

The Right to Information Authenticity

A Missing Institution for the Digital Economy

“Just as secure property rights became one of the institutional foundations of modern economies, trustworthy digital communication is becoming one of the institutional foundations of the digital economy and the age of artificial intelligence.”

Luis Ángel Rodríguez Alemán

Computer Engineer · Master in Public Policy · Master in Regional and Urban Planning
Founder of AliPsé

August 2026

Publication Note

This document proposes the Right to Information Authenticity as a normative and institutional principle for the digital economy. It does not claim that this right is already universally recognized in positive law, nor does it seek to replace copyright, personal-data protection, freedom of expression, due process, or existing rules concerning evidence and electronic signatures. Its purpose is to open an interdisciplinary conversation among jurists, technologists, economists, philosophers, public-policy makers, development institutions, companies, creators, and citizens.

The essay carefully distinguishes authenticity from truth. A communication may be authentic and nevertheless mistaken; it may also be true without having been registered. The proposed capability is narrower: a legitimate person or institution should be able to demonstrate what content it actually issued, and those who receive that content should have a practical opportunity to verify it without surrendering their freedom to interpret, criticize, transform, or reject it.

Title	The Right to Information Authenticity: A Missing Institution for the Digital Economy
Series	AliPsé White Paper No. 1
Author	Luis Ángel Rodríguez Alemán
Version	Publication edition, August 2026
Suggested citation	Rodríguez Alemán, Luis Ángel (2026). The Right to Information Authenticity: A Missing Institution for the Digital Economy. AliPsé White Paper No. 1.

© 2026 Luis Ángel Rodríguez Alemán / AliPsé. Quotation and partial reproduction are authorized with proper attribution. Full reproduction, translation, or adaptation for commercial purposes requires prior authorization. Contact: luisangel@alipse.net · www.alipse.net

Abstract

The Internet became the dominant infrastructure for distributing information without acquiring an equally universal infrastructure for authenticating it. From the outset, this architectural gap enabled forgery, impersonation, and manipulation; generative artificial intelligence did not create the problem, but it industrialized it by radically reducing its cost, time, and technical difficulty.

This essay argues that information authenticity is not merely a technological problem. It is a condition of possibility for large-scale human cooperation. The principal strength of *Homo sapiens* does not lie in individual physical capacity, but in the ability to coordinate with large numbers of people, share knowledge, create institutions, and act upon common realities. That cooperation depends on language, the attribution of responsibility, and a sufficient degree of trust in source identity, message integrity, and continuity of provenance.

The essay therefore proposes the Right to Information Authenticity: a normative and institutional principle under which every person or organization should have reasonable means to establish, preserve, and demonstrate which content, words, images, sounds, or communications it actually issued, and to distinguish them from altered, fabricated, or falsely attributed versions. The proposed right protects attribution and communication integrity; it does not grant infallibility to the issuer or authorize the imposition of an official truth.

The document examines the digital dimension as an instrumental extension of physical life—the “4.5 dimension” proposed by the author; analyzes the personal, economic, democratic, and institutional costs of inauthenticity; proposes an open architecture of registries, certification, public verification, and detection; and sets out safeguards against censorship, surveillance, centralization, and false certainty. AliPsé appears at the end as a concrete implementation hypothesis for an institution that, because of its importance, must transcend any individual company, government, or platform.

Keywords: information authenticity; fake news; digital trust; human cooperation; provenance; content integrity; 4.5 dimension; digital public infrastructure; generative artificial intelligence; institutional resilience; post-quantum cryptography.

Contents

Prologue. The Right to Our Own Words	5	11. Governments, Public Services, and Institutional Communication	12
1. Civilization, Cooperation, and Institutions	5	12. Democracy, Elections, and the Public Sphere	12
2. The Internet: The Most Powerful Megaphone in History	6	13. The Missing Institution of the Digital Economy	13
3. The Liquid, the Ephemeral, and the Fragility of the Word	7	14. Principles of Authenticity Infrastructure	13
4. The 4.5 Dimension of Human Existence	7	15. Risks, Safeguards, and Limits	14
5. The Historical Evolution of the Authenticity Crisis	8	16. AliPisé as an Implementation Hypothesis	15
6. Words, Ideas, and Communicative Identity	9	Conclusion. Who Will Protect Our Words?	16
7. Authenticity Is Not Truth	9	Notes and References	18
8. The Right to Information Authenticity	10	Selected Bibliography and Institutional Sources	19
9. From Certainty About Property to Certainty About Attribution	10	About the Author	20
10. The Social and Economic Costs of Inauthenticity	11		

Prologue

What does it mean to preserve the right to our own words?

The Right to Our Own Words

The idea that would eventually become AliPsé began to take shape during the lockdown caused by the COVID-19 pandemic. In those months, much of human life changed settings almost overnight: work, education, health information, commerce, personal relationships, public deliberation, and even society's most intimate rituals moved into the digital dimension.

Lockdown also revealed another, less obvious transformation. In a world marked by speed, instability, and continual replacement, it seemed increasingly difficult to retain genuine control over what we considered our own. Jobs could disappear; bonds became more fragile; platforms controlled data, audiences, and memory; images circulated out of context; a sentence could be clipped until it acquired the opposite meaning; a screenshot could outlive its source; a fake account could speak in the voice of a real person.

