into end-to-end security controls, the platform ensures that every interaction is:

- authenticated
- time-stamped
- traceable
- legally valid
- jurisdictionally compliant

This is compliance by design, not by tooling. Rather than treating regulation as an overlay, Trust Services embed regulatory requirements into architectural patterns: native logging, strong identity verification, role segregation, lifecycle governance, and non-repudiable audit trails. Board-level accountability, increasingly formalized under NIS2, becomes operationally demonstrable.

Integrity becomes verifiable.
Aruba's Trust Services can be understood across five complementary guarantees:

1. PROOF OF IDENTITY
Digital identity frameworks, qualified certificates (QWAC, QSEALc), and wallet-based identity systems ensure that actors, individuals, organisations, and delegated agents, are verifiably authenticated.

Identity governance extends across lifecycle management, revocation, and traceability. In an AI-enabled environment, this becomes foundational. An AI agent is not a new legal subject; it is a delegated projection of an accountable identity. Trust Services ensure that delegation remains explicit, bounded, and auditable.

2. PROOF OF INTENT

Qualified electronic signatures and seals bind intention to identity. They eliminate ambiguity in contracts, approvals, authorisations, and formal declarations. Used at scale across private and public sectors, they replace friction with verifiable certainty.

3. PROOF OF TIME

Qualified timestamps anchor digital actions within recognized temporal frameworks. In regulated sectors, this is not procedural detail, it is evidentiary integrity.

4. PROOF OF DELIVERY

Certified electronic delivery (PEC and compliant e-delivery systems) provides legally recognized transmission with non-repudiation. Managing over 10 million PEC mailboxes, Aruba operates one of the core infrastructures of Italian and European digital trust.

5. PROOF OF PRESERVATION

Compliant digital archiving ensures that documents, fiscal, contractual, administrative, remain authentic, accessible, and legally valid across time. Preservation is not storage; it is governed continuity.

Together, these guarantees embed digital trust into every interaction, ensuring integrity, compliance, and resilience.

Digital Identity as the Anchor of Authenticity

In a fragmented trust landscape, identity mechanisms such as SPID, CIE, and the forthcoming European Digital Identity Wallet provide structured identity governance at continental scale. These frameworks ensure that digital signatures, access controls, and certified communications are bound to verifiable, state-recognized identities.

As Europe transitions toward interoperable digital wallets under eIDAS 2.0, identity becomes programmable, portable, and legally enforceable.
Trust Services thus operate not only as validation tools but as identity anchors in an increasingly decentralised digital economy.

Scale, Integration, and Sovereignty

Trust Services are not standalone tools. They are embedded within Aruba's end-to-end architecture. Hosted on Tier IV data centers under European jurisdiction, integrated with European cloud environments and managed cybersecurity services, Trust Services operate within a unified accountability chain. Infrastructure ownership, operational security, and legal validation converge.

This vertical coherence reduces fragmentation. It aligns technical execution with jurisdictional clarity. It transforms compliance into competitive advantage.

At scale, this model supports:

- public sector digital transformation
- regulated industry workflows
- cross-border identity interoperability
- enterprise automation and AI governance

Millions of users and partners rely on this infrastructure daily. Trust, here, is measurable.

Compliance as Competitive Advantage
In many organizations, compliance is episodic and reactive. Trust Services invert this model.

By embedding qualified trust mechanisms from day zero, enterprises reduce audit friction, accelerate market access, and strengthen insurer and investor confidence. Digital signatures replace paper bottlenecks. Certified delivery reduces legal ambiguity. Identity governance clarifies responsibility chains.

Security enables digital evolution. When trust is structurally embedded, innovation does not accumulate risk debt. It operates within verifiable boundaries.

In Europe's integrity economy, this distinction matters. Markets increasingly reward organisations that can demonstrate control over identities, documentation, and legal validity, not merely claim it.

A Composable Path to Integrity
Trust Services are modular by design. Organisations may begin with a single building block, e-signature, PEC, digital identity, or compliant archiving, and progressively integrate broader capabilities across their workflows. As systems mature, trust becomes systemic rather than transactional.

