Registered in Germany Europa Revue Journal
ISSN: 1862-6564 Vol. 6 No. 4 (2026) Published April 30, 2026

GOVERNING THE DIGITAL NOTARY: COOPERATION BETWEEN THE STATE AND NOTARIAL SELF-GOVERNMENT IN IDENTITY, DATA AND CYBERSECURITY

Munavvarova Naimakhon Zokhidulaevna
Independent Researcher, University of World Economy and Diplomacy
ORCID: 0009-0001-2789-9509
e-mail: naimaxonmunavvarova@gmail.com

Abstract

Digital notarisation changes not only the form of a notarial act but also the institutional allocation of responsibility. This article analyses how a competent state body and a professional self-governing notarial organisation should cooperate in governing remote acts, electronic archives, registers, identity assurance and cybersecurity. Uzbekistan's recent introduction of videoconference-based notarial acts and broader digital-government reforms are compared with chamber-operated infrastructures in Germany and Spain and remote authentication in Estonia. The study proposes a shared-governance architecture in which the State sets binding legal and security baselines and supervises legality, while the Notarial Chamber operates or co-governs professional infrastructure, validates workflows, trains notaries, monitors practice and coordinates first-line incident response. The article moves beyond a descriptive comparison and proposes an operational allocation of powers, information flows and safeguards that can be translated into legislation and joint administrative procedures.

Keywords

digital notariat; remote notarisation; electronic authentic instrument; digital identity; cybersecurity; electronic archive; Notarial Chamber; Ministry of Justice; Uzbekistan; comparative law

Introduction

The digital transformation of the notariat is often described as a technical modernisation. In legal terms, however, it is an institutional redesign. When identity verification, document preparation, consent, signature, registration and archival

preservation occur through connected systems, legal reliability depends on the allocation of responsibilities among the State, the professional chamber, the individual notary and technology providers.

Uzbekistan has moved from digitising records toward remote performance of selected notarial acts. Presidential Resolution No. PP-280 of 9 September 2025 required further development of the institution and the preparation of updated administrative regulations, including rules for notarial acts by videoconference [2]. In January 2026, the Ministry of Justice approved a regulation governing notarial acts through videoconference, expressly coordinated with the Notarial Chamber [3]. These reforms create a timely question: who should design, operate, audit and improve the digital environment in which public authenticity is produced?

The problem is common across jurisdictions. Germany entrusts the Federal Chamber of Notaries with statutory digital infrastructures, including electronic archives, special electronic mailboxes and a video communication system [6]. Spain's General Council of Notaries has developed a nationwide electronic notarial network connecting notaries with public authorities [8]. Estonia combines state legal supervision with a Chamber-supported e-notary environment and remote authentication [9; 10]. These models show that professional self-government can be more than a consulted stakeholder: it can be an infrastructure institution, provided public accountability and security duties are clear.

This article aims to develop a cooperative governance model for digital notarial services applicable to Uzbekistan and other civil-law jurisdictions. It focuses on digital identity, system design, data governance, cybersecurity, continuity and the use of automated or artificial-intelligence tools.

Materials and Methods

The research analyses Uzbekistan's Law on Notariat, Resolution No. PP-280, the 2026 videoconference regulation, legislation on personal data and electronic government, and the Digital Uzbekistan 2030 framework [1-5]. Comparative materials include Germany's Federal Notaries Act, EU rules on electronic identification and data

protection, official Spanish notarial materials, Estonia's Notaries Act and Chamber information, and UINL principles on digital notarial activity [6-12].

A legal-doctrinal method identifies duties relating to authenticity, secrecy, data protection and supervision. A socio-technical method treats the digital notarial act as a chain of legal and technical controls rather than a single video call. Comparative functional analysis examines which institution sets rules, operates infrastructure, authenticates users, retains records, responds to incidents and audits compliance. Scenario analysis tests the proposed model against realistic failures.

Results and Analysis

A qualified electronic signature does not by itself reproduce the legal function of a notary. Authenticity also depends on the notary's assessment of identity, capacity, authority, informed consent, voluntariness and legality. Remote performance adds risks of impersonation, coercion outside the camera frame, synthetic media, compromised devices and jurisdictional uncertainty. Accordingly, digital notarisation must preserve the functional safeguards of the physical act while using different technical evidence.

