2026, Cilt 3, Sayı 4, 662-669

OPEN ACCESS
ISSN: 3062-262X

Akademik Eğitim ve Sosyal Bilimler Dergisi (AJESS Journal)

Digital trust and Enhancing the citizen-state relationship in Algeria A Study of Law No. 26-02 on Trust Services for Electronic Transactions and Electronic Identification

Dr. Bouriah Selma, Boumerdes University , Algeria
s.bouriah@univ-boumerdes.dz, https://orcid.org/0009-0006-3084-3844

Article History
Received: 31/07/2026; Accepted : 11/09/2026; Published : 19/09/2026

Abstract:
This paper addresses digital trust in Algeria. It first defines trust and digital trust, then examines their connection to the relationship between citizen and state. Afterwards, it turns to Algeria's approach in this field, focusing on the legal framework through an analysis of Law No. 15-04 on electronic signature and electronic certification, and then Law No. 26-02, which sets out the general rules governing trust services for electronic transactions and electronic identification.
The study yielded that the establishment and consolidation of digital trust in Algeria depend on a clear and explicit legal framework able to strengthen citizens' trust in the state. In that respect, Law No. 26-02 is significant because it brings together technical, legal, institutional, and judicial dimensions within a single framework. That broader structure supports digital transformation and helps root digital trust in the sphere of transactions and contracts.

Keywords: trust. digital trust. Algeria. digital environment. Citizen-State Relationship. Law No 26-02.

Introduction

In a world that is becoming increasingly interconnected and digitized, trust has emerged as a basic and multi-layered concept. It includes perceptions of reliability, credibility, and integrity in the interactions between government bodies and the citizens they serve. Trust reflects the belief that public authorities will act in the public interest, meet their obligations, and protect citizens' rights. In the digital age, trust goes beyond its traditional meaning in the relationship between individuals and government. It also extends to confidence in technical systems, data processing, and information security. From this broader field comes a more specific dimension, digital trust, which concerns citizens' confidence in public services delivered through the safe and ethical use of digital technologies by government institutions and by the private actors connected to them.

In our country, with digital transformation advancing and with increasing reliance on electronic service delivery and electronic transactions, digital trust has become a very important issue. It is necessary for building citizens' confidence in the digital environment, ensuring the exchange of information, enabling the use of electronic services and electronic transactions, and allowing contracts to be concluded without doubt or fear. This requires the establishment of a strong infrastructure and a clear, explicit legal framework capable of supporting successful digital transformation and safe, reliable use. On that basis, the following problematic may be raised:

How does Law No. 26-02, laying down the general rules relating to trust services for electronic transactions and electronic identification, contribute to establishing and strengthening digital trust in Algeria?

Based on the research problem, the following hypothesis is proposed:

The clarity of the legal and regulatory framework governing trust services in the field of electronic transactions, electronic identification, and digital identity determination in Algeria contributes to strengthening citizens' trust in electronic transactions and electronic contracts, in a way that guarantees their right to the protection of their information and data, as well as the reliability and integrity of the service.In order to address the problem and hypothesis of this study, we used the analytical method to examine the concepts of trust and digital trust, as well as the role of digital trust in strengthening the relationship between the citizen and the state. We also adopted the legal approach in order to study and analyze the legal and regulatory frameworks relating to trust services in Algeria.

Accordingly, the study is divided into two sections:

- **Section One**: Digital trust: the concept and the problematic relationship between the citizen and the state.
- **Section Two:** Enhancing Digital Trust in Algeria in light of Law No. 26-02 on Trust Services for Electronic Transactions and Electronic Identification.

Section I: Digital Trust: The Concept and the Problematic of the Relationship Between Citizen and State

The transition from traditional methods of work to electronic modes requires individuals to be convinced of the usefulness of electronic services, and that such services will provide them with added value and opportunities not afforded by traditional methods of work. It also requires them to be convinced that electronic modes of work do not pose a threat to their information, data, or property (United Nations 2003). Trust is among the key elements required for a secure digital space, both in terms of the use of digital services and in ensuring information security in identity verification, commercial transactions (buying and selling), and electronic deliberations. This, in turn, requires building trust through the provision of data protection in its various forms, as well as network protection. (United Nations 2003)

Interest in building trust in the digital space can be traced back to the principles and plan of action of the World Summit on the Information Society, which emphasized the need to build the trust of individuals and business actors in the digital environment(United Nations 2003), on the basis that building trust in the use of information and communication technologies and ensuring their security constitutes a central section within ICT strategy. This is necessary in order to preserve citizens' privacy, establish legislation for data protection, and strengthen international cooperation in combating crime in cyberspace. (United Nations 2003)

A. Trust

The word **"trust"** is used very widely in human interaction and across different scientific fields. Its meaning changes with the discipline, the context, and the point of view from which it is approached. Still, regardless of the field, most definitions of trust revolve around positive and negative expectations. (Söllner and al 2010)

From a terminological standpoint, trust is described by Mayer, Davis, and Scho Pankaj orman as the readiness of one party to place itself in a position of vulnerability to another, on the assumption that the latter will perform an action significant to the former, regardless of whether such conduct can be supervised or controlled. This understanding refers to a relationship involving an identifiable other party, one regarded as acting freely in relation to the trustor. (Mayer and al 1995)

The Organization for Economic Co-operation and Development approaches trust differently. For it, trust is the belief that another person or an institution will act in a way that matches expectations of positive behavior. Trust, in that sense, implies a positive assessment of the conduct of an individual or an organization. It is subjective in nature and is rooted in the "receiver's perspective," which gives it practical importance because it helps shape behavior. Trust in government illustrates this clearly. It concerns citizens' confidence in the government's capacity to do what is right and fair, and that confidence is tied to the degree of correspondence between citizens' preferences, their understanding of fairness and injustice, and the government's actual conduct as they perceive it. Since citizens' preferences vary, they use multiple criteria to evaluate government performance. What one person regards as right and fair may not be seen likewise by another. This is central to analyzing the factors affecting trust in government. (OCED 2013)

It may therefore be said that trust brings together two persons: one who initiates trust, and the other who is the object of trust, that is, the trusted party, within the context of human, social, legal, and economic relations.

Mayer further argues that, despite the considerable attention paid by researchers to the concept of trust, its study in organizations remains problematic for several reasons: difficulties in defining trust itself; the lack of clarity in the relationship between risk and trust; confusion between trust and its antecedents and consequences; the failure to specify the referents of trust, which leads to ambiguity in levels of analysis; and the failure to take into account both the trusting party and the party receiving that trust. (Mayer and al 1995)

B. Digital Trust

Digital transformation has brought about cultural, organizational, and relational changes that may affect the individual, the organization, or society, with the aim of improving public value and service delivery. Among the factors contributing to digital transformation is the building of public trust. (Virnandes and al 2024) Trust is also a fundamental element in the continued use of electronic services and electronic transactions, since citizens need confidence in security, integrity, and reliability.(Jarbi and mokbul 2025) Digital trust is a specialized dimension of trust relating to citizens' confidence in public services delivered through government institutions, as well as in the safe and ethical use of digital technologies by private sector actors. (Pankaj 2023)

Mayer's trust theory seeks to clarify the psychological mechanisms that shape technology adoption, whether by encouraging it or holding it back. One of its central points is that perceived risk has a negative effect on the intention to adopt technology. For first-time users of digital systems, privacy concerns and questions of ease of use carry particular weight. Yet these same concerns can work in the opposite direction and become drivers of adoption once users feel reassured. Trust, then, is tied not only to perception but also to system features, especially the transparency and permanence of transaction records, the consistency of consensus mechanisms, and confidence in the system's ability to limit fraud and manipulation. (Pardos-Castilo and al 2025)

A similar logic applies at the legal and regulatory level. Rules that strengthen trust are needed if privacy and security concerns are to be addressed, since those concerns directly affect market confidence. Public authorities and regulatory bodies must therefore develop clear guidelines and legal frameworks, especially in sectors such as financial services, supply chain management, and digital identity verification. Still, regulation is effective only if it does not interfere with

the essential functions of the technology. Where that condition is respected, it may help speed up adoption rather than slow it down. (Pardos-Castilo and al 2025)

C. Foundations of Digital Trust

According to the OECD report, digital trust includes the availability of a set of core elements, as follows:

- **Data security:** Citizens need to feel confident that their personal and sensitive data are properly safeguarded against breaches, misuse, and any form of unauthorized access.
- **Service reliability:** Trust also depends on the consistent availability of digital services. These services must remain accessible, responsive, and dependable whenever citizens need them, without disruption or unexpected downtime.
- **Privacy assurance:** Another key element is the assurance that privacy rights are respected and that data collected for public service purposes are handled responsibly and within legitimate limits. (Pankaj 2023)
- **Transparency:** Trust grows when public service delivery processes and the technological systems that support them are transparent. Citizens expect clear information about how services are provided and how their data are collected, processed, and used.
- **Accountability:** Governmental bodies strengthen trust when they assume responsibility for their actions and respond promptly to mistakes or problems as soon as they arise. (Pankaj Pankaj 2023)

Based on the foregoing, public trust in digital public services increases as positive expected beliefs increase regarding factors such as accountability, credibility, reputation, reliability, usefulness, ease of use, security, and privacy.

Accountability refers to the obligation of governmental bodies responsible for specific services, com pliance, security, data governance, privacy, and related functions to answer for their conduct, whether its effects are favorable or adverse.

Credibility operates at the level of the product or service itself. It concerns the degree of confidence placed in the devices, software, particular service delivered, or technical frameworks such as zero-trust architecture.

Reputation, by contrast, is formed at the institutional or brand level. It relates to the standing and perceived value of the institution that provides the digital infrastructure through which particular public services are delivered. (ESCWA 2023)

Reliability rests on continuity and operational consistency. It also depends on availability, predictability, and timely responsiveness, without interruptions or service stoppages.

Usefulness concerns the extent to which the public believes that a digital service will actually produce efficiency and transparency, while also helping reduce corruption, error, and delay.

Under European Union standards, **ease of use** refers to the extent to which people are convinced that digital public services are accessible and simple to use across differences in age, educational background, language, and levels of digital literacy. It also includes compliance with accessibility requirements.

Security relates to protecting services against unforeseen cyber incidents and to safeguarding personal and sensitive data from breaches or unauthorized access. (Pankaj 2023)

Privacy relates to the public's belief that collected data will be used responsibly, and not for irresponsible or unethical purposes such as profiling.

Intentions refer to the perceived malicious intentions of a private supplier, especially a foreign supplier, as well as the malicious intentions of governmental entities, such as espionage and political surveillance, underlying a particular digital public service .(ESCWA 2023)

Nevertheless, public trust in digital public services declines as negative expected beliefs about those services increase.

D. The Importance of Digital Trust in Government-Citizen Relations

At the level of government-citizen relations, trust is indispensable. This is particularly true in the area of digital public services, where trust should not be viewed as an optional advantage, but as a necessary foundation. The adoption of digital technologies in the public sector, and their effective use over time, depend heavily on it. Trust influences patterns of interaction with public services, readiness to exchange information, and broader perceptions of how effectively government performs. Citizens are more likely to engage and respond to digital public services when they trust that their interactions will be secure and reliable, that their privacy will be respected, and that their information and data will be handled responsibly and used solely for their intended purpose. (OCED 2025)

By contrast, a low level of citizen trust may lead to suspicion toward government and its effectiveness, reduced participation, and reluctance to use digital services.

1. Citizens' Trust in Government and Digital Public Services

In the context of the provision of digital public services and the conduct of electronic transactions, citizens' trust in government revolves around three central points:(ESCWA 2023)

First, transparency: trust is strengthened when governmental procedures and decision-making processes are made more transparent. Citizens expect clear and accessible communication explaining how digital services operate, how their data are handled, and on what basis decisions are reached.

Second, accountability: public authorities are expected to answer for their actions. When mistakes occur, or when data breaches take place, trust is more likely to endure if institutions respond quickly and openly, showing that they are prepared to address the problem and reduce the likelihood of its recurrence.

Third, ethical conduct: citizens also expect technology to be used in ethically responsible ways. This includes avoiding discriminatory algorithms, safeguarding individual rights, and ensuring that emerging technologies remain consistent with broader societal values. (ESCWA 2023)

2. Trust in Technology

In the digital era, trust is no longer directed only toward government institutions themselves. It also concerns the technologies on which digital public services depend. Citizens need assurance that the underlying digital infrastructure is secure, dependable, and ethically governed. Security measures are central here, because confidence in technology depends in part on the belief that personal data are protected against unauthorized access, cyberattacks, and security breaches. Reliability matters just as much. Service interruptions, system breakdowns, and technical failures tend to weaken trust, sometimes quite quickly. (ESCWA 2023) For that reason, maintaining strong service performance and continuous availability remains essential. Ethical concerns are equally important, since citizens expect technologies to be used in ways that protect their rights, including privacy, and that do not reproduce bias or discrimination.

3. Trust-Building Strategies

Building and maintaining trust in digital public services requires proactive strategies and measures. In Europe, the Council of Europe, in Resolution 68/01 C/2007 issued on 22 March 2007 concerning the development of a strategy for a secure information society in Europe, emphasized the importance of trust as a fundamental element in the successful construction of an information society, as well as its connection to end-user experiences and the importance of respecting privacy. Since 2005, the International Telecommunication Union has also made major efforts in the field of building trust in cyberspace through the preparation of reports and the organization of periodic expert meetings and workshops devoted to cyber security. (Pankaj 2023)

Similarly, the Economic and Social Commission for Western Asia recommended the formulation of a national strategy for building trust in electronic services and enhancing their security at both the national and institutional levels, in order to determine the state's general plans and orientations in this area and encourage various stakeholders to take measures aimed at winning citizens' trust in electronic services.(OCED 2025) Trust here is linked to the user's confidence in the application used, the website, and the institution providing the service, as well as to trust in technology as a tool for storing, processing, transmitting, and handling information. ESCWA also encouraged strengthening international cooperation in order to activate collaboration in the field of building trust in electronic services and exchanging solutions and expertise in this area. (ESCWA 2023)

Trust-building strategies should also include the following:

- **Transparency and communication:** Public authorities need to explain clearly how digital services operate, how data are processed, and what measures are in place to protect citizens' information. Clear and open communication plays a direct role in strengthening trust.
- **Data protection:** Strong safeguards for personal data, including encryption and access-control mechanisms, signal a serious commitment to protecting citizens' information.
- **Ethical considerations:** When adopting emerging technologies, governmental bodies should place ethical concerns at the forefront. Ethical frameworks and impact assessments can support a more responsible use of technology. (Panjak 2023)
- **Accountability:** Trust is more likely to be maintained when effective accountability mechanisms are in place, such as incident-response plans and supervisory bodies capable of dealing with problems without delay. (OCED 2025)

Section Two: Enhancing Digital Trust in Algeria under Law No. 26-02 on Trust Services for Electronic Transactions and Electronic Identification

An analysis of the policies followed by Algeria in the field of digital transformation, and in strengthening the legal and regulatory frameworks governing cyber legislation, shows that Algeria issued its first legal text dealing with digital trust in 2015 through Law No. 15-04 laying down the general rules relating to electronic signature and electronic certification. Eleven years after the issuance of that law, Algeria enacted a new legal text in 2026, namely Law No. 26-02 laying down the general rules relating to trust services for electronic transactions and electronic identification.

A. A study of Law No. 15-04 on the general rules on electronic signature and electronic certification

In 2015, Algeria enacted Law No. 15-04 laying down the general rules relating to electronic signature and electronic certification. This law set out the rules governing electronic certification, the mechanisms for its creation, and the means of verifying it. It also defined electronic certification, the electronic certification certificate, and its requirements. The law further provided for the establishment of the National Electronic Certification Authority as an administrative authority attached to the Prime Minister, whose task is to promote and develop the use of electronic signature and electronic certification and to ensure the reliability of their use. (Law15-04 2015) It also provided for the creation of the Governmental Electronic Certification Authority as an authority attached to the Minister of Post and Information and Communication Technologies, responsible for monitoring and supervising the electronic certification activity of trusted third parties, as well as for providing electronic certification services for actors in the governmental branch. (Law15-04 2015) The law also provided for the establishment of an Economic Electronic Certification Authority, (Law15-04 2015) whose role is to monitor and supervise providers of electronic certification services offering electronic signature and certification services to the public.

The law also laid down the legal regime governing the provision of electronic certification services, including the service providers themselves, the procedures for granting qualification certificates and authorizations, the delivery of electronic certification services, oversight and auditing, the obligations and liability of electronic certification service providers, and the possible sanctions in the event that such providers act in breach of the electronic certification policy.