This composable model supports strategic control: the capacity to choose, orchestrate, and evolve digital architecture without surrendering governance.

Integrity, in this context, is not an abstract principle. It is operational discipline.

Legal Validity as Infrastructure
From identity verification to timestamping, from certified delivery to preservation, Aruba's Trust Services translate regulation into architecture and architecture into verifiable trust.

They are the legal validation engine of the full digital stack.

In Europe's maturing digital era, trust is no longer an attribute. It is infrastructure.

And infrastructure, when engineered with integrity, becomes the foundation of secure growth.

APPENDIX / B

Brand Protection

appendix

Within the Digital Integrity framework, Brand Protection safeguards the external expression of organisational identity across domains, communications and digital assets.

Integrity at the Digital Edge

If Trust Services represent the legal validation layer of Digital Integrity, Brand Protection secures its most exposed frontier: the digital edge. Today, reputation travels at network speed. A fraudulent domain, a spoofed email, a cloned website, or an impersonated identity can erode trust within hours. In an environment shaped by AI-enabled phishing, automated impersonation, and increasingly sophisticated social engineering, the brand itself becomes an attack surface.
Digital Integrity therefore extends beyond infrastructure and identity governance. It must protect the visible perimeter where users encounter the organisation.

Brand Protection protects organisational identity where it is most visible: at the digital edge.

The New Attack Surface: Reputation

The digital perimeter is no longer defined by firewalls alone. It includes:

- domains and subdomains;
- DNS configurations;
- trademarks and logos;
- public-facing services;
- email infrastructures;
- online identity assets.

Every domain registered in bad faith, every typo-squatted extension, every impersonation campaign is not merely a technical nuisance, it is a direct assault on reputational capital. In what many analysts describe as a "trust recession," organisations cannot afford reactive protection. Visibility, monitoring, and rapid recovery must become continuous disciplines. Integrity at the edge requires proactive protection.

Domain Management as Strategic Control

Domain governance is often treated as administrative overhead. In reality, it is strategic infrastructure.

Aruba manages over 2.7 million domains and serves as the official registry operator for the cloud extension. This scale reflects not only operational capacity, but jurisdictional and technical authority.

Domain management encompasses:

- registration and renewal across global extensions;
- secure transfer procedures;
- portfolio rationalisation;
- DNS configuration governance;
- lifecycle oversight.

In regulated sectors, domain mismanagement can trigger compliance exposure under NIS2 supply chain obligations. Boards are increasingly required to demonstrate visibility over digital assets beyond core infrastructure. Domain control is therefore not clerical. It is structural.

Continuous Domain Monitoring

In a dispersive digital ecosystem, threats often emerge outside direct organisational boundaries. Domain Monitoring services proactively scan for:

- typo-squatting and lookalike domains;
- fraudulent registrations;
- brand impersonation attempts;
- suspicious DNS activity.

Automated alerting and investigative workflows reduce response time and limit reputational shock.

Rather than waiting for customers or regulators to identify malicious domains, organisations gain early visibility.

Proactive monitoring aligns directly with compliance-by-design principles. Under NIS2 and related frameworks, incident awareness and reporting are not optional; they are mandated. Continuous oversight transforms brand protection from reactive remediation into operational resilience.

Recovery & Brokerage: Regaining Control

When digital assets fall outside legitimate control, through expiration, hostile registration, or legacy fragmentation, recovery becomes a strategic necessity.

Aruba provides negotiation, brokerage, and structured recovery processes for contested or expired domains. This capability is not merely transactional. It restores control over digital identity components that may otherwise undermine long-term brand strategy.
Integrity, in this context, means re-establishing alignment between brand identity and digital presence.

In these situations, control must be actively re-established rather than assumed.

Trademark & Legal Authority

Brand protection extends beyond domains to legal recognition. Trademark verification, registration, monitoring, and renewal across national, European, and international frameworks ensure that brand assets are not only technically managed but legally defensible.

This integration of legal oversight with digital asset governance reflects the broader thesis of Digital Integrity: technical security must align with legal validity.
In regulated environments, the brand itself becomes a governed digital asset.