A robust workflow has at least seven layers: verified entry to the platform; authoritative identity data; liveness and document checks; secure audiovisual communication; the notary's substantive legal assessment; qualified signing and time-stamping; and tamper-evident registration and preservation. Each layer may be controlled by a different institution or vendor. Without a governance map, a failure can fall between contracts and public-law mandates.

The Notarial Chamber has a unique role because it can translate professional duties into system requirements. For example, a software designer may view a completed identity match as sufficient. A practising notary knows that identity certainty does not resolve capacity or coercion. The Chamber should therefore validate the legal workflow and interface prompts, while the competent state body sets binding minimum standards and supervises legality.

The 2025-2026 reforms in Uzbekistan provide a positive basis for joint work. Resolution No. PP-280 identifies both the Ministry of Justice and the Notarial Chamber among the bodies responsible for updated notarial regulations [2]. The 2026

videoconference regulation was agreed with the Chamber [3]. This demonstrates institutional recognition that remote notarisation cannot be governed by the Ministry or the profession acting alone.

Nevertheless, regulation of a procedure does not automatically settle ownership of operational risk. The legal framework should expressly allocate responsibility for platform operation, cybersecurity monitoring, identity-service integration, retention of audiovisual or technical evidence, access logging, incident notification, backup, disaster recovery, vendor management and periodic penetration testing. It should also explain which failures invalidate an act, which merely trigger remediation, and which require suspension of the remote channel.

Uzbekistan's wider digital-government agenda favours interoperability and common infrastructure. Digital Uzbekistan 2030 and subsequent measures promote integrated public information systems [4; 5]. Notarial systems benefit from direct access to civil-status, identity, cadastral, corporate and restriction data, but integration also creates cascading risk. An inaccurate source register can silently affect many acts; excessive data replication can expand the consequences of a breach. Cooperation must therefore include both service design and data-quality accountability.

Comparative models demonstrate different approaches. Germany provides a strong example of chamber-operated statutory infrastructure. The Federal Notaries Act assigns the Federal Chamber functions concerning the Central Register of Lasting Powers of Attorney, Central Register of Wills, Electronic Archive of Authentic Instruments, electronic notarial file storage, special electronic notarial mailbox and video communication system (sections 78a-78q) [6]. The practical advantage is institutional alignment: the body responsible for professional standards is deeply involved in building the tools through which those standards are performed. State legislation still defines authority, access and supervision.

Spain has developed a centralised electronic platform connecting all notaries with public administrations. Official notarial materials report that the notariat's electronic headquarters has enabled electronic supply of information and rapid cadastral ownership changes, supported by millions of electronically signed documents [8]. The example

shows how a national professional body can reduce fragmented bilateral integrations. Moreover, the public value lies not only in speed, structured notarial data can also enhance tax, cadastral, antimonopoly, and legal functions.

Estonia's e-notary environment integrates notarial work with state registers and supports remote authentication for eligible transactions [9; 10]. Its experience demonstrates the importance of controlled scope, strong digital identity and the notary's continuing discretion. Remote accessibility should not become an absolute right to perform any action online. At the same time, a notary must have the authority to require physical presence in cases where identity, legal capacity, voluntariness, or technical reliability give rise to doubt.

European Union law supplies horizontal safeguards. The eIDAS framework governs electronic identification and trust services, while the GDPR requires lawfulness, purpose limitation, data minimisation, security and accountability [7; 11]. UINL's digital principles emphasise that technology must preserve the notary's personal control, the authentic act and high security standards [12]. These standards support a "law first, architecture second" approach, that meaning that technological convenience cannot override the essential legal function.

A comparative analysis shows that the state must define mandatory legal conditions: eligible acts, territorial connection, accepted identity assurance, signature and time-stamp standards, evidence retention, accessibility, security baselines, audit powers and legal consequences of failure. It should approve high-risk changes and supervise compliance. The State should also ensure interoperability with authoritative registers and allocate responsibility for source-data accuracy.