From that observation arose a very simple intuition: even if contemporary life makes ownership of many things more uncertain, people should retain, at the very least, the right to their own words. There should be a trustworthy way to demonstrate: "This is what I actually said," "This is the image I published," "This statement came from my institution," "These words were never mine."

A word is not a trivial object. Through words we express ideas, intentions, commitments, knowledge, affections, disagreements, and projects. People cannot be reduced to their words, but a substantial part of their public identity, shared thought, and capacity to participate in social life is manifested through them. When someone succeeds in putting false words into another person's mouth and making them indistinguishable from authentic ones, the act does not merely alter a file: it interferes with the continuity of that person's communicative identity.

This essay therefore begins with a question that appears technological, but is in fact civilizational:

In a civilization that has built institutions to protect property, contracts, identity, and money, what institution protects the authenticity of the words, ideas, and communications of people and organizations in the digital dimension?

The answer developed in the following pages is uncomfortable: that institution does not yet exist in a universal, accessible, interoperable, and independent form. And while it remains absent, the problem will not remain static. As with many institutional deficiencies, it will tend to worsen over time, with the expansion of digital life and the development of technologies capable of fabricating the appearance of authenticity with ever greater precision.

1. Civilization, Cooperation, and Institutions

What enabled human beings to cooperate beyond small groups?

Civilization is, to a large extent, the product of accumulated cooperation. No individual, however intelligent or capable, can build a city, a university, a health system, an electrical grid, cumulative science, or the rule of law alone. Societies prosper when they coordinate efforts among people who do not know one another, live in different places, and may even belong to different generations.

Yuval Noah Harari has popularized the thesis that the singular advantage of *Homo sapiens* is not simply cooperation—many species cooperate—but flexible cooperation in large numbers through shared narratives, rules, and institutions.¹

That capacity for coordination does not depend solely on individual intelligence. It depends on language, memory, the ability to make promises, attribute responsibility, and share representations of reality. A society can organize taxes, hospitals,

schools, elections, or supply chains because millions of people recognize symbols, rules, authorities, documents, and statements endowed with sufficiently common meaning.

Cooperation is one of the great powers of our species. Language made that cooperation possible; institutions extended it beyond small groups; and trust made it sustainable over time. From this follows a central proposition of this essay:

Large-scale human cooperation depends on communication; communication capable of coordinating action requires a sufficient degree of trust; and that trust deteriorates when we can no longer distinguish words that were authentically issued from words that were falsely attributed.



Figure 1. Conceptual chain of large-scale human cooperation.

Institutions perform precisely a stabilizing function. Douglass C. North described them as the formal and informal rules that structure human interaction and reduce uncertainty. Property rights clarify ownership; contracts make commitments enforceable; public registries preserve legal acts and statuses; courts resolve disputes; monetary institutions sustain expectations about value.²

Not all institutions are just, effective, or neutral. Some distribute power unequally; others preserve privilege or become obsolete. But the general lesson remains valid: without credible mechanisms for establishing rights, responsibilities, and records, the costs of coordination rise and the capacity for long-term planning declines.

Information authenticity therefore belongs in a conversation about institutions, not merely software. When a communication can be falsely attributed to an issuer and there is no practical method for comparing it with an authorized version, uncertainty increases around one of the raw materials of cooperation: who said what, when, and in what form.

2. The Internet: The Most Powerful Megaphone in History

What changed when anyone could speak to millions of strangers?

Never before in history could a single person speak, at the same time, to millions of strangers. For centuries, reaching a mass audience required control of a printing press, radio station, television channel, publishing house, or political structure. The Internet radically lowered those barriers. A person with a phone can address a community, document abuse, organize assistance, create knowledge, or participate in a global conversation.

This capability has had profound political consequences. Social movements, protests, campaigns, and solidarity networks have used digital connectivity to coordinate action and challenge traditional information monopolies. The power of the Internet lies not only in transporting messages, but in changing who can produce them, who can receive them, and how quickly they can generate a collective response.

But the same design that favors openness, copying, and recombination makes provenance difficult to preserve. A file can be downloaded, cropped, translated, recompressed, and republished. A statement can be separated from its context. An authentic image can be paired with a false caption. Audio can be edited to reverse its meaning. Content retains its persuasive power even after losing its history.

The network became extraordinarily efficient at answering the question, “How do I deliver this message to millions of people?” but did not develop an equally simple answer to, “How do I demonstrate that this was actually my message?”

Humanity acquired the most powerful megaphone in its history without simultaneously building a widely available capacity to preserve and verify continuity between the source, the message, and the versions that reach its audiences. That asymmetry is the architectural root of the authenticity crisis.

3. The Liquid, the Ephemeral, and the Fragility of the Word

What happens to authorship when everything circulates, changes, and is recontextualized?

Contemporary life appears to have lost many of its former solid forms. Zygmunt Bauman used the metaphor of “liquid modernity” to describe the transition toward conditions marked by flexibility, uncertainty, mobility, and fragile bonds. In his work, liquidity reaches employment, identity, relationships, consumption, and the experience of time itself.³

One need not accept every implication of that theory to recognize that much of contemporary life is experienced as provisional. Platforms change their rules; digital identities fragment; memory is externalized; employment and emotional bonds are reorganized; published material may disappear and, paradoxically, may also remain forever beyond the control of the person who issued it.