Integration Across the Full Digital Stack

Brand Protection does not operate in isolation. It integrates with:

- managed cybersecurity operations (SOC, threat intelligence, DDoS mitigation);
- identity governance frameworks;
- trust Services (for verified communications and delivery);
- European infrastructure and DNS control.

When domain monitoring connects to SOC telemetry, response becomes coordinated. When certified delivery mechanisms validate official communications, impersonation risks diminish. When identity governance aligns with brand asset oversight, accountability strengthens.

End-to-end integrity across the full digital stack requires coherence at the edge.

European Infrastructure as the Foundation of Brand Integrity

Brand protection is strengthened when digital assets operate on European infrastructure.

Aruba Enterprise's Private Cloud and Bare Metal environments provide controlled, jurisdictionally anchored infrastructure for data-intensive workloads, Private AI initiatives, and mission-critical applications. In a perimeter-less security model, where data and applications operate across hybrid environments, European infrastructure ensures that DNS control, domain governance, and identity systems remain under direct architectural authority. Integrity at the edge depends on sovereignty at the core.

From Protection to Competitive Advantage

In mature digital markets, trust is measurable. Investors evaluate risk exposure. Insurers assess cyber posture. Regulators examine supply chain controls. Customers expect authenticity.

Brand Protection reduces uncertainty across all these dimensions.

By embedding proactive domain governance, continuous monitoring, and legal alignment into operational models, organisations:

- reduce reputational volatility;
- shorten incident response cycles;
- demonstrate regulatory diligence;
- strengthen stakeholder confidence.

Compliance becomes competitive advantage. Security enables digital evolution.

A Composable Model for Sustainable Trust

Brand Protection services are modular. Organisations may begin with domain consolidation or monitoring and expand toward integrated digital asset governance. As ecosystems scale, brand identity becomes increasingly distributed across platforms, geographies, and partners. Integrity at the edge ensures that expansion does not create unmanaged exposure.

Brand protection must function as a governance discipline rather than a reactive security measure.