In turn, the Chamber of Notaries must transform legal obligations into professional and technical specifications, operate or co-govern the professional platform where authorised, certify workflows, maintain training and competence requirements, monitor practice, issue non-binding methodological guidance and manage the first professional response to incidents. It should represent notarial users in procurement and change management, preventing a vendor-centred design from displacing professional judgment.

The competent state body and the Notary Chamber must jointly approve the e-governance charter and a confidential security annex. The charter should identify digital system owner, data controller or joint controllers, processor relationships, access roles, audit frequency, change-control thresholds, incident severity levels and service-continuity objectives. Decisions affecting the legal validity of acts must rest on legislation, not a software release note.

As a result of digitalization, technology providers must remain contractors, not bearers of public authenticity. Contracts should provide audit rights, data-location rules, subprocessor controls, secure development requirements, vulnerability disclosure, exit assistance and escrow or continuity arrangements where necessary. Neither the Ministry nor the Chamber should outsource accountability merely because operations are outsourced.

The proposed system will serve as a vital tool for the effective performance of notarial functions, addressing issues such as source-register inconsistency, national outage during signing, and remote identity fraud detection and, most importantly, enabling the rational use of AI.

A language model suggests clauses based on transaction data. The tool must be treated as assistance, not an autonomous decision-maker. Confidential data should not be transferred to an unapproved model; outputs must be traceable and reviewed by the notary. The Chamber should validate professional use cases and training, while the State defines prohibited automation and audit requirements. No system should make a final determination of capacity, voluntariness or legality without the notary.

It is recommended to treat AI as an assistant rather than an independent decision-maker. Confidential data must not be transmitted to an unapproved model, and results must be traceable and verified by a notary. The Chamber should validate professional use cases and training, while the State defines prohibited automation and audit requirements. No system should make a final determination of capacity, voluntariness or legality without the notary.

The detecting fraud using remote identification is no less important. The fraud detection function within the remote identification platform is equally important. In

practice, an individual seeking to perform a notarial act might present a genuine identity document while using a manipulated video feed. In such a case, the platform's "liveness check" tool would indicate a low level of confidence. Therefore, it is proposed that the system should not automatically reject or approve the transaction. Instead, it should notify the notary, preserve the relevant technical evidence, and facilitate a transition to in-person service.

Thus, the Law on Notariat should recognise "digital notarial infrastructure" as infrastructure used to create, perform, register, transmit or preserve notarial acts and related evidence. It should authorize a defined state-professional governance arrangement rather than leaving core responsibility to administrative practice. The law should state that use of technology does not diminish the notary's independence, duty of personal assessment or responsibility for the legal act.

In light of the foregoing, it is proposed to introduce the following amendments and additions to the Law on Notariat:

1) The Ministry of Justice establishes mandatory legal and information-security requirements for digital notarial infrastructure and supervises their observance. The Notarial Chamber participates in system governance, validates professional workflows, organises user competence, monitors notarial practice and coordinates operational response within its powers. The allocation of operational, data-protection and incident-management responsibilities shall be published, except for information whose disclosure would prejudice security.

2) A significant incident affecting identity verification, integrity, confidentiality, availability or preservation shall be reported without delay through the unified incident channel. The system operator shall contain the incident and preserve evidence; the Notarial Chamber shall notify and guide notaries, Ministry of Justice shall decide on mandatory restrictions and legal consequences. Resumption shall require documented verification against predefined criteria.

3) Automated systems may assist document preparation, consistency checks and risk alerts but shall not independently determine identity, capacity, voluntariness,

legality or the notary's decision to perform or refuse an act. Material automated outputs shall be reviewable and logged.

In turn, implementation should include annual independent security audits, role-based access, hardware-backed professional credentials, data-minimising logs, tested backups, recovery exercises, accessible alternatives for persons with disabilities, and regular red-team exercises addressing synthetic identity and social engineering. Aggregate performance indicators should include failed identity attempts, false positives, outages, recovery time, security incidents, cross-register discrepancies, remote-to-in-person conversion and user complaints.

Discussion

Chamber participation in infrastructure may raise concerns about monopoly and conflict of interest. Those concerns are legitimate because the same organisation may design a workflow and monitor professional compliance with it. The answer is not to exclude the Chamber, which would sacrifice essential practical knowledge, but to require transparent governance, independent technical audit, public procurement safeguards, appeal channels and state oversight of binding standards.

Centralisation also produces both benefits and systemic risk. A unified platform promotes uniform practice and efficient integration, yet a single vulnerability may affect the entire service. Architecture should therefore separate critical components, apply least privilege, maintain independent backups and provide legally defined degraded-service procedures. Governance must assume failure and prepare for it.

Finally, digital inclusion is a legal-certainty issue. Remote notarisation may benefit persons abroad, persons with mobility limitations and businesses requiring rapid transactions. Yet digital-only access can exclude users with low digital literacy or inadequate devices. The cooperative model should preserve in-person channels and provide assisted access without weakening identity and confidentiality safeguards.

Conclusion

Digital notarisation is sustainable only when legal authority, professional expertise and technical operations are connected by explicit accountability. Uzbekistan's recent joint regulatory work offers a promising foundation. Comparative practice shows that a

professional chamber can successfully operate or co-govern high-trust infrastructure while the State retains normative authority and legality supervision.

The recommended model assigns mandatory standards, public oversight, and legal consequences to a competent state authority, while entrusting the professional workflow, training, monitoring, and coordination at the primary level to the Chamber of Notaries, alongside shared responsibility for risks, changes, and incidents.

The recommended model assigns binding standards, public supervision and legal consequences to the competent state body, while professional workflow, training, monitoring and first-line coordination to the Notarial Chamber; and shared responsibility for risk, change and incidents. This arrangement protects authentic legal judgment while enabling secure, interoperable and citizen-centred digital services.

References

1. Republic of Uzbekistan. Law No. 343-I of 26 December 1996 “On Notariat,” as amended. https://lex.uz/docs/54458.

2. President of the Republic of Uzbekistan. Resolution No. PP-280 of 9 September 2025 “On Additional Measures to Further Develop the Institution of Notariat and Widely Introduce Modern Information and Communication Technologies.” https://lex.uz/docs/7722035.

3. Ministry of Justice of the Republic of Uzbekistan. Regulation on Performing Notarial Acts by Videoconference, registered No. 3742, 5 January 2026. https://lex.uz/docs/7976742.

4. President of the Republic of Uzbekistan. Decree No. PF-6079 of 5 October 2020 “Digital Uzbekistan 2030.” https://lex.uz/docs/5030957.

5. President of the Republic of Uzbekistan. Resolution No. PP-286 of 16 September 2025 on further development of the Digital Government system. https://lex.uz/docs/7730357.

6. Germany. Bundesnotarordnung [Federal Notaries Act], ss. 33, 35-36 and 78a-78q. https://www.gesetze-im-internet.de/bnoto/.

7. European Union. Regulation (EU) No. 910/2014 on electronic identification and trust services, as amended by Regulation (EU) 2024/1183 (European Digital Identity Framework). EUR-Lex.

8. Consejo General del Notariado. Official materials on the Notariat electronic headquarters and interconnection with public administrations. https://www.notariado.org/.

9. Estonia. Notaries Act, consolidated English text. Riigi Teataja. https://www.riigiteataja.ee/en/.

10. Chamber of Notaries of Estonia. E-notary and remote authentication information. https://www.notar.ee/en.

11. European Union. Regulation (EU) 2016/679 (General Data Protection Regulation), arts. 5, 25 and 32. https://eur-lex.europa.eu/eli/reg/2016/679/oj.

12. International Union of Notaries. Conclusions of the 29th International Congress of Notaries, Theme I: New Technologies and the Notarial Function. Jakarta, 2019. https://uinl.org/wp-content/uploads/2024/03/Jakarta-2019_Conclusions-Theme-I_EN.pdf.

13. OECD. Digital Government Index: 2019 Results. OECD Public Governance Policy Papers. Paris: OECD Publishing, 2020.

14. ENISA. Cybersecurity Guidelines for Trust Service Providers. European Union Agency for Cybersecurity.