In this environment, even one’s own words become liquid. They can circulate without a stable medium, detach from their context, and acquire successive versions. The fragility lies not only in words disappearing, but in their continuing to exist in forms that no longer correspond to what was issued while their attribution may still appear authentic.

The digital world paradoxically combines the ephemeral and the indelible. A message may be visible for only seconds and, at the same time, be captured, reproduced, and recontextualized indefinitely. This tension makes the traditional idea that a later denial repairs the damage insufficient. A forgery may have reached millions before the original is located; the manipulated version may outlive the context that made it understandable.

Liquid modernity does not cause the authenticity crisis, but it helps explain the cultural environment in which it unfolds: a world in which permanence, authorship, and continuity are more difficult to secure. For precisely that reason, digital society needs institutions capable of making verifiable what it can no longer make solid.

4. The 4.5 Dimension of Human Existence

Why does protecting authenticity in the digital dimension matter?

Digital life no longer takes place outside life. We work, learn, shop, save, form relationships, exercise rights, build reputations, and participate politically in digital spaces. A growing share of the consequences we experience in the physical world originate in interactions that began on a screen.

I have called this condition the “4.5 dimension.” It is neither a dimension completely separate from physical life nor a mere spatial metaphor. It is an instrumental extension of our existence: a realm that multiplies the possibilities of the material world, partially removes the constraints of distance and time, and produces effects that continually return to the body, the economy, reputation, health, and political life. The concept was initially developed in the chapter “Computing in an Interdisciplinary World” (Rodríguez Alemán, 2016).

The term 4.5 seeks to reflect this intermediate condition. The digital dimension does not replace physical dimensions or constitute a self-sufficient reality; but neither can it be reduced to a secondary channel. A banking decision made online changes physical wealth. A forgery spread through a network can cause violence in a street. A digital health alert can save lives. A fabricated statement can move markets or alter an election.

The importance of protecting authenticity in the digital dimension therefore follows from an elementary reason: that dimension is already part of human life. Asking why it matters to protect words on the Internet is largely equivalent to asking why it matters to protect people’s actions, rights, and identities in any sphere where their existence produces real consequences.

If rights and institutions were created to make physical life more secure, their functional equivalents must extend into the space where a growing part of that life takes place. Identity, privacy, property, evidence, security, and authenticity do not lose relevance when they cross a screen; on the contrary, they must be reconstructed for a medium with different properties.

5. The Historical Evolution of the Authenticity Crisis

How did forgery move from a costly practice to an industrial capability?

Forgery is ancient. Its contemporary scale is not. Human history is filled with fabricated documents, rumors, propaganda, impersonations, and accounts attributed to authorities that never issued them. What has changed is not the existence of deception, but its economics: who can produce it, how much it costs, how quickly it circulates, and how convincing it can become.

A cumulative evolution can be distinguished in four stages. Each adds capabilities and risks without completely replacing the previous ones:

Stage 1 — Analog Communication

Manipulation was possible, but it usually required access to physical media, specialized skills, or distribution channels. Forging a photograph, document, or recording could be expensive and leave material traces. Scale was limited by printing presses, tapes, laboratories, transmitters, or organizational networks.

Stage 2 — Digitization and the Internet

Copying, editing, and redistributing became inexpensive. The digital copy lost visible differences from the original. Content could circulate globally and become separated from its medium, date, author, and context. The network made it possible for an alteration made by one person to reach audiences once reserved for large organizations.

Stage 3 — Social Networks and Instant Messaging

Distribution became algorithmic, emotional, and nearly instantaneous. Content ceased to travel mainly as formal publication and began to move as forwarded fragments, screenshots, memes, clips, or audio. The speed of propagation surpassed the capacity for verification, while social signals—who sends it, how many times it is shared, how much outrage it produces—began to substitute for evidence of origin. The phenomenon popularly described as fake news is a visible manifestation of this transformation, but it does not exhaust the institutional problem that made it possible.

Stage 4 — Generative Artificial Intelligence

Convincing fabrication became accessible, automatable, and scalable. Voices, faces, writing styles, documents, and scenes can be synthesized or altered with minimal investment. An attacker can produce multiple variants adapted to languages, audiences, and platforms. Artificial intelligence did not create the authenticity crisis: it industrialized it.

This evolution shows why responses focused exclusively on “detecting AI-generated content” are insufficient. Legitimate institutions also use generative tools to create official materials; malicious actors combine AI with traditional editing; and a forgery can be created from scratch or derived from an authentic original. The operational question is not which brand of software produced the file. It is whether the circulating content corresponds to a reference version that the legitimate source registered or recognized as its own.



Figure 2. Cumulative evolution of the authenticity crisis.

6. Words, Ideas, and Communicative Identity

What are we really protecting when we protect the authenticity of words?

Words do not merely describe the world: they also act upon it. Through them we promise, command, authorize, educate, condemn, forgive, contract, legislate, and organize. Much of institutional life exists because certain words are spoken or recorded by people vested with recognized authority.

A law is language. A contract is language. A judgment is language. An academic degree, a medical prescription, an emergency alert, and a central-bank statement are symbolic expressions that produce effects because a community recognizes their origin and authority.

Wittgenstein wrote that the limits of his language meant the limits of his world. Hannah Arendt placed speech and action at the center of people's public appearance. Habermas developed a theory of communicative action in which social cooperation depends on validity claims that can be discussed.⁴

It is unnecessary to claim that people “are” only their words. We are also bodies, memory, relationships, actions, and silences. But a substantial part of our public identity and social participation is expressed through communications that others attribute to us. The continuity of that attribution forms what may be called communicative identity: the possibility of being recognized over time by what we actually said, published, authorized, or denied.

When a society loses the ability to distinguish words authentically issued by a person from those falsely attributed to them, more than a reputation is placed at risk. One of the mechanisms through which people cooperate, deliberate, assume responsibility, and build shared memory is weakened.

Protecting the authenticity of our words means protecting the symbolic infrastructure of human cooperation.

7. Authenticity Is Not Truth

Can a communication be authentic and nevertheless mistaken?

Authenticity and truth are not the same. This is the essay's most important distinction. An authentic communication is one that genuinely corresponds to the source to which it is attributed. That does not guarantee that its content is correct, complete, legal, moral, or scientifically true.

A government can authentically issue an incorrect statistic. A company can authentically publish a promise it later breaks. A person can authentically say something false. Authenticity infrastructure does not turn those statements into truth; it merely makes it possible to establish that they were in fact issued by that source.

This limitation does not weaken the proposed right. It makes it viable and compatible with a plural society. An infrastructure that attempted to determine the absolute truth of every statement would have to concentrate epistemic and political power incompatible with freedom. By contrast, an infrastructure that demonstrates provenance answers a narrower and verifiable question: “Does this content match the version issued by this source?”

Four concepts that are often confused should be distinguished. Identity answers who claims to be the source; integrity indicates whether the bits or evidence have changed; provenance reconstructs origin and known transformations; and authenticity expresses the sufficiently supported correspondence between content and the source to which it is attributed. None of these elements, by itself, determines the truth of what is asserted.

Authenticity also does not replace journalism, science, courts, public debate, or fact-checking. It complements them. First, it can be established what an institution actually said; then it can be debated whether it was correct, acted lawfully, or deserves trust.

This distinction prevents the Right to Information Authenticity from becoming a “ministry of truth.” The infrastructure should not decide which ideas may circulate, but should make the relationship between content and its source visible.

Criticism, satire, parody, quotation, transformation, and disagreement must remain open, provided they are not deceptively presented as the unaltered original.

8. The Right to Information Authenticity

What minimum capabilities should an authenticity institution recognize?

The proposal can be stated simply: every person and every organization should have proportionate means to demonstrate what their communications actually were. We call that normative principle, and the institutional capability intended to make it effective, the Right to Information Authenticity:

Every person or organization should have a practical capability to establish, preserve, and verifiably demonstrate which content, words, images, sounds, or communications it actually issued; and every person who receives such content should have a reasonable opportunity to determine whether it corresponds to a reference version recognized by the source.

At this initial stage, this right should be understood as an institutional aspiration and a design criterion, not as a premature assertion of a new universal cause of action. It can guide standards, technological architecture, public procurement, corporate governance, research, and public policy before any general legal recognition exists.

The proposed right contains at least four dimensions:

These dimensions should not necessarily be understood as four independent subjective rights. At this stage, they function as components of a single institutional capability and as criteria for evaluating rules, products, and public policies.

1. Evidence of issuance: the capability to leave evidence of which communication was issued by a legitimate or authorized source.
2. Preservation: the capability to retain durable evidence of the issued version, even when platforms, formats, or institutional officers change.
3. Verification: the possibility for third parties to confirm correspondence with a registered reference through accessible channels, without depending exclusively on a later statement by the issuer itself.
4. Verifiable disavowal: the capability to provide evidence that a fabricated, altered, or falsely attributed version does not correspond to the communication registered by the source.

A mature implementation should avoid false binarism and provide for at least four outcomes: authentic match; material alteration detected; content not found; and insufficient evidence. Absence from a registry does not prove falsity, just as technical uncertainty should not be hidden behind a categorical answer.

Evidence of issuance Record which communication the source recognizes as its own.	Preservation Preserve durable evidence of the reference version.
Verification Allow third parties to verify attribution with low friction.	Verifiable disavowal Demonstrate that an altered or fabricated version was not issued by the source.

Figure 3. Functional dimensions of the Right to Information Authenticity.

The value of the right does not lie in guaranteeing that no one will attempt forgery. Institutions rarely eliminate the conduct they regulate entirely. Their purpose is to reduce the success of deception, lower verification costs, and restore to the legitimate source an evidentiary capability that today often arrives too late.

9. From Certainty About Property to Certainty About Attribution

Can the digital economy prosper without sufficient certainty about who said what?

The analogy with property rights is powerful, but it requires precision. Information is not identical to a plot of land, a house, or a machine; ideas can be shared without depriving their original holder of their use; and freedom of expression limits any claim to total control over language.

For the same reason, speaking of a “right to one’s own words” does not mean granting the issuer perpetual dominion over every quotation, interpretation, or transformation. It means recognizing a legitimate interest in allowing the attribution of the original message to be established and contested through evidence.

The analogy does not lie in claiming that every word should be capable of ownership. It lies in institutional functions. Property rights make it possible to attribute, register, transfer, defend, and resolve disputes concerning certain assets. They reduce uncertainty about who may do what and on what basis.

Information authenticity requires functionally similar capabilities: attributing a communication; registering its version of origin; preserving evidence; verifying the correspondence of a copy; identifying alterations; and resolving disputes when there are errors, compromised keys, or competing claims.

Just as economic development required institutions that reduced uncertainty about who owned what, the digital economy needs institutions that reduce uncertainty about who said what.

This formulation does not seek to turn every communication into exclusive property. It seeks to protect attribution. A person may quote, criticize, or transform a speech, but should not be able to present the transformation as though it were the original speech. A platform may host content, but should not be the sole authority capable of demonstrating its origin. An institution may correct a statement, but the history of versions should remain verifiable.

The Right to Information Authenticity therefore complements copyright, electronic signatures, identity protection, the right of reply, and rules of evidence. Each protects a different dimension. Its specific contribution is to make continuity between the source and the circulating version verifiable for the ordinary public and at Internet scale.

10. The Social and Economic Costs of Inauthenticity

When does a digital forgery cease to be intangible?

A forgery appears intangible until someone acts upon it. Fabricated audio can trigger a fraudulent transfer; a false statement can affect a market price; a manipulated health alert can discourage vaccination; a false evacuation order can cause panic; a video attributed to a candidate can alter electoral preferences.

The first cost is uncertainty. When recipients cannot quickly determine whether a communication is authentic, they must invest time, knowledge, and resources in verifying it. Every critical message generates search, confirmation, and coordination costs. Institutions must activate crisis teams; the media must locate sources; citizens must decide whether to wait or act.

The second cost is asymmetric speed. A forgery can be distributed in seconds; clarification usually requires locating the content, analyzing it, obtaining authorization, and reaching an audience that has already fragmented. The correction rarely follows the same path or generates the same emotional attention as the initial deception.

The third cost is the generalized erosion of trust. When the public learns that any image, audio recording, or document can be forged, the so-called “liar’s dividend” emerges: even authentic content can be dismissed as artificial. The crisis no longer consists only in believing what is false; it also consists in ceasing to believe what is true.

In markets, this dynamic can produce “trust runs.” Economic theory on bank runs showed how expectations and rumors can coordinate behavior that ultimately materializes a crisis. In the digital economy, a communication attributed to a company, central bank, or authority can trigger decisions before there is time to verify it.⁵

Authenticity infrastructure can reduce these costs by providing an early point of reference. It does not eliminate judgment or guarantee compliance, but it shortens the path between doubt and evidence. In situations where minutes matter, that reduction can have significant economic and social value.

11. Governments, Public Services, and Institutional Communication

What happens when the voice of an institution that serves millions is forged?

Few organizations speak daily to audiences as large as those addressed by governments. And their role is not limited to security, defense, taxation, or regulation. In many countries, public institutions form the backbone of healthcare, education, social protection, scientific research, culture, information, and economic infrastructure.

States operate hospitals, health centers, laboratories, vaccination campaigns, schools, universities, scholarship systems, civil registries, courts, central banks, tax authorities, transportation networks, civil-protection systems, meteorological services, public media, television channels, and national news agencies. Each of these institutions communicates instructions, decisions, and data that can affect millions of people.

Governments are also moving an increasing number of procedures and services online. Digital identity, tax filings, records, medical appointments, school enrollment, licenses, payments, alerts, and inquiries are handled through digital platforms. Communication authenticity ceases to be a matter of institutional image and becomes a condition of operational continuity and access to rights.

A false public-health statement can alter health behavior; a fabricated educational announcement can defraud families; a manipulated emergency alert can place lives at risk; a false regulatory circular can affect markets; a fabricated news report attributed to public media can be amplified by the legitimacy of the State.

Governments already conduct a growing share of their activity in the 4.5 dimension. Therefore, “making trust native to the Internet” is not an abstract aspiration: it means equipping digital public services with mechanisms of provenance, integrity, and verification equivalent to the registries, seals, and formalities that sustained public action in the physical world for centuries.

The infrastructure must, however, be designed not to confuse governmental authenticity with governmental truth. Citizens should be able to demonstrate that a statement came from an authority while preserving their full right to question it. Verification strengthens accountability precisely because it establishes what the institution said at a particular moment.

12. Democracy, Elections, and the Public Sphere

Can democratic deliberation exist when the attribution of words is uncertain?

Democracy requires knowing who held which position. Citizens evaluate candidates and governments by what they say and do; parties compete through proposals; electoral authorities communicate rules, dates, and results; the media document statements and events.

Manipulation of these communications can distort deliberation before a vote is cast. An altered video can attribute to a candidate a position they never held; synthetic audio can fabricate a confession; false electoral instructions can discourage participation; a forged statement can sow doubt about a result.

Hannah Arendt emphasized the role of speech and action in the public sphere; Habermas linked democratic legitimacy to processes of deliberation in which participants can formulate and discuss validity claims. Authenticity does not guarantee rational deliberation, but its absence makes it more difficult even to know who is participating and what position they actually defended.⁶

The right to authenticity must not be used to privilege official voices over dissenting ones. A democracy needs legitimate anonymity, investigative journalism, satire, public-interest leaks, and whistleblower protection. The architecture must distinguish between concealing one's identity for protection and impersonating another person's identity to deceive.

The specific contribution of electoral-authenticity infrastructure would be to enable candidates, parties, authorities, and media organizations to establish verifiable versions of their communications, and allow citizens to consult those references through everyday channels. It would not by itself resolve polarization or propaganda, but it would reduce a particularly corrosive form of manipulation: successfully attributing to another person words they never uttered.

A public sphere unable to recognize the authorship of its messages loses the minimum basis for assigning responsibility. And without attributable responsibility, freedom of expression risks becoming freedom to speak through another person's identity.

13. The Missing Institution of the Digital Economy

What piece is still missing from the institutional architecture of the Internet?

Recognizing the problem requires thinking in terms of an institution, not a single tool. The solution cannot depend on one platform, an artificial-intelligence company, or a central authority that determines truth. Nor can it be reduced to a detection algorithm: every probabilistic technique makes errors, and every signal can disappear when formats change.

The missing institution should be conceived as an ecosystem of interoperable capabilities: legitimate issuer identity, origin registration, cryptographic evidence, provenance, universal verification, alteration detection, governance, auditing, and correction mechanisms.

Provenance standards such as C2PA and Content Credentials are important advances. Watermarking systems from AI providers also contribute useful signals. But the real life of content takes place outside ideal environments: files forwarded through messaging applications, screenshots, printed and scanned documents, excerpts, translations, clips, and recompressions. The institution must integrate multiple signals and continue functioning when some of them are lost.⁷

The institution should not be confused with a single database either. A healthy model should allow plural registries that share standards, trust mechanisms, and resolution processes. Neutrality and interoperability are indispensable so that authenticity does not depend on the platform on which content was created or published.

The aspiration can be summarized in one idea: verifying the provenance of a digital communication should become as ordinary as checking a website's secure connection. Not because the two problems are technically identical, but because trust works best when it is integrated into ordinary use rather than reserved for specialists.

14. Principles of Authenticity Infrastructure

What capabilities must trustworthy infrastructure combine?

Internet-scale authenticity infrastructure can be understood through six components and several cross-cutting properties.

1. Legitimate Issuer Identity

The system must establish who is authorized to register content on behalf of a person or organization. In complex institutions, identity is not enough: roles, delegations, separation of duties, periods of validity, and revocation are also required.

2. Origin registration

The source should be able to declare and register a reference version before or at the time of publication, with sufficient date, context, and metadata. That reference status establishes which version the source recognizes as issued; it does not make it true or legally superior to all subsequent evidence. The registry need not always store the complete content: it may preserve fingerprints and references under privacy and retention rules.

3. Cryptographic evidence

Digital signatures, hash functions, timestamps, and tamper-resistant records should be combined to corroborate integrity, technical authorship, and the temporal sequence of evidence. None of these elements, used in isolation, resolves the entire chain of trust. Security must include key custody, hardware modules, recovery, rotation, revocation, and compromise response.

4. Universal verification

Evidence loses much of its value if ordinary citizens cannot use it. Verification should be available through the web, APIs, and messaging channels, ideally without payment, specialized knowledge, or a required user profile.

5. Alteration detection

When content does not match exactly, perceptual hashing, fingerprints, forensic analysis, similarity models, and multimodal detection can identify relationships to an original. Their results must express uncertainty and be subject to adversarial evaluation.

6. Governance and due process

Procedures must exist for corrections, revocations, disputes, changes of government, mergers, institutional dissolution, and credential compromise. Trustworthy infrastructure needs rules as robust as its algorithms.

Cross-Cutting Properties

- Interoperability and openness: documented APIs, open standards, and portability.
- Privacy by design: data minimization and verification without unnecessary surveillance.
- Accessibility: languages, disability, limited connectivity, and diverse levels of digital literacy.
- Cryptographic agility: the ability to change algorithms without invalidating the entire system.
- Post-quantum resilience: progressive adoption of NIST standards according to function—for example, ML-DSA or SLH-DSA for signatures and ML-KEM for key establishment when confidentiality is required—together with strategies for transition, renewal, and cryptographic coexistence. The objective is to reduce future risks of signature forgery and retrospective exposure of protected information.⁸
- Long-term preservation: renewal of attestations, auditable archives, and institutional continuity.

The combination of these elements must avoid a common illusion: believing that a single tool will solve an institutional problem. Authenticity is a chain. Failure in identity, key custody, the verification interface, or governance is enough to weaken trust.

1. Legitimate identity Links the source to a recognizable authority.	2. Origin registration Preserves a reference version and its context.
3. Cryptographic evidence Protects integrity, signature, and timing.	4. Universal verification Enables low-friction authenticity checks.
5. Alteration detection Relates modified versions to their references.	6. Governance and due process Corrects errors, resolves disputes, and limits abuse.

Figure 4. Components of authenticity infrastructure.

Cross-cutting properties: interoperability · privacy · accessibility · cryptographic agility · post-quantum resilience

15. Risks, Safeguards, and Limits

How can trust be built without creating censorship, surveillance, or concentrations of power?

Every trust infrastructure also contains a possibility of power. Its safeguards should therefore not be added at the end: they must be part of the architecture from the beginning.

Do Not Become Censorship

The system should establish provenance, not decide which ideas may circulate. Unregistered content must be able to exist and be expressed. The label “not found” must not become synonymous with false or prohibited.

Do Not Create a Universal Authority of Truth

No company, government, or platform should hold a monopoly over truth. Registries should be plural, auditable, and interoperable. Technical authenticity should not displace human judgment, investigation, or debate.

Protect Anonymity and Freedom of Expression

Protecting attribution does not imply requiring public identity from everyone. Journalists, whistleblowers, victims, and dissidents may need anonymity. The system must prevent impersonation without turning every expression into mandatorily identified communication.

Minimize Personal Data

Public verification must not become a mechanism for profiling who consults what. Unnecessary collection of verifier identity, location, contacts, or behavior should be avoided.

Express Uncertainty

Detection systems should distinguish exact match, similarity, probable alteration, absence of a reference, and insufficient evidence. Conceptual humility is a safeguard: a technical result is never equivalent to omniscience.

Guarantee Correction and Appeal

A source may register content in error, a key may be stolen, and an institution may change authorities. Procedures for revocation, correction, auditing, traceability, and dispute resolution must exist.

Avoid Structural Exclusion

If only large organizations can certify content, the infrastructure will reproduce inequalities. Proportionate mechanisms must exist for individuals, small businesses, communities, local media, and civil-society organizations.

The goal is not an Internet in which everything must be certified. It is an Internet in which legitimate sources can demonstrate what they issued, and people can verify it when the consequences justify doing so.

16. AliPsé as an Implementation Hypothesis

How can an institutional idea become a simple and useful experience?

AliPsé was born from the intuition that opens this essay: people and institutions should retain a practical right to their own words in the digital dimension. Its aspiration is to materialize that idea through open infrastructure that is agnostic to the tools used to create content.

The hypothesis is deliberately simple. It combines four capabilities: a registry of authentic content; certification at origin; low-friction public verification; and an intelligence layer capable of identifying alterations or relationships to registered

versions. Institutional clients would register—or “AliPseal”—their communications before publication; users could “AliPse-check” content and determine whether it matches an authentic reference.

The model distinguishes between those who fund the system and those who verify. Organizations pay for registry, certification, integration, and compliance services; public verification should be free and, whenever possible, require no login. This structure seeks to reduce transaction costs and foster a network effect: every authentic item registered increases the system’s usefulness for all verifiers.

AliPsé does not seek to replace C2PA, Content Credentials, SynthID, OpenAI Verify, or other technologies. It treats them as signals that can be integrated into a broader architecture. AliPsé’s question is not merely “Which tool produced this?” but “Does this content correspond to a version that the legitimate source registered or recognized as its own?”

The proposal must be evaluated rigorously. It will be necessary to demonstrate accuracy, adversarial resilience, institutional adoption, citizen utility, economic sustainability, rights protection, and independent governance. AliPsé is an implementation hypothesis, not the only possible way to build the institution described in this document.

Information authenticity is too important to belong exclusively to one company, platform, or government. If it becomes a native capability of the Internet, it will have to rest on open standards, competition, cooperation, and control mechanisms sufficient to outlive any one of its participants.

Standards and signals C2PA · Content Credentials · signatures · watermarks	Legitimate sources Individuals · governments · media · companies	Distribution channels Web · social networks · messaging · APIs
Registry and verification AliPsé and other interoperable services	Users and audiences Citizens · customers · journalists · authorities	Governance Auditing · competition · correction · due process
Digital trust does not depend on a single technology: it emerges from a plural, interoperable, and verifiable ecosystem.		

Figure 5. Open ecosystem of authenticity and digital trust.

Conclusion

Who Will Protect Our Words?

For centuries, societies built institutions to protect property, make contracts enforceable, preserve identity, stabilize money, and record legal acts. Not because those institutions eliminated every dispute, but because without them uncertainty made it more difficult to cooperate, invest, govern, and project the future.

Today, a growing part of human existence takes place in the digital dimension. There we work, learn, love, trade, govern, deliberate, and preserve memory. The Internet amplified the human voice as never before, but left unresolved an elemental vulnerability: separating words from the person who issued them, altering them, and returning them to the world with the appearance of authenticity.

Artificial intelligence has made that deficiency more urgent, but it did not create it. The problem began when we acquired the ability to communicate globally without simultaneously building a universal capability to demonstrate who said what.

Words are not mere characters. They carry ideas, commitments, knowledge, and decisions. Through them, people participate in society and institutions coordinate collective life. Protecting their authenticity does not mean immunizing every statement from criticism; it means preserving the possibility of attributing it correctly.

If cooperation is one of the great powers of our species, and if that cooperation depends on communication and trust, then information authenticity belongs to the symbolic infrastructure that allows civilization to continue existing and thriving.

The question that remains is:

What institution will enable people and organizations to retain, in the digital economy, the right to their own words?

This essay argues that this institution is still missing.

And that the time has come to begin building it.

Notes and References

1. Yuval Noah Harari, “Cognitive Revolution — Power and Imagination,” the author’s official website; see also *Sapiens: A Brief History of Humankind*. The thesis is influential and useful as an interpretive framework, although it should not be treated as a unique or incontrovertible anthropological explanation.
2. Douglass C. North, “Economic Performance Through Time,” Nobel Lecture, 1993; the Nobel Prize presentation emphasized the role of institutions in reducing uncertainty and creating relatively stable structures for human activity.
3. Zygmunt Bauman, *Liquid Modernity*, Polity Press, 2000; and *Liquid Love: On the Frailty of Human Bonds*, Polity Press, 2003. The essay uses the metaphor as cultural context, not as a sufficient causal explanation of the authenticity problem.
4. Ludwig Wittgenstein, *Tractatus Logico-Philosophicus*, proposition 5.6; Hannah Arendt, *The Human Condition*, 1958; Jürgen Habermas, *The Theory of Communicative Action*, 1981. These references are not the axis of the essay, but they illustrate the philosophical depth of the relationship among language, public identity, and cooperation.
5. Douglas W. Diamond and Philip H. Dybvig developed the classic model of bank runs; together with Ben S. Bernanke, they received the 2022 Prize in Economic Sciences for their research on banks and financial crises. The analogy with “trust runs” is conceptual and is proposed here as a line of inquiry, not as a formal equivalence.
6. See Hannah Arendt, *The Human Condition*, and Jürgen Habermas, *Between Facts and Norms*, as well as the Stanford Encyclopedia of Philosophy entry on Habermas. These references provide theoretical context for the relationship between communication and democratic legitimacy.
7. Coalition for Content Provenance and Authenticity (C2PA), specifications and Content Credentials materials. The standard seeks to preserve verifiable information about origin and transformations, but does not seek to determine the truth of content.
8. National Institute of Standards and Technology, FIPS 203 (ML-KEM), FIPS 204 (ML-DSA), and FIPS 205 (SLH-DSA), published in 2024. ML-KEM is a key-encapsulation mechanism; ML-DSA and SLH-DSA are signature schemes. The appropriate strategy is not to fix one algorithm forever, but to design for cryptographic agility, coexistence during transition, and periodic renewal of evidence.

Selected Bibliography and Institutional Sources

- ARENDT, Hannah. *The Human Condition*. University of Chicago Press, 1958.
- BAUMAN, Zygmunt. *Liquid Modernity*. Polity Press, 2000.
- BAUMAN, Zygmunt. *Liquid Love: On the Frailty of Human Bonds*. Polity Press, 2003.
- COALITION FOR CONTENT PROVENANCE AND AUTHENTICITY (C2PA). C2PA Technical Specification, version 2.4, and explanatory materials on Content Credentials. <https://c2pa.org/> and <https://spec.c2pa.org/>
- DIAMOND, Douglas W.; DYBVIG, Philip H. "Bank Runs, Deposit Insurance, and Liquidity." *Journal of Political Economy*, 1983.
- HABERMAS, Jürgen. *The Theory of Communicative Action*. Beacon Press, 1984/1987.
- HABERMAS, Jürgen. *Between Facts and Norms*. MIT Press, 1996.
- HARARI, Yuval Noah. *Sapiens: A Brief History of Humankind*. Various editions.
- HARARI, Yuval Noah. "Cognitive Revolution — Power and Imagination." Author's official website. <https://www.ynharari.com/topic/power-and-imagination/>
- NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY. FIPS 203, Module-Lattice-Based Key-Encapsulation Mechanism Standard; FIPS 204, Module-Lattice-Based Digital Signature Standard; and FIPS 205, Stateless Hash-Based Digital Signature Standard. August 13, 2024. <https://csrc.nist.gov/projects/post-quantum-cryptography>
- NORTH, Douglass C. *Institutions, Institutional Change and Economic Performance*. Cambridge University Press, 1990.
- NORTH, Douglass C. "Economic Performance Through Time." Nobel Lecture, 1993. <https://www.nobelprize.org/prizes/economic-sciences/1993/north/lecture/>
- UNITED NATIONS. Our Common Agenda Policy Brief 8: Information Integrity on Digital Platforms. EOSG/2023/8, 2023.
- UNITED NATIONS DEVELOPMENT PROGRAMME. *Information Integrity: Forging a Pathway to Truth, Resilience and Trust*. Strategic Guidance, 2022.
- RODRÍGUEZ ALEMÁN, Luis Angel. "Computing in an Interdisciplinary World." In: *Reflections of the Mexican Academy of Informatics Forty Years After Its Founding*. University of Guadalajara, October 2016.
- UNESCO. *Guidelines for the Governance of Digital Platforms: Safeguarding Freedom of Expression and Access to Information through a Multistakeholder Approach*. Paris, 2023.
- WITTGENSTEIN, Ludwig. *Tractatus Logico-Philosophicus*. 1921/1922.
- WORLD ECONOMIC FORUM. *The Global Risks Report 2025*, 20th Edition; and *The Global Risks Report 2026*, 21st Edition. Geneva, 2025 and 2026.
- WORLD INTELLECTUAL PROPERTY ORGANIZATION. *Copyright and Related Rights and institutional copyright resources*. <https://www.wipo.int/copyright/>
- WORLD BANK GROUP. *Digital Public Infrastructure and Development*. Digital Public Infrastructure Policy Note Series, Washington, D.C., 2025; and resources on Digital Public Infrastructure and Services.

About the Author

Luis Ángel Rodríguez Alemán holds a degree in Computer Engineering from ITAM, a Master in Public Policy from Georgetown University, and a Master in Regional and Urban Planning from the London School of Economics. He has held senior technology-leadership responsibilities in banking, government, and education, and is a full member of the Mexican Academy of Informatics (AMIAC), the CIO Club, CISO Club, and CIOs LATAM. He is the founder of AliPsé, an initiative focused on building trust infrastructure for digital content.

Contact: luisangel@alipse.net · www.alipse.net

Notice: this document is a conceptual and public-policy essay. It does not constitute legal advice, a technical standard, or a claim that the proposed right is currently recognized in any particular jurisdiction.