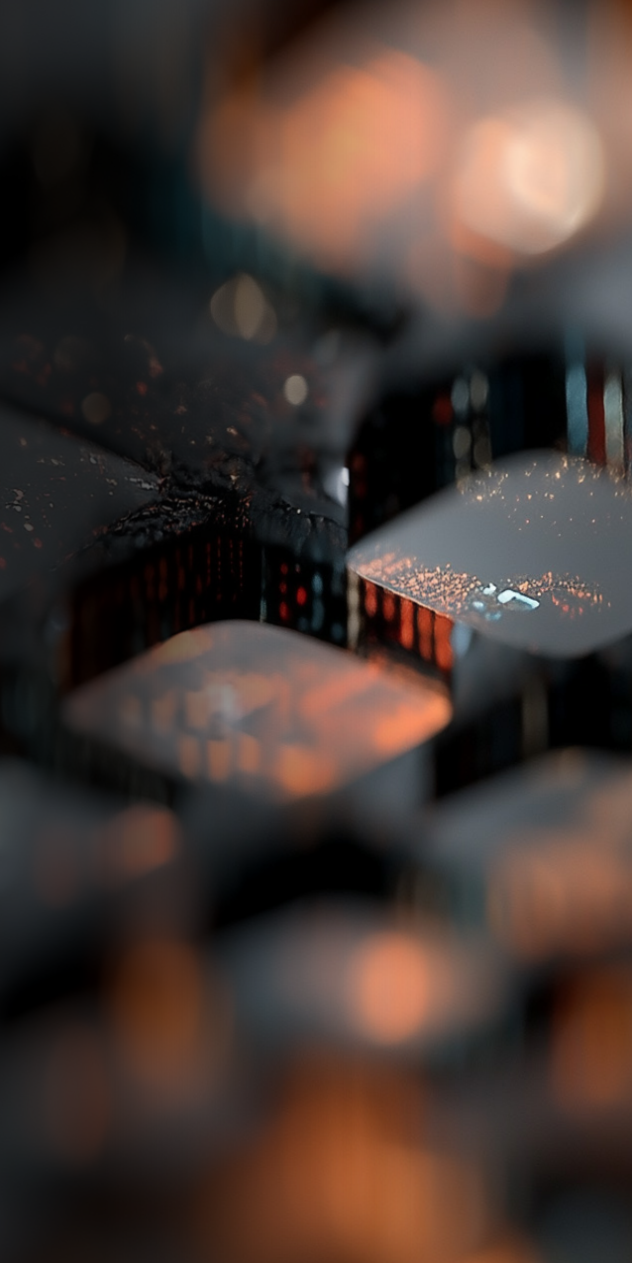
Integrity at the Edge

Digital Integrity is not confined to data centers or identity certificates. It extends to every point where the organisation is visible, searchable, and contactable.

At that edge, trust is fragile.

Brand Protection secures that frontier, preserving authenticity, preventing impersonation, and ensuring that digital presence remains aligned with legal identity and operational accountability. From physical infrastructure to the outermost domain registration, integrity must be continuous.

In Europe's integrity economy, the brand is not only an asset. It is a responsibility.



APPENDIX / C

Cybersecurity

appendix

Within the Digital Integrity framework, Cybersecurity protects the systems and infrastructures through which digital identities operate.

Continuous Resilience at Scale
If Trust Services provide legal validity and Brand Protection secures the digital edge, Cybersecurity operationalises integrity across the dynamic perimeter.

In dispersed, hybrid, and AI-driven ecosystems, security is no longer a boundary function. It is a continuous discipline.

Remote workforces, multi-cloud environments, SaaS dependencies, operational technology, API integrations, and autonomous systems have dissolved the traditional perimeter. Every connection becomes an entry point. Every integration introduces interdependency.

In this environment, resilience cannot rely on static controls. Security must be engineered by design and governed by default.

From Controls to Coherent Resilience

Many organisations assemble cybersecurity as a collection of tools: firewalls, endpoint protection, monitoring dashboards. While necessary, these controls often remain fragmented, generating visibility without unified accountability.

Aruba's cybersecurity model is structured differently.

Aligned with the NIST Cybersecurity Framework, it integrates prevention, detection, response, and recovery into a coherent operating discipline.

Security is not an overlay; it is embedded into infrastructure, identity governance, and operational processes.

Integrity across the full digital stack requires continuity of protection from physical facilities to cloud workloads, from applications to user identities.

Cybersecurity ensures the continuity of that protection.

The Dynamic Perimeter

Modern attack surfaces are fluid. They include:

- cloud-native applications;
- web services and APIs;
- hybrid and multi-cloud architectures;
- industrial and IoT systems;
- user endpoints and remote access environments.

Managing this complexity requires continuous oversight rather than periodic assessment.

Aruba's cybersecurity portfolio combines several operational capabilities designed to secure distributed digital environments:

Vulnerability Assessment & Penetration Testing (VAPT)

Structured vulnerability scans and simulated intrusion testing identify weaknesses before adversaries do.
These exercises are not merely technical diagnostics; they inform compliance readiness under NIS2 and sector-specific regulations.

Web Application Protection (WAP)
Protection mechanisms defend web applications against exploitation attempts, injection attacks, and malicious traffic patterns. In digital ecosystems where customer interaction is primarily web-based, application-layer protection becomes essential to preserving trust.

Managed SOC & Continuous Monitoring
A 24/7 Security Operations Center monitors cloud and on-premise environments, correlating telemetry, analysing anomalies, and coordinating response.
Continuous detection reduces dwell time and transforms incident response into an evidence-based discipline.

MDR & xMDR
Managed Detection and Response services unify visibility across endpoints, networks, cloud workloads, and applications. Extended detection (xMDR) aggregates intelligence across layers, enabling proactive defense against advanced threats.

Anti-DDoS
Mitigation services protect infrastructure from volumetric and application-layer denial-of-service attacks, preserving availability and business continuity.

SSL/TLS Certificate Management
Automated lifecycle management of SSL/TLS and code-signing certificates ensures secure communications and authenticated software distribution. In an era of machine identities and service-to-service trust, certificate governance becomes foundational. Together, these services operationalise security by design.

