

LEGAL WHITE PAPER

Legalities of electronic signatures in the Philippines

Twala's tamper-proof electronic signature: the key to a fully digital economy.

PUBLISHED
October 2026
Version 20.0

AUTHORS
Atty. Herminio Bagro III, JD, MPA
Engr. Jeffrey Reyes, ECE, MTM
Atty. Emil Samaniego, JD

ISSUED BY
Twala (Ohelio Inc.)
Supreme Court-accredited ENF

■ CONTENTS

Legalities of electronic signatures

–	Introduction	3
01	Why are we still transacting things on paper?	3
02	Is an electronic signature the same as a digital signature?	3
03	What distinguishes digital signatures?	5
04	What is Twala, and how does it leverage PKI-based digital signatures and blockchain technology to ensure document security and prevent tampering or fraud?	7
05	Are documents signed with Twala legally acceptable and court-admissible?	9
06	Is electronic notarization legal in the Philippines?	18
07	Are electronic signature providers required to be accredited as such by any government agency to be valid and legally binding?	19
08	How does Twala ensure the security of its documents and network from cyber-attacks?	21
09	How does Twala protect users' data privacy?	22
10	Can government offices use Twala as a digital signing platform?	23
11	Does the Philippine government encourage the general public to use electronic documents and signatures?	26
12	Is blockchain a recognized technology in securing electronic documents, electronic signatures, and other digital transactions here in the Philippines and the rest of the world?	28
–	Conclusion	29
–	The authors	31
–	About Twala	33

■ ABOUT THIS EDITION

This white paper outlines the legal framework for electronic documents, electronic signatures, and electronic notarization in the Philippines, and how Twala complies with the applicable legal standards. Version 20 adds Twala's accreditation by the Supreme Court as an Electronic Notarization Facility, the country's first two eNotarized documents, Twala's HashOrigin™ document-security technology, and Twala's integration with the eGovPH Super App.

■ INTRODUCTION

Introduction

The Philippines' Republic Act No. 8792 or the E-Commerce Act of 2000 (ECA for brevity) aims to facilitate domestic and international dealings, transactions, arrangements, agreements, contracts, and exchanges and storage of information. This objective can be accomplished through the use of electronic, optical, and similar technologies and by recognizing the authenticity and reliability of electronic documents.

Close to a quarter of a century after the law's passage, there remains an ocean of potential for electronic signatures usage in the Philippines. While the Covid-19 pandemic forced both the public and private sector to work from home and meet online, transactions are still largely done via wet-signatures on paper.

But this too, is quickly changing. The private sector has been using electronic signatures, both for domestic and international transactions. Government agencies are catching up and have started to adopt and promote the use of these signatures by the public.

■ 01

Why are we still transacting things on paper?

Both the public and private sector agree that digitalization is the way of the future. But there is a huge gap between what is desired and what is put in practice. The reason for this is two-fold.

First, there are still many lingering questions as to the legality and trustworthiness of electronic documents and signatures. How are we sure all parties to the agreement actually signed it? Is the reviewed document the most current version? Will the reviewed document be exactly the same as the one the signer will approve? How can the document be verified before and after it was signed? Can one know if the signed document is unaltered even though it is viewed years down the road? Are electronic documents and signatures legal and admissible in court?

Second, there is a perceived high cost of migrating document processes and signing online. There are document management solutions offered at present but using them seems like imposing additional work to their users. Digital signatures have been offered by the private sector, but these are accessible only to large businesses due to its high cost. Government itself provided a free digital signature service, but its use has been very limited due to onboarding and ease of use issues.

Twala offers a service that addresses all these concerns. This white paper contains a brief on Twala and the technology that powers its intelligent document processing platform. It also outlines the current legal framework around electronic documents and signatures and how Twala complies with the applicable legal standards.

■ 02

Is an electronic signature the same as a digital signature?

Although many people use the terms "electronic signature" and "digital signature" interchangeably, they are actually two distinct concepts. While a digital signature is a specific type of electronic signature, not all electronic signatures are digital signatures.

Some online document signing solutions provide secure electronic signatures, but these differ from digital signatures. An electronic signature can take many forms, such as a drawn signature, an emoji, a photo, a typed name, a click on a button, or a recorded sound. The essential requirement is that the user adopts the mark and associates it with the electronic document or data message.

In contrast, a digital signature relies on complex mathematical algorithms to ensure the authenticity and integrity of an electronic document and signature. It generates a unique code that secures the data and prevents unauthorized alteration or forgery. Digital signatures are provided by trust service providers or information certifiers that verify the identity of the signers and guarantee the security, integrity, and reliability of the document.

The Philippines, like many other countries that have adopted the UNCITRAL Model Law on Electronic Commerce, has defined several types of electronic signatures.

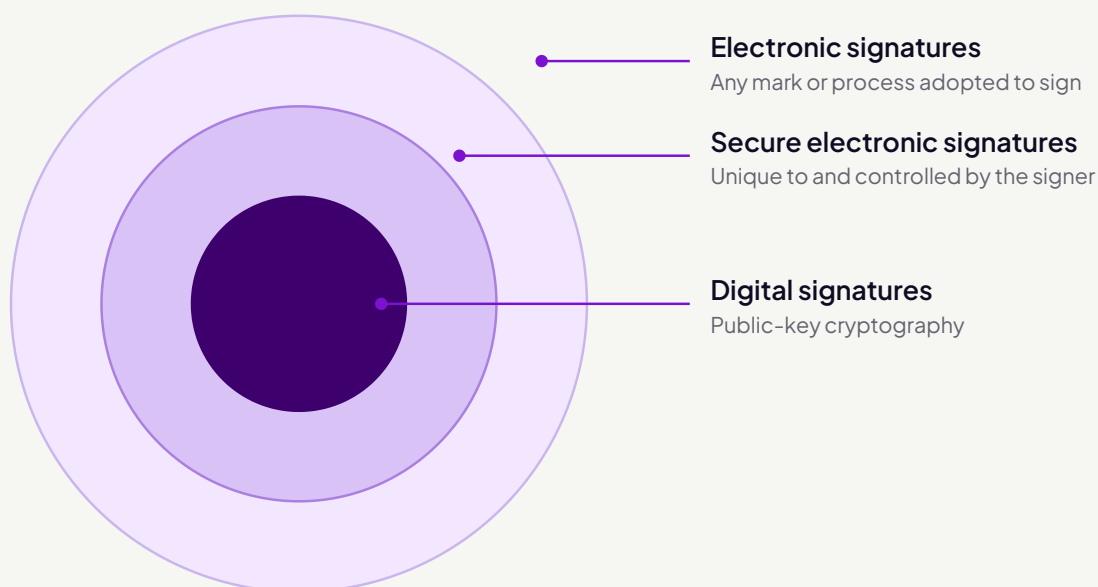


FIGURE 1 Types of electronic signatures. Every digital signature is a secure electronic signature, and every secure electronic signature is an electronic signature.

An *electronic signature* is any distinctive mark, characteristic, or sound in electronic form that represents the identity of a person and is attached to or associated with an electronic data message or document. It can also refer to any methodology or procedure employed or adopted by a person with the intention of authenticating or approving an electronic data message or document.¹

A *secure electronic signature* is one that is created and verified through a security procedure or combination of procedures that ensure its uniqueness to the signer, its objective identification of the signer, its creation and attachment to the data message by the signer or through a means under the signer's sole control, and its linkage to the data message in a way that reveals any change in the message.²

A *digital signature*, on the other hand, is an electronic signature that uses an asymmetric or public cryptosystem to transform an electronic document or data message, such that a person with the initial untransformed document and the signer's public key can accurately determine whether the transformation was created using the private key that corresponds to the signer's public key, and whether the initial document had been altered after the transformation was made.³

FIGURE 2. COMPONENTS OF ELECTRONIC SIGNATURES

TYPE	SIGNATURE MARK (IMAGE)	PASSWORD, MFA, OR DIGITAL SEAL	CRYPTOGRAPHIC DIGITAL SIGNATURE
Electronic signature	●		
Secure electronic signature	●	●	
Digital signature	●	●	●

PW = Password | MFA = Multi-Factor Authentication | Digital Seal = Cryptographic Digital Seal

NOTES

- 1
- Republic Act No. 8792, Electronic Commerce Act, Section 5(5)(e).
- 2
- DTI-DOST Joint Department Administrative Order No. 2–2001, Sec. 3(p).
- 3
- Supreme Court Rules on Electronic Evidence (SC REE), Sec. 1(e), and DTI-DOST Joint Department Administrative Order No. 2–2001, Sec. 3(d).

03

What distinguishes digital signatures?

Digital signatures are a foundational element of modern cybersecurity, enabling the verification of identity, data integrity, and non-repudiation across digital systems. They rely on asymmetric encryption, also known as public-key cryptography, which uses a public key to verify signatures and a private key to sign them. This cryptographic approach ensures that data remains secure, authentic, and tamper-proof—even when shared over insecure networks.⁴

Several algorithms power digital signatures, including:

- **RSA** – The most established algorithm used in PKI systems, widely applied in web and email security.⁵
- **ECDSA** – A modern, efficient algorithm offering strong security with smaller key sizes, heavily used in blockchain and mobile.⁶
- **DSA, ElGamal, and PKCS standards** – Other algorithms used in secure communications and compliance frameworks.

Real-world applications of digital signatures

- **Domain Validation & Web Security (SSL/TLS)** – Digital certificates signed using RSA or ECDSA are used to secure websites. Through SSL/TLS protocols, they authenticate domain ownership and encrypt web traffic, ensuring that users connect safely to legitimate websites.⁷
- **Email Security** – Standards like S/MIME and PGP use digital signatures to secure email content. Signed emails verify the sender’s identity and ensure the message hasn’t been altered, protecting sensitive communications from phishing and tampering.⁸
- **Code Security** – Software developers digitally sign code, installers, and updates to guarantee origin and integrity. Operating systems and app stores (like Windows, macOS, Android) verify these signatures to block malicious software and maintain software trust chains.⁹
- **Electronic Delivery Services** – In the context of trusted electronic registered delivery, digital signatures certify the sender, timestamp the transaction, and ensure that content cannot be altered during

transmission. These services are becoming standardized under eIDAS in Europe.¹⁰

- **Digital Identity & Verifiable Credentials** – Digital signatures are foundational to digital identity systems. Verifiable credentials such as diplomas, health records, and digital IDs are cryptographically signed and can be independently verified without relying on the issuer.¹¹
- **Document Security** – Digital signatures ensure that digital documents (e.g., contracts, board resolutions, permits) are authentic and tamper-evident. They provide legal enforceability and are widely adopted in e-governance, legal tech, and enterprise workflows.¹²
- **Distributed Ledger Technology (DLT)** – In blockchain networks, digital signatures (particularly ECDSA) are used to sign transactions and secure decentralized applications. Beyond cryptocurrency, they are also used in voting, supply chain traceability, document security, and identity systems. Upcoming EU regulations under eIDAS 2.0 will legally recognize DLT-based digital identity and signature solutions.¹³

Global and Philippine preference for digital and secure electronic signatures

Many jurisdictions around the world prefer the use of digital signatures or at minimum, secure electronic signatures, to ensure the authenticity, integrity, and legal admissibility of electronic documents. These types of signatures are considered tamper-evident and legally compliant.

In the Philippines, this preference is reflected in Section 8 of the E-Commerce Act, which underscores the importance of using reliable electronic signatures for legal validity. Various government bodies and sectors follow this standard:

- The Bangko Sentral ng Pilipinas (BSP), in its amended rules on deposits, requires that electronic signatures comply with Section 8 of the E-Commerce Act.
- The Anti-Red Tape Authority (ARTA), through its Memorandum Circulars, echoes the same requirement for secure electronic transactions.
- The Supreme Court, in its Rules on Electronic Evidence, acknowledges the probative value of digital signatures.
- Most recently, the 2025 Rules on Electronic Notarization mandate that electronic notaries (ENPs) must use digital or secure electronic signatures in their official acts.

This unified approach emphasizes the government's commitment to trusted digital transformation by promoting technologies that safeguard document security and legal enforceability.

NOTES

- 4 NIST FIPS PUB 186-5: Digital Signature Standard – <https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.186-5.pdf>
- 5 IETF RFC 5280: X.509 Certificate and CRL Profile – <https://datatracker.ietf.org/doc/html/rfc5280>
- 6 Ethereum.org: Cryptography and Digital Signatures – <https://ethereum.org/en/developers/docs/cryptography/#digital-signatures>
- 7 Mozilla Developer Network (MDN): How HTTPS Works – https://developer.mozilla.org/en-US/docs/Web/Security/How_https_works
- 8 IETF RFC 4880: OpenPGP Message Format – <https://datatracker.ietf.org/doc/html/rfc4880>
- 9 Microsoft Docs: Introduction to Code Signing – <https://learn.microsoft.com/en-us/windows/win32/seccrypto/code-signing-introduction>
- 10 ENISA: Electronic Identification and Trust Services (eIDAS) – <https://www.enisa.europa.eu/topics/trust-services/eidas>
- 11 World Economic Forum: Digital Identity Whitepaper – <https://www.weforum.org/whitepapers/digital-identity-towards-shared-principles-for-public-and-private-sector-cooperation/>
- 12 NIST: Using Digital Signatures for Document Authentication – <https://csrc.nist.gov/publications/detail/sp/800-102/final>
- 13 European Commission: eIDAS 2.0 Regulation Proposal – <https://digital-strategy.ec.europa.eu/en/policies/eidas-regulation>

What is Twala, and how does it leverage PKI-based digital signatures and blockchain technology to ensure document security and prevent tampering or fraud?

Twala is an intelligent document solutions platform that provides legally binding and secure electronic signatures, electronic notary services, digital identity services, and AI-powered document processing solutions. It is also an Electronic Notarization Facility (ENF) accredited by the Supreme Court of the Philippines. Designed to streamline and secure digital transactions, Twala combines traditional Public Key Infrastructure (PKI) with advanced technologies like blockchain and artificial intelligence to deliver trust, compliance, and efficiency across industries.

Twala secures electronic documents through a dual-layer approach, trademarked as **HashOrigin™**, that combines conventional PKI-based digital signature technology and blockchain-based integrity mechanisms. This hybrid model ensures robust protection against tampering, forgery, and data loss while complying with international legal and technical standards.

a. Object-level security: digital signatures and seals using PKI technology

At the document level, Twala uses Public Key Infrastructure (PKI) to apply digital signatures and seals that cryptographically bind the document content to a verifiable identity. Every completed document is sealed with the **Twala Platform Seal**, a digital signature made with Twala's X.509 certificate over the finished PDF, applied after the organization's own digital seal where a business has one. Each seal carries an RFC 3161 trusted timestamp, and long-term validation evidence is embedded so the signatures remain verifiable after their certificates expire. These signatures are:

- **Legally recognized** under the Philippine E-Commerce Act and Supreme Court Rules on Electronic Evidence.
- **Standards-based**, supporting the Cloud Signature Consortium (CSC) specifications to ensure compatibility with trusted certificate authorities and government requirements.
- **Tamper-evident**, meaning any alteration to the signed document will invalidate the signature, alerting all parties to potential fraud.

This layer provides the same trusted digital signature experience as conventional PKI solutions, making it ideal for users and jurisdictions that require compliance with established digital signature frameworks.

b. Blockchain-level security: HashOrigin™ technology

To strengthen the integrity and auditability of documents beyond PKI, Twala developed **HashOrigin™**, its trademarked blockchain-based verification technology, which answers a simple question for any document: is this exactly the file that was signed, sealed, or notarized, down to the last byte? Here's how it works:

- **Seal.** Each completed document is converted to PDF/A-2b and sealed with the Twala Platform Seal.
- **Fingerprint.** Twala computes and records the SHA-256 hash of the sealed file, a unique and irreversible fingerprint that changes completely if even one character of the document changes.
- **Batch.** Every 15 minutes, the fingerprints recorded since the last run are organized into a Merkle tree, ensuring that any change in content affects the final hash, while each document keeps its own anchor proof.
- **Anchor.** The Merkle root is written to Twala's smart contract on a public blockchain, in its own transaction, providing immutable and decentralized timestamping for verification.

- **Verify.** Anyone holding a copy can check it on Twala's verify page, or independently using the document's anchor proof.

This ensures that document integrity can be independently verified without exposing the document's contents, metadata, or actual signatures: only fingerprints are anchored, never documents or personal data. Because the proof is recorded on a public blockchain, verification does not depend on Twala as a single point of trust, enhancing both transparency and system resilience. This setup allows users to verify that a document has remained unchanged since it was sealed and securely anchored on the blockchain.

TWALA'S HASHORIGIN™ TECHNOLOGY

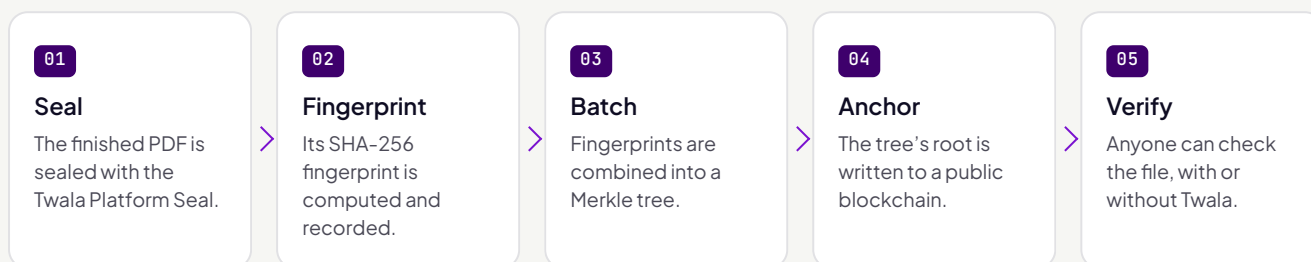


FIGURE 2 HashOrigin™ in five stages: every document Twala seals, whether signed, timestamped, or notarized, passes through the same process.

Batched anchoring on a public blockchain

HashOrigin anchors document fingerprints in batches. Every 15 minutes, the fingerprints of documents sealed within Twala are consolidated through a Merkle tree, and the root hash is anchored on a public blockchain in a transaction of its own. The anchoring contract stores each root with the time of its block, and every block produced afterward makes the record more difficult to alter, so the proof only grows stronger as the chain continues.

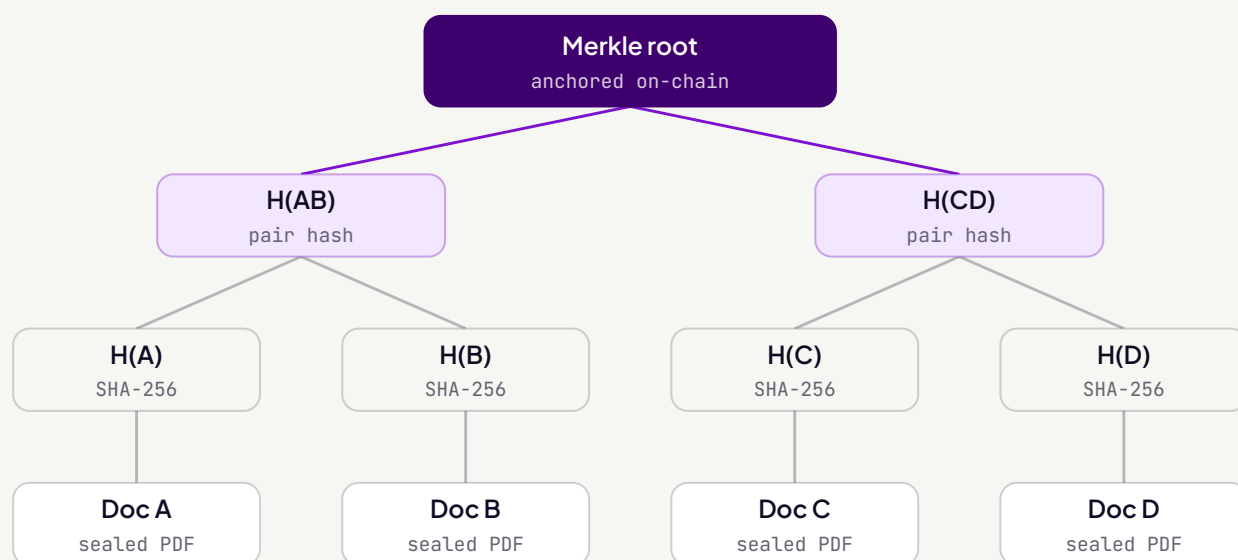


FIGURE 3 HashOrigin™ batching, simplified to four documents. Each document can be proven on its own by following its trail to the anchored root.

Industry recognition and R&D support

Twala's innovative use of blockchain for digital signatures has been officially recognized:

- In 2022, Twala received a ₱4.6 million grant from the Department of Science and Technology (DOST) through its Startup Grant Fund Program to enhance its R&D in blockchain-based trust services.
- Twala also signed an R&D partnership with the Advanced Science and Technology Institute (ASTI) to further its work on blockchain applications in digital signatures and digital identity.
- In 2026, Twala's document-security technology was trademarked as HashOrigin™, with a dedicated technical home at hashorigin.io that publishes anchor proofs and a sample verifier for anyone who would rather check than trust.

Twala bridges the gap between traditional PKI digital signatures and modern blockchain technology, providing a future-ready solution for secure and legally binding digital transactions. By combining object-level signatures with ledger-based proof, Twala protects documents from tampering, supports legal compliance, and ensures long-term verifiability in a decentralized and privacy-preserving manner.

■ 05

Are documents signed with Twala legally acceptable and court-admissible?

Yes. The Philippines has sufficient legal and administrative rules and issuances that recognize electronic signatures as equivalent to wet signatures. Twala uses technology, standards, and processes that comply with these rules.

a. The Electronic Commerce Act of 2000 (R.A. 8792)

The ECA establishes the legal framework for electronic commerce in the Philippines. Under Section 4, the law states that the law applies to all kinds of electronic data messages and electronic documents used in the context of both commercial and non-commercial activities, including domestic and international dealings, transactions, arrangements, agreements, contracts, and exchanges, and storage of information.

Following the structure of the UNCITRAL Model Law on Electronic Commerce, the ECA includes provisions for the legal recognition of data messages, electronic documents, and electronic signatures. It adopts the principle of functional equivalence, and Section 6 explicitly provides that “information shall not be denied validity or enforceability solely on the ground that it is in the form of an electronic data message purporting to give rise to such legal effect, or that it is merely incorporated by reference in that electronic data message.”

Legal standards for electronic documents and electronic signatures

The ECA provides for stringent standards that must be met before electronic documents and signatures can be considered equivalent to their analog counterparts. The relevant sections provide:

SECTION 7. Legal Recognition of Electronic Documents. — Electronic documents shall have the legal effect, validity, or enforceability as any other document or legal writing, and —

(a) Where the law requires a document to be in writing, that requirement is met by an electronic document if the said electronic document maintains its integrity and reliability and can be authenticated so as to be usable for subsequent reference, in that —

(i) The electronic document has remained complete and unaltered, apart from the addition of any endorsement and any authorized change, or any change which arises in the normal course of communication, storage and display; and

(ii) The electronic document is reliable in the light of the purpose for which it was generated and in the light of all relevant circumstances.

SECTION 8. Legal Recognition of Electronic Signatures. — An electronic signature on the electronic document shall be equivalent to the signature of a person on a written document if that signature is proved by showing that a prescribed procedure, not alterable by the parties interested in the electronic document, existed under which —

(a) A method is used to identify the party sought to be bound and to indicate said party’s access to the electronic document necessary for his consent or approval through the electronic signature;

(b) Said method is reliable and appropriate for the purpose for which the electronic document was generated or communicated, in the light of all circumstances, including any relevant agreement;

(c) It is necessary for the party sought to be bound, in or order to proceed further with the transaction, to have executed or provided the electronic signature; and

(d) The other party is authorized and enabled to verify the electronic signature and to make the decision to proceed with the transaction authenticated by the same.

These requirements prescribe a higher standard of reliability and integrity than what was provided under the UNCITRAL Model Law on Electronic Commerce.¹⁴ Thus, while the principle of functional equivalence was adopted by the ECA, not all electronic documents and electronic signatures enjoy this benefit. To rise to the legal status of a written document or a handwritten signature, the electronic document or signature must be shown to satisfy the specific requirements laid down in the law.

Twala’s document management and signing solution complies with these requirements, as follows:

TABLE 1. ELECTRONIC DOCUMENTS (SEC. 7, ECA; SEC. 10, ECA IMPLEMENTING RULES AND REGULATIONS)

	REQUIREMENTS TO ATTAIN FUNCTIONAL EQUIVALENCE	HOW TWALA IMPLEMENTS THE REQUIREMENT
1	Integrity is maintained	Twala uses both conventional public key infrastructure and blockchain-based integrity through HashOrigin™: every completed document is sealed with a PKI digital seal and its cryptographic fingerprint is anchored on a public blockchain, using international standards in cryptographic technology to make electronic documents tamper-proof.
2	Reliability is maintained	Twala adheres to international standards and best practices in information security and data privacy to ensure the reliability of its system. These include: Web Application ■ Strict password requirements for user accounts ■ Opt-in secure login using self-sovereign digital identity (Twala ID) for multi-factor authentication ■ Web Application Firewall (WAF) policy to protect the web and server applications from known vulnerabilities such as OWASP Top 10 vulnerabilities and attacks ■ Regular vulnerability assessments and penetration testing (VAPT) to identify and remediate potential security weaknesses ■ Proper network segmentation for private and public-facing applications as well as development and production environment ■ Daily database and object storage encryption and backup ■ Encryption in transit and at rest for sensitive data, using protocols such as SSL/TLS for transport layer encryption and AES for data at rest ■ Use of code analysis or Static Application Security Testing (SAST) tools to ensure code-level security and up-to-date security ■ Proactive adoption of industry best practices and guidelines

REQUIREMENTS TO ATTAIN FUNCTIONAL EQUIVALENCE	HOW TWALA IMPLEMENTS THE REQUIREMENT
	■ Branch policies used for source control management, where the main branch is protected and code reviews, quality gates, and security gates are required Mobile Security Standards ■ Use of PIN delegation and opt-in biometrics features, such as fingerprint and Face ID, for multi-factor authentication and transaction validation ■ Encrypted local data storage on device, using the secure key management systems native to Android and iOS ■ Use of code obfuscation techniques to make it difficult for attackers to reverse engineer the app, extract sensitive information, or exploit vulnerabilities ■ Use of app attestation and certificate pinning to help protect access to the backend server and prevent man-in-the-middle attacks, by attesting that the incoming traffic is coming from the app and blocking traffic that doesn't have valid credentials
3 Can be authenticated so as to be usable for subsequent reference, in that:	
3.a Document remains complete and unaltered, apart from any endorsement, authorized changes, or other changes in the normal course of communication, storage and display	When a document is completed in Twala, it is converted to the archival PDF/A-2b format and sealed with the Twala Platform Seal: a digital signature over a SHA-256 digest of the finished document, made with Twala's private key and backed by Twala's X.509 certificate. Where a business has its own digital seal, that seal is applied first and the Twala Platform Seal last, so it covers every signature on the document. Each seal carries an RFC 3161 trusted timestamp. The sealed file's SHA-256 fingerprint is then recorded and anchored on a public blockchain through HashOrigin™, ensuring that the document is complete, unalterable, and tamper-evident.
3.b Document is reliable in light of the purpose for which it was generated and in the light of all relevant circumstances.	Twala uses an internationally accepted digital signature algorithm standard used in digital signatures, smart contracts, and digital currencies around the world. This standard, called Elliptical Curve Digital Signature Algorithm (ECDSA) has been adopted by global standardization bodies such as: ■ The International Standards Organization (ISO 14888-3)¹⁵ ■ The American National Standards Institute (ANSI X9.62)¹⁶ ■ Accredited Standards Committee X9 Inc. (ECDSA. X9.142)¹⁷ ■ The Institute of Electrical and Electronic Engineers (IEEE 1363-2000),¹⁸ and ■ The US Department of Commerce's Federal Information Processing Standards Publication (FIPS 186-4 and 186-5)¹⁹ ECDSA is the digital signature algorithm used by major public blockchain networks, including the network on which HashOrigin™ anchors document fingerprints, to digitally sign transactions made in their network. Blockchain-based or DLT digital signature is now being used globally to sign and secure electronic documents. The European Union accredited the world's first blockchain-based trust service provider last 2020. Several companies in the EU, US, and Singapore are now offering blockchain-based digital signature services. Twala's seals are PKI-based digital signatures built on the X.509 standard used by the Cloud Signature Consortium, a global organization that advocates for cloud-based electronic and digital signature standards. Twala is a member of this Consortium.

TABLE 2. ELECTRONIC SIGNATURES (SEC. 8, ECA; SEC. 13, ECA IMPLEMENTING RULES AND REGULATIONS)

	REQUIREMENTS TO ATTAIN FUNCTIONAL EQUIVALENCE	HOW TWALA IMPLEMENTS THE REQUIREMENT
1	A prescribed procedure exists which is not alterable by the parties interested in the electronic document, under which:	When a document is completed in Twala, it is converted to the archival PDF/A-2b format and sealed with the Twala Platform Seal: a digital signature over a SHA-256 digest of the finished document, made with Twala's private key and backed by Twala's X.509 certificate. Where a business has its own digital seal, that seal is applied first and the Twala Platform Seal last, so it covers every signature on the document. Each seal carries an RFC 3161 trusted timestamp. The sealed file's SHA-256 fingerprint is then recorded and anchored on a public blockchain through HashOrigin™, ensuring that the document is complete, unalterable, and tamper-evident. For signers using PKI-based signatures to secure their documents, Twala also has the capacity to integrate these on top of the Twala Platform Seal and HashOrigin™ anchoring, while maintaining the above level of security.
1.a	A method is used to identify the signer and to indicate signer's access to the electronic document necessary for his consent or approval through an electronic signature	Twala uses a combination of industry-standard and bank-level technologies and processes to verify the identity of signers having access to its platform. This includes the following: ■ Email verification including via e-mail OTP, Open Authentication (OAuth), Single Sign On (SSO), and Active Directory (AD) standards ■ Mobile number verification via SMS One Time PIN (OTP) ■ Government-issued ID verification complemented by: ■ Optical character recognition (OCR) technology ■ Facial/biometric recognition technology ■ Liveness test powered by artificial intelligence ■ Manual verification Only verified users will be given a Twala account with access to the electronic document. A verified user can then access the electronic document necessary for his/her consent only after (1) being assigned access by the document owner, (2) being informed that a document was assigned to him/her for signing via email, and (3) logging onto their Twala account (via the Twala web app) using their password or their phone's biometric or facial authentication procedure.
1.b	Said method is reliable and appropriate for the purpose for which the electronic document was generated or communicated, in the light of all circumstances, including any relevant agreement	Twala uses an internationally accepted digital signature algorithm standard used in digital signatures, smart contracts, and digital currencies around the world. This standard, called Elliptical Curve Digital Signature Algorithm (ECDSA) has been adopted by global standardization bodies such as: ■ The International Standards Organization (ISO 14888-3) ■ The American National Standards Institute (ANSI X9.62) ■ The Institute of Electrical and Electronic Engineers (IEEE 1363-2000), and ■ The US Department of Commerce's Federal Information Processing Standards Publication (FIPS 186-2) (Citations on Table 1) ECDSA is the digital signature algorithm used by major public blockchain networks, including the network on which HashOrigin™ anchors document fingerprints, to digitally sign transactions made in their network. Blockchain-based or DLT digital signature is now being used globally to sign and secure electronic documents. The European Union accredited the world's first blockchain-based trust service provider last 2020. Several companies in the EU, US, and Singapore are now offering blockchain-based digital signature services. Twala's seals are PKI-based digital signatures built on the X.509 standard used by the Cloud Signature Consortium, a global organization that advocates for cloud-

REQUIREMENTS TO ATTAIN FUNCTIONAL EQUIVALENCE	HOW TWALA IMPLEMENTS THE REQUIREMENT
1.c The signer executes or provides the electronic signature in order to proceed further with the transaction, and	based electronic and digital signature standards. Twala is a member of this Consortium. Once the user has access to the electronic document after going through the verification described in 1.a above, s/he will be able to review the document in entirety. Once s/he is ready to sign, the user can: ■ Affix his electronic signature in the box assigned by either writing or typing his or her name in the space provided, or uploading a signature image then dragging-and-dropping the same to the space provided; ■ Once the signer is satisfied, s/he must click on the “submit signature” button to create and attach his/her signature to the document, which Twala then seals with the Twala Platform Seal. Twala deploys several layers of security to ensure that only verified users have access to their accounts and the means of signature creation to sign electronic documents. These include but are not limited to: ■ Device PIN or Patterns ■ Device Biometric Key – Fingerprint ■ Device Biometric Key – Facial ID ■ Identity App – PIN ■ Email OTP or token ■ SMS OTP or token ■ Password Twala’s digital identity also complies with internal standards on authentication/digital ID such as Fast Identity Online (FIDO2)²⁰, World Wide Web Consortium (W3C)²¹ and the US National Institute of Standards and Technology Special Publication (NIST SP) 800–63²².
1.d The other party is authorized and enabled to verify the electronic signature and to make the decision to proceed with the transaction authenticated by the same.	To verify a document, anyone can check the Twala Platform Seal using Twala’s public X.509 certificate: a PDF reader recomputes the document’s digest and confirms it against the seal, so any alteration after sealing is detected. Twala’s verify page also computes the file’s SHA-256 fingerprint, matches it with Twala’s records, and traces it to the Merkle root anchored on a public blockchain through HashOrigin™, returning “Document verified” for an unaltered file. Because the anchor is recorded on a public blockchain, creating an immutable record of the document’s existence and integrity, the document cannot be altered or tampered with without detection, providing an additional layer of security.

Since electronic documents and signatures transacted using Twala satisfy the requirements under the ECA, these documents and signatures rise to the level of and are afforded the same legal protection as written documents and handwritten signatures, respectively.

For example, if an electronic document or electronic signature becomes an issue in any litigation or other court process, they can be submitted as evidence. The ECA provides: “For evidentiary purposes, an electronic document shall be the functional equivalent of a written document under existing laws.”²³ It likewise states: “In any legal proceedings (sic), nothing in the application of the rules on evidence shall deny the admissibility of an electronic data message or electronic document in evidence on the sole ground that it is in electronic form; or on the ground that it is not in the standard written form.”²⁴

However, while a particular piece of electronic document or signature may be admissible as evidence, actually presenting it to a judge and be considered in deciding a case requires compliance with the Rules of Court²⁵, issued by the Philippine Supreme Court²⁶, particularly the rules of admissibility of evidence.

b. The Supreme Court Rules on Electronic Evidence

On July 17, 2001, the Supreme Court issued the Rules on Electronic Evidence²⁷ (REE for brevity) to align the Rules of Court with the substantive changes brought about by the ECA, which took effect a year before. The REE is applicable in all criminal²⁸ and civil actions and proceedings, as well as quasi-judicial and administrative cases.²⁹

Under the Rules of Court, a document can only be presented in court as evidence, if (1) it is an original copy³⁰ and, (2) for private³¹ documents, its due execution and authenticity is proven.³² Significantly, the REE provides that “a person seeking to introduce an electronic document in any legal proceeding has the burden of proving its authenticity” in the manner it specified.³³

Below is a summary of the relevant rules and how Twala-signed documents squarely address them.

TABLE 3. PRESENTING ELECTRONIC DOCUMENTS IN COURT (REE)

REQUIREMENTS	HOW TWALA ADDRESSES THE REQUIREMENT
1 Must be an original copy. An electronic document shall be regarded as the equivalent of an original document “if it is a printout or output readable by sight or other means, shown to reflect the data accurately.” (Rule 4, Section 1)	When a document is completed in Twala, it is converted to the archival PDF/A-2b format and sealed with the Twala Platform Seal: a digital signature over a SHA-256 digest of the finished document, made with Twala’s private key and backed by Twala’s X.509 certificate. Where a business has its own digital seal, that seal is applied first and the Twala Platform Seal last, so it covers every signature on the document. Each seal carries an RFC 3161 trusted timestamp. The sealed file’s SHA-256 fingerprint is then recorded and anchored on a public blockchain through HashOrigin™, ensuring that the document is complete, unalterable, and tamper-evident. Every completed document is thus protected at the object level by an X.509 digital seal, the Twala Platform Seal, and organizations that prefer conventional PKI-based digital signatures via their own X.509 digital certificate can also apply a digital signature or digital seal at the object-level. Twala-signed documents are readable by sight using a PDF viewer on any computer or mobile device. It includes a statement that it has been digitally signed, and contains a document universal unique identifier (UUID), a QR code containing the signer’s digital ID, a QR code for document verification, and a comprehensive audit trail that includes: ■ Name of the signer/s ■ The digital ID of the signer/s ■ Email of the signer/s ■ ID information such as type of ID and ID number if required by the document owner ■ Digital timestamp of transactions related to the document/s (e.g. when the document has been sent, viewed, and signed). If needed, the original electronic document may also be printed out and will bear all the information above and reflect the data in the document accurately.
1.b Duplicate originals allowed. When a document is “in two or more copies executed at or about the same time with identical contents, or is a counterpart produced by the same impression as the original, or from the same matrix, or by mechanical or electronic re-recording, or	Once a document is signed and completed using Twala, copies of the electronic document are emailed to the owner of the document, all the signers, as well as other recipients identified by the document owner. All these copies are actually originals in themselves as these are exactly the same. But these too fall squarely within the definition of duplicate originals under this Section, as these documents are executed at the same

REQUIREMENTS	HOW TWALA ADDRESSES THE REQUIREMENT
by chemical reproduction, or by other equivalent techniques which accurately reproduces the original, such copies or duplicates shall be regarded as the equivalent of the original.” (Rule 4, Section 2)	time with identical contents. Either way, the legal effect is the same – that these electronic documents are all regarded as original.
2 Document must be authenticated. Before any private electronic document offered as authentic is received in evidence, its authenticity must be proved by any of the following means: ■ a. by evidence that it had been digitally signed by the person purported to have signed the same; ■ b. by evidence that other appropriate security procedures or devices as may be authorized by the Supreme Court or by law for authentication of electronic documents were applied to the document; or ■ c. by other evidence showing its integrity and reliability to the satisfaction of the Judge. (Rule 5, Section 2)	For a party intending to authenticate a Twala-processed document, s/he must only present the original electronic document (the PDF or, if required, a print-out of the same). The document includes a statement that it has been digitally or securely e-signed, and an audit trail that records the data of the signers and the document -- their digital ID, e-mail, mobile number, ID submitted during the sign-up process, IP address, geolocation, and digital timestamp. Twala’s electronic signature complies with the standards provided by the rules. Twala also provides an easy method for the Judge to easily check -- in real-time -- the integrity and reliability of the document, as follows: ■ Its digital seal³⁴ uses a public cryptosystem: the Twala Platform Seal is created with Twala’s private key and verified with Twala’s public X.509 certificate, which ensures that any transformation of the electronic document after sealing is detectable. It also provides an accessible way to verify whether the document has been altered or tampered with after the transformation was made, i.e. by uploading the signed document on Twala’s verify page, or independently, using the document’s anchor proof to check its fingerprint against the record on the public blockchain, as described at hashorigin.io. ■ Its secure electronic signature³⁵ uses the same HashOrigin™ technology, identification and security procedures, and verification processes: the signer’s electronic signature is bound to the document by the cryptographic digital seal. These security measures ensure the integrity and reliability of the electronic document, which can easily be verified by any person having access to the document itself.
3 Signature must be authenticated. An electronic signature may be authenticated in any of the following ways: ■ a. By evidence that a method or process was utilized to establish a digital signature and verify the same; ■ b. By any other means provided by law; or ■ c. By any other means satisfactory to the judge as establishing the genuineness of the electronic signature. (Rule 6, Section 2)	For a party intending to authenticate a digital or secure electronic signature, s/he must only present the original electronic document (the PDF or, if required, a print-out of the same). This serves as evidence that the document underwent a process to establish a digital signature or electronic signature, as follows: ■ A Twala-signed document includes a statement that it has been digitally or securely e-signed, and an audit trail that records the relevant data of the signers and the document -- their digital ID, e-mail, mobile number, ID submitted during the sign-up process, IP address, geolocation, and digital timestamp. ■ Twala provides an accessible way to verify whether the document has been altered or tampered with after the transformation was made, i.e. by uploading the signed document on Twala’s verify page, or independently, using the document’s anchor proof to check its fingerprint against the record on the public blockchain, as described at hashorigin.io. This provides a way to satisfactorily establish the genuineness of the electronic signature used. ■ For customers that prefer the use of PKI-based digital signatures and seals, this can be done via AATL verification on the PDF-level. ■ For documents securely e-signed using Twala, we refer to Section 11³⁶ of the ECA, which identifies the means to

REQUIREMENTS	HOW TWALA ADDRESSES THE REQUIREMENT
	authenticate electronic documents and electronic signatures. As mentioned above, secure electronic signature uses the same HashOrigin™ technology, identification and security procedures, and verification processes, with a cryptographic digital seal binding the signature to the document. This methodology ensures that the person signing had the intention of authenticating or approving the electronic document, and that a security procedure is in place to verify the originator of said document.
4 Method of proof in court. “All matters relating to the admissibility and evidentiary weight of an electronic document may be established by an affidavit stating facts of direct personal knowledge of the affiant or based on authentic records. The affidavit must affirmatively show the competence of the affiant to testify on the matters contained therein.” (Rule 9, Section 1)	The party intending to present in evidence a document that is digitally signed or securely e-signed, in the context of a court proceeding, must: ■ Produce the original electronic document (the PDF or, if required, a print-out of the same, including the audit trail), and ■ Ensure that a person who has personal knowledge of the preparation, signing, transmission, and/or receipt of the document executes an affidavit showing his/her competence in testifying on the matters contained in the document.³⁷ As a guide in preparing said affidavit, the affiant may simply refer to, affirm, and attest the truth of the audit trail’s contents, and declare that said affidavit is being made to comply with the requirements of the REE.
5 When authentication is not required. A document electronically notarized in accordance with the rules promulgated by the Supreme Court (SC) shall be considered as a public document and proved as a notarial document under the Rules of Court. (Rule 5, Section 3)	The Supreme Court of the Philippines, through A.M. No. 24–10–14–SC, or the Rules on Electronic Notarization, promulgated on February 4, 2025, and effective as of March 24, 2025, now allows the notarization of electronic documents. On August 5, 2026, the Supreme Court accredited Twala as an Electronic Notarization Facility (ENF) under these Rules. Twala, through its electronic notarization platform, utilizes the same secure and standards-based digital signature technology to enable notaries public to perform legally binding, remote, and paperless notarization. By integrating identity verification, audit trails, and tamper-evident digital seals secured by HashOrigin™, Twala ensures that electronic notarization is not only compliant with Supreme Court rules but also enhances efficiency and accessibility in legal workflows, preserving the integrity and trustworthiness of notarized documents in the digital age.³⁸ Note that the ECA gave the SC the option to “adopt such other authentication procedures, including the use of electronic notarization systems as necessary and advisable.”³⁹

After an electronic or digital signature is authenticated in the manner described above, they give rise to certain beneficial legal presumptions. This means certain statements are by law presumed to be factual, and may only be overturned by presenting evidence to the contrary.⁴⁰ As can be seen from the table below, digital signatures are entitled to presumptions that not only pertain to the signature, but to the information contained in the certificate⁴¹ or digital ID, as well as the reliability of the message associated with the digital signature, among others.

TABLE 4. DISPUTABLE PRESUMPTIONS RELATING TO ELECTRONIC SIGNATURES (REE)

	UPON AUTