Preventing Notary Fraud: Leveraging Existing Technologies & Trusted Records

June 2024

By Yehoshua Silberstein, Senior Counsel, Product Compliance R&D at Proof

Preventing Notary Fraud: Leveraging Existing Technologies & Trusted Records

As public officials, notaries are trusted to verify signers' identities and ensure the integrity of transactions. For hundreds of years, notarizations have been a trusted source in our communities to imbue everyday transactions with trust and legitimacy. However, notary fraud and impersonation have severely undermined this process, leading to significant legal and financial consequences. Today, criminals are exploiting current practices by stealing and forging notary credentials and seals to create counterfeit documents that appear legitimate.

The advent of remote online notarization (RON) allowed states to improve conventional notarization practices to ensure greater transparency, accountability, and authenticity in notarizations and associated documents.

States, through organizations such as the National Association of Secretaries of State (NASS), have put forth a common set of standards for the authorization and performance of RON, grounded in the issuance and application of digital certificates and a series of steps for remote signer identity verification.

As we continue into the second decade of RON, existing frameworks for identity proofing, digital certificates, and public registries can be leveraged and improved to thwart the threat of notary impersonation and forged notarizations and ensure a more secure notary ecosystem.

Addressing Notary Fraud and Impersonation

Over the past year, news stories involving allegations of notary fraud have been plentiful, particularly within the real estate industry. The schemes vary but often involve lifting a notary’s information and seal from public records to forge documents, impersonating signers to deceive unsuspecting notaries, or simply fraudulent notaries executing documents.

To help prevent these attacks, states should start by reviewing current commissioning procedures to ensure adequate identity verification for individuals applying for a commission. The signer identification process and records created during online notarization, such as video recordings, are significant deterrents to impersonation and fraud and should be leveraged to verify the identity of those applying for a commission.

Confirmation of a notary’s identity is foundational to the recommendations we make in the following sections regarding the use of digital certificates and registries. It empowers states to fortify the integrity of notarized documents and protect against the misuse of notary seals. By leveraging digital technologies to enhance the commissioning process, states can significantly reduce the risks associated with notary fraud and bolster the security and trustworthiness of notarization.

Enhancing the Security and Trustworthiness of Notarization

Digital certificates are the backbone of RON, replacing the traditional notary's physical stamp in a digital environment. They serve as a record of the notary's identity and a tamper seal for notarized documents, preserving their integrity post-notarization.

Role of Certificate Authorities

Notaries obtain their digital certificates from trusted issuers, referred to as Certificate Authorities, who are responsible for the maintenance, renewal, and revocation of digital certificates. Certificate Authorities subject each notary to an identity proofing process before issuing them a digital certificate. This certificate includes an X.509[1] file that identifies the Certificate Authority and notary and contains public and private encryption keys, known as an asymmetric key pair, which are used to encrypt and tamper-seal notarized documents.

Public Key Infrastructure (PKI) Technology

Digital certificate technology is based on public key infrastructure (PKI), which functions as a digital lock and key system. PKI, the same technology that secures websites and is foundational to the internet, is built on numerous technical standards developed by several organizations and international standards bodies.[2] Most modern-day operating systems, cloud services, and software applications support PKI technology, making digital certificates widely used for authentication, encryption, and digital signatures in various applications, including notarization.

Online Notarization Process

In the context of notarization, after verifying a signer's identity and completing the notarization, the notary uses their digital certificate to seal the document. The document is 'hashed' to create a unique identifier, which is then encrypted with the certificate's private key to produce ciphertext. This encrypted hash and the X.509 file are embedded in the document, creating a unique digital fingerprint and tamper-sealing it. This fingerprint shows who performed the notarization and confirms that the document has not been modified, as only the notary who was issued the digital certificate can access the private key and apply it to a document.

When the document is opened, the PDF reader will hash the document again to produce a plain-text hash, decrypt the embedded hash with the public key, and compare the two hashes to verify the document's integrity. Matching hashes confirm the document hasn't been modified, while different hashes indicate it has been changed and should not be trusted. PDF readers may use visual indicators, such as a

[1] ITU-T X.509: Public-Key and Attribute Certificate Framework

[2] ITU-T X.509: Public-Key and Attribute Certificate Framework; ISO/IEC 9594 Open Systems Interconnections; IETF RFC 5280: Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL); RSA Public Key Cryptography Standards (PKCS); NIST FIPS 186 Digital Signature Standard

green checkmark, for easy confirmation of the document's integrity and may also verify the certificate's status and whether it was issued by a trusted Certificate Authority.

Enhancing Private Key Security

Ensuring the security of private keys is critical to the success of digital certificates in notarization. While most states and Certificate Authorities acknowledge the need to secure the private keys of digital certificates, they often mandate only basic protections such as passwords. We strongly recommend that states enforce stronger security measures, such as multi-factor authentication. Additionally, states should mandate that notaries store their private keys on specialized USB sticks with cryptographic chips (e.g., Yubikeys) or hardware security modules (HSMs) compliant with NIST FIPS 140 Security Requirements. These devices enhance security by ensuring private keys are stored in a secure environment resistant to tampering, unauthorized access, and compromise. Finally, states should require notaries to use Certificate Authorities that adhere to industry best practices and hold third-party certifications, such as WebTrust for Certificate Authorities or Registration Authorities, Adobe Approved Trust List Membership, and US Federal Bridge Certificate Authority Certification. These stronger security measures will significantly reduce the risk of private key theft and help prevent notary impersonation.

Establishing a Digital Certificate Registry

Another measure that will significantly enhance the security and trustworthiness of notarized documents is the creation of a digital certificate registry. While some states, such as Kentucky, Tennessee, Texas, and Virginia, already require notaries to register their notary digital certificates with the state's notary public administrator, every state lacks a publicly accessible digital certificate registry. A more effective solution would be to enhance each state's notary lookup tool to include the issuing Certificate Authority and public key of each notary's certificate. This would allow recipients to open notarized documents in a PDF reader and inspect the signature properties. By comparing the "Issued to," "Issued by," and public key fields with the registry, recipients can cryptographically verify the identity of

notaries and the integrity of notarized documents.

Conclusion

In summary, stronger notary identification, enhanced security of private keys, compliance with industry best practices through third-party certifications, and a robust digital certificate registry are essential steps in ensuring the integrity and trustworthiness of digital notarizations. With these measures, states can provide greater assurance to the public and protect the integrity of the notarization process. These improvements build upon the existing infrastructure of online notarization, PKI technology, and Certificate Authorities, leveraging them to their full potential and securing the future of notarization.

About Proof:
Proof (formerly Notarize) is the industry leading platform for identity verification and online notarization. Proof is designed to deter and detect fraud. After years leading the market as an online notarization platform, Proof launched the first platform certified by the Kantara Initiative - a global non-profit assessing conformance with industry standards - linking a verified identity to an electronic signature compliant with NIST's rigorous Identity Assurance Level 2 (IAL2) standards.

Proof is an active partner and trusted resource to all levels of government and works to advance policies that prioritize consumer safety, accessibility, and the future of digital commerce.

Contact: James Fulgenzi, james.fulgenzi@proof.com