Compliance Embedded, Not Bolted On
Under European regulatory frameworks, including NIS2, GDPR, DORA, and the AI Act, cybersecurity obligations extend beyond incident response. They encompass:

- risk management;
- supply chain oversight;
- incident reporting;
- business continuity;
- audit traceability.

Security telemetry and logging are therefore not merely defensive instruments; they are governance evidence.
By embedding continuous monitoring, structured vulnerability management, and documented response procedures into operating models, organisations reduce

regulatory friction. Compliance becomes an emergent property of architecture rather than a reactive afterthought.

Compliance by default strengthens executive accountability.
Boards require visibility into risk posture. Regulators require demonstrable controls. Insurers require measurable mitigation strategies. Cybersecurity, when structured coherently, provides this transparency.

Backup and Disaster Recovery as Structural Resilience
Continuous oversight is incomplete without recoverability. Backup and Disaster Recovery services provide the final guarantee of operational integrity when preventive controls fail. Structured data replication, geo-redundant storage, automated recovery testing, and orchestrated failover capabilities transform resilience from theoretical assurance into measurable continuity. In the Integrity Economy, availability is not assumed; it is engineered.

Talent Scarcity and Managed Resilience
Market data consistently highlights a structural shortage of cybersecurity expertise across Europe.
For many organisations, building and sustaining in-house 24/7 capabilities is economically unrealistic. Managed cybersecurity services address this structural constraint.

By leveraging scale, automation, and standardized operating procedures aligned with international frameworks, organisations gain access to enterprise-grade protection without fragmenting governance responsibilities. Security becomes transferable discipline, not dependent on individual staffing cycles.

SOC as Continuous Oversight
Security Operations Center (SOC) services function as the operational nerve center of Digital Integrity. Through real-time monitoring, correlation of threat intelligence, incident response coordination, and documented reporting, the SOC enables continuous oversight across cloud, on-premise, and hybrid infrastructures. In an AI-accelerated threat environment, resilience must be dynamic. The SOC institutionalizes that dynamism.

Integration Across the Stack
Cybersecurity is most effective when integrated. Within Aruba's architecture, cybersecurity services operate in conjunction with:

- European cloud environments;
- Tier IV data center infrastructure;
- Trust Services and identity governance frameworks;
- Brand Protection monitoring.

This vertical coherence reduces gaps between infrastructure, identity, and detection. Incident response aligns with jurisdictional clarity. Certificate governance connects to trust services. Domain monitoring feeds into SOC intelligence. End-to-end integrity is not conceptual. It is operational.

Infrastructure & Cloud as Security Architecture

Aruba Enterprise's Private Cloud and Bare Metal solutions provide the European execution domain required for high-performance workloads, Private AI environments, and data-heavy operations.

In architectures where traditional perimeters dissolve, security must be embedded within compute, storage, and network layers. European infrastructure ensures jurisdictional clarity, workload isolation, and architectural control, enabling perimeter-less security without sacrificing governance.

From Risk Mitigation to Competitive Advantage

In mature digital markets, resilience influences valuation. Investors assess cyber posture.

Customers evaluate data protection commitments. Regulators examine continuity plans. Insurers adjust premiums based on demonstrable controls.

When security is embedded architecturally:

- innovation accelerates within defined risk boundaries;
- audit processes simplify;
- incident response times shorten;
- stakeholder confidence strengthens.

Security enables digital evolution. Rather than constraining growth, cybersecurity safeguards strategic control, the ability to choose, adopt, and orchestrate technologies without accumulating structural fragility.

Integrity in Motion

Cybersecurity is not a static shield. It is a continuous process. Threat landscapes evolve. Attack techniques adapt. Automation scales both risk and defense. In such an environment, resilience must be dynamic.
By aligning with international frameworks, embedding continuous oversight, and integrating detection, response, and identity governance across hybrid environments, Aruba operationalises integrity at scale.
From facilities to certificates, from cloud workloads to endpoints, cybersecurity preserves coherence across the full digital stack.

In Europe's integrity economy, security is not a defensive layer. It is the operational expression of trust. And trust, when engineered systemically, becomes the foundation of sustainable digital growth.

Trust, when engineered systemically, becomes the foundation of sustainable digital growth.

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