This law may be considered the second legal text in the sequence of legislative texts supporting the course of digital transformation in Algeria, after Law No. 09-04 containing the specific rules for the prevention of offences related to information and communication technologies and the fight against them. (Law09-04 2009), It was followed by a series

of other texts, such as Law No. 18-04 laying down the general rules relating to postal services and electronic communications, which provided that postal and electronic communications activities are subject to State control, (Law18-04 2018) then Law No. 18-05 on electronic commerce in 2018, (Law18-05 2018) and Law No. 18-07 on the protection of personal data. (Law18-07 2018)

Yet the actual implementation of Law No. 15-04 did not begin until 2020, that is, a full five years after its enactment. The Governmental Electronic Certification Authority only effectively began operating in 2020 as part of a strategy to build trust in electronic transactions through the generalization of electronic signature services and the issuance of certificates among actors in the governmental sector. It also contributed to securing internet communications, managing verified digital identities, automating authentication and encryption processes, and monitoring and controlling electronic certification activity.(The Governmental Electronic Certification Authority 2026) The same applies to the Economic Electronic Certification Authority, which only began operating effectively in 2020, when it created an electronic portal dedicated to public and private economic operators, (The Governmental Economic Certification Authority 2026) in order to enable them to register their organizations, request certificates, and make online payments.

The delay in implementing the provisions of Law No. 15-04, including the operation of the institutions falling within its scope, namely the National Electronic Certification Authority, the Governmental Electronic Certification Authority, and the Economic Electronic Certification Authority, may be attributed to its connection with a set of laws enacted after it, as well as to Algeria's lag in implementing the system of electronic transactions, electronic payment methods, and electronic commerce.

B. Law No. 26-02 and the entrenchment of digital trust in Algeria

The enactment of Law No. 26-02 laying down the general rules relating to trust services for electronic transactions and electronic identification constitutes a general, comprehensive, and integrated regulation of digital trust. It marks a shift from partial and fragmented regulation in previous texts to a total and comprehensive framework that keeps pace with the accelerated developments in the digital environment and in electronic transactions.

In Article 2, Law No. 26-02 laying down the general rules relating to trust services for electronic transactions and electronic identification defined thirty-three terms related to the content of the law, including: electronic signature certificate, electronic signature, signatory, electronic seal certificate, electronic seal, creator of the electronic seal, data for the creation of the electronic signature or electronic seal, mechanism for creating the electronic signature or electronic seal, data for verifying the validity of the electronic signature or electronic seal, validation, electronic time stamp, registered electronic delivery service, website authentication certificate, trust service, qualified trust service, authorization, actors in the governmental sphere, trusted third party, trust service provider, authority, trust list, user party, holder of the electronic signature or seal certificate, electronic certification policy, audit, electronic identification, attribute, identity, electronic identification means, proof of identity, electronic identification system, electronic document, and electronic transaction.(Law26-02 2026)

Defining these concepts helps regulate the stages of creation, authentication, verification, and proof in the digital environment.

The law also determined everything relating to trust services, beginning with their definition in Article 2 as "an electronic service ensuring certain attributes of the electronic document and including, in particular, methods for the creation and management of electronic signatures, electronic seals, electronic time stamps, website authentication, electronic preservation, website authentication, electronic preservation, and registered electronic delivery services".(Law26-02 2026)

In Article 4, the legislature also laid down a set of conditions that a reliable electronic signature and a reliable electronic seal must meet. These conditions ensure identification of the signatory or the creator of the seal, and also ensure the protection of data against any modifications that may affect them, in a manner that sustains the confidence of the signatory or the creator of the seal. In addition, the electronic signature and the electronic seal must be created on the basis of an electronic certificate and an approved electronic signature or seal creation mechanism.

The same Article 4 also provided for the contents of qualified electronic signature and electronic seal certificates. These certificates must include an indication of automated processing, the full set of data necessary for trust services, the name of the signatory, or the pseudonym, the data for the validity of the electronic signature or seal, the beginning and end of the certificate's period of validity, and the electronic link through which the certificate may be obtained. (Law26-02 2026) Law No. 26-02 also provides in Article 7 that a qualified electronic signature is equivalent to an electronic signature. Article 9 states that conformity of the mechanism for creating the electronic signature or electronic seal shall be established by the national body responsible for information systems security. Article 10 of Law No. 26-02 further sets out the requirements applicable to approved electronic signature and electronic seal creation mechanisms, one of the most important being the guarantee of confidentiality of the data used to create the electronic signature, while ensuring that those data are protected against any forgery that may affect them. (Law26-02 2026)

One of the most important provisions of this law is contained in Article 16, which states that an electronic signature or electronic seal may not be deprived of its legal effectiveness, nor may it be rejected before the courts on the ground that it was issued in electronic form or that it does not satisfy the requirements of this law. The law also sets out in Article 20 the conditions that must be satisfied by qualified website authentication certificate. (Law26-02 2026)

Law No. 26-02 also permits trust services provided by a trust service provider established in a foreign country to be treated in the same manner as trust services provided by a trust service provider resident in Algeria, provided that the foreign provider acts within the framework of a concluded mutual recognition agreement. (Law26-02 2026) This opens the way to the international dimension of digital trust.

The law further specifies that its provisions apply to natural and legal persons who use electronic transactions and/or trust services, as well as to electronic transactions, trust services, and the procedures necessary for their implementation. It defines actors in the governmental sphere as public institutions and administrations determined by the applicable legislation, independent national institutions, regulatory authorities, and every legal person or body of a non-industrial, non-economic, or non-commercial nature. (Law26-02 2026)

As for trust service providers, trusted third parties and providers of trust services are both regarded as trust service providers. The law also determines the conditions that must be satisfied by applicants seeking authorization to provide trust services.

On the institutional side, Law No. 26-02 provides for the creation of a National Electronic Certification Authority. This is a public institution of a special nature entrusted with supervising, monitoring, promoting, developing, and regulating activities relating to trust services. Its functions include:

- preparing its policies relating to electronic certification and ensuring their implementation after approval in accordance with the legislation and regulations in force;
- determining the requirements necessary for trust services;
- approving the electronic certification policies prepared by trust service providers;
- preparing the specifications laying down the conditions and modalities for providing trust services;
- supplying trust services and qualified trust services;
- monitoring and supervising trust service providers in accordance with the requirements and modalities for providing trust services;
- carrying out audits, either through approved audit service providers or through its own means, of actors in the governmental sphere wishing to act as trusted third parties and of applicants for authorizations wishing to become trust service providers;
- in addition, carrying out periodic audits, issuing authorizations to trust service providers, preparing, updating, and publishing the trust list, contributing to the preparation and updating of national audit references in the field of trust service provision, and taking the measures necessary to ensure continuity of services and protect the interests of subscribers when a trust service provider is no longer able to provide its services or when authorization is withdrawn;
- promoting research and development activity in the field of trust services, promoting the use and development of trust services, and ensuring the reliability of their use. The Authority is also consulted when any legislative or regulatory draft text relating to its field of competence is prepared.

The creation of a single authority specialized in trust services, after there had been three authorities under Law No. 15-04, indicates a unification of competence and a coordination of efforts in the field of trust services, as well as rationalization of expenditure, which suggests governance and soundness in public management.

With regard to the electronic document, Law No. 26-02 provides that where the law requires information to be in writing, this condition is deemed fulfilled in the case of an electronic document if the information it contains is preserved in a manner that permits its use and retrieval. It also provides that where the law requires the existence of a signature or seal on a document, this condition is fulfilled in the case of an electronic document in certain situations, including the use of an identification means to establish the identity of the signatory or the creator of the seal, and provided that this means is reliable and sufficient in light of the purpose for which the document was created or sent. The law also considers a contract to be valid, proven, and enforceable where it has been concluded by means of an electronic document.

As for preservation, original form, and the evidentiary force of electronic documents, an electronically signed document must be preserved using technology that makes it possible to extend its reliability throughout its period of usefulness. A legal document or electronic transaction may not be rejected before the courts merely because it was issued in electronic form.

In the field of attribution and electronic identification, the law determines the cases in which an electronic document may be considered to have been issued by the sender, as well as the cases in which the addressee may regard the document as having been sent by the sender, together with all the situations that may be associated with this. As regards electronic identification, it determines the cases of its use in order to provide the necessary guarantees concerning the relationship between a natural person, a legal person, or the legal representative of a legal person and the identity. (Law26-02 2026) The national body responsible for information systems security, in consultation with the parties concerned, determines the standards and conditions that the assurance levels of the electronic identification system must satisfy.

In the field of audit, supervision, and sanctions, Law No. 26-02 entrusts the national body responsible for information systems security with determining, in consultation with the Authority, the modalities for accrediting providers of audit services in the field of trust service provision. In cases of transgressions and non-compliance with the rules relating to information systems security and the protection of personal data, the two bodies responsible for those matters shall be notified. The law also establishes financial and administrative sanctions against persons who violate the conditions applicable to trust service providers under the specifications and the decisions of the Authority. (Law26-02 2026)

C. Prospects for improving trust mechanisms in the digital environment in Algeria in light of Law No. 26-02

Law No. 26-02 came as an integrated framework for digital trust in Algeria because it regulates the concepts connected to all aspects of digital trust, matters that had been addressed only partially and inadequately in earlier legal and regulatory texts, especially Law No. 15-04. It sets out the conditions governing trust services, regulates signature, seal, and registered delivery, frames the activity of trust service providers, and then recognizes the evidentiary value of

the electronic document and regulates attribution and electronic identification, the authority competent for supervision, the consequences of violating the law, and the forms of proof before the courts. This makes it a unified national framework that expands the scope of trust services and confirms legal recognition of electronic documents, electronic contracts, and electronic transactions.

Law No. 26-02 also brings together the technical dimension, through its definition of many technical terms and its specification of the procedures to which they are subject; the legal dimension, through its clarification of all legal procedures arising from trust services, from the beginning of the service to its end and the effects resulting from it; and the institutional dimension, through its identification of the bodies vested with supervisory and monitoring powers, namely the National Electronic Certification Authority and the National Agency for Information Systems Security, the latter being the body responsible for formulating and implementing the national strategy in the field of information systems security. (Presidential Decree 20-05 2020) This is consistent with ensuring national cyber resilience in order to support digital transformation in Algeria and preserve digital sovereignty. For that reason, it may be regarded as an integrated text laying the foundation for digital trust in Algeria, since it turned matters that had remained subject to interpretation, hesitation, or debate into explicit and enforceable rules. This strengthens legal certainty in the digital environment and supports digital transformation in Algeria in the fields of administrative, commercial, and judicial transactions. It also enhances the credibility and reliability of Algerian companies and individuals in global markets, since they will be able to participate more effectively in international trade and e-commerce, while also strengthening the country's international reputation as a safe and reliable destination for online transactions.

The law provides that the National Electronic Certification Authority, the Governmental Electronic Certification Authority, and the Economic Electronic Certification Authority shall continue to exercise their functions under Law No. 15-04 until the effective installation of the new authority. It also provides for the repeal of the provisions of Law No. 15-04, while stipulating that its texts shall remain in force until the implementing texts of this law are issued. On that basis, the effectiveness of the law remains tied to the speed with which the regulatory texts are issued, the degree of legal coordination in the fields of information systems security and personal data protection, and institutional coordination in transferring the material and human resources of the three authorities established under Law No. 15-04 to the National Electronic Certification Authority within the framework of Law No. 26-02. It also depends on training judges, public administration employees, and economic operators in the use of its new concepts, so that it may contribute to establishing and consolidating digital trust in Algeria in step with digital transformation and within the national strategy for digital transformation and information systems security.

Conclusion

Building a national framework for trust in the information society, while also strengthening its security, is necessary for creating a reliable and secure digital environment that encourages the use and development of electronic applications and services across administrative, governmental, practical, commercial, cultural, and educational activities.

Trust remains a cornerstone of effective relations between government and citizens. For that reason, the responsible adoption of these technologies, attention to security, and sensitivity to ethical considerations all remain necessary. As governments adapt to an evolving digital environment, trust, security, responsible use, and ethical judgment should guide decision-making at each stage. When these principles are treated as priorities, public authorities are better placed to build and sustain the confidence of citizens and other stakeholders, while also ensuring that emerging technologies are used to improve the quality, accessibility, and responsiveness of public services. In this way, they do not simply shape a better future for digital public services. They also reinforce a stronger relationship of trust between government and the people it serves.

With regard to Law No. 26-02, it may be observed that it has established the main elements of trust in electronic exchanges and transactions through verification of the identity of the parties, protection of data integrity and confidentiality, recognition of the evidentiary value of transactions and contracts, their non-repudiation, and the safeguarding of data confidentiality. Yet proof of its effectiveness and practical efficiency remains contingent on the completion of the regulatory texts associated with it, as well as on institutional coordination among State bodies. In That context, the following recommandations may be advanced :

- The regulatory texts required for the implementation of Law No. 26-02 should be issued as soon as possible in order to strengthen digital trust in Algeria and keep pace with rapid digital transformation.
- Institutional coordination between ministerial sectors and the governmental institutions concerned with the law's provisions is necessary to ensure effective and practical implementation of its content.
- The necessary human resources, particularly judges and government employees, should receive appropriate training in order to ensure the proper application of the law's provisions.
- Cooperation between universities, research centers, and State institutions should be strengthened through the opening of specialized academic workshops on the fields covered by Law No. 26-02, with a view to advancing research and keeping pace with developments relating to electronic transactions.
- Citizens should be made aware of the content of the law and of the ways in which it is applied, in order to strengthen their trust in electronic services and transactions.

References

Aksoy, C. 2023. Digital Business Ecosystems: An Environment of Collaboration, Innovation, And Value Creation in The Digital Age. *Journal of Business and Trade (JOINBAT)* 4(2):156-180. https://doi.org/10.58767/joinbat.1358560.

ESCWA. 2009. Building trust in e-services in the ESCWA region, *Economic and Social Commission for Western Asia.*

ESCWA. 2023. *Workshop on Building Trust in Digital Government Services*, Beirut, 11-12 September.
Jabri, A., and M. A. Mokbul. 2025. E-Service quality and public trust: A foundation for effective digital service delivery in Northern Tunisian municipalities, *Social Sciences & Humanities Open*, 12. https://doi.org/10.1016/j.ssaho.2025.102308.
Mayer, R,. C, Davis, J. H, & Schoorman, F. D,1995. An integrative model of organizational trust, *The Academy of Management Review*, 20(3): 709-734 https://www.jstor.org/stable/258792.
National Agency for Information Systems Security .2025. *National Strategy for Information Systems Security 2025-2029*.
Law09-04. 2009. *Special Rules for the Prevention and Combat of Crimes Related to Information and Communication Technology*, Issue 47.
Law15-04. 2015. *General Rules Relating to Electronic Signature and Certification*, Official Gazette, Issue 06.
Law18-04. 2018. *General Rules Relating to Postal and Electronic Communications*, Official Gazette, Issue 27.
Law18-05. 2018. *Relating to Electronic Commerce*, Official Gazette, Issue 28.
Law18-07. 2018. *Relating to the Protection of Natural Persons with Regard to the Processing of Personal Data*, Official Gazette, Issue 34.
Presidential Decree 20-05. 2020. *relating to the establishment of a national information security system*, Official Gazette, Issue 04.
Law26-02. 2026. Trust Services for Electronic Transactions and Electronic Identification, Official Gazette, Issue 14.
OECD. 2013. Government at a Glance 2013, *OECD Publishing*, Paris.
OECD. 2025. Government at a Glance 2025, *OECD Publishing*, Paris.
Prados-Castillo, J, F., J, M, Martín., I, Alexeeva-Alexeev., J, M, Guaita-Martínez. 2025. Understanding blockchain by digital natives: innovation, trust and psychological factors, *Journal of Innovation & Knowledge*, 10. https://doi.org/10.1016/j.jik.2025.100806.
Pankaj, P. 2023. Navigating the Future: Building Trust in Digital Government Services Through Emerging Technologie, *United Nations, ESCWA*.
Söllner, M., Hoffmann, A., Hirdes, M., Rudakova, L., Leimeister, S., Leimeister, J, M. 2010. Towards a Formative Measurement Model for Trust. *BLED 2010 Proceedings* 23: 65-79.
United Nations. 2003. *World Summit on the Information Society*, Plan of Action,(Document WSIS-03/GENEVA/DOC/5), Geneva.
Virnandes, R ,S,. Shen,J., Vlahu-Gjorgievska, E. 2024. Building public trust through digital government transformation: A qualitative study of Indonesian civil service agency. *Procedia Computer Science,* 234: 1183-1191.
*The Governmental Electronic Certification Authority***,** Viewed: on 25 Mars2026 at 11:20 P.M. https://www.agce.dz/ar/evenement/lagce-et-lance-obtiennent-la-certification-webtrust/
*The Governmental Economic Certification Authority***,** Viewed: on 30 Mars2026 at 9:00 P.M. https://aece.dz/ar/services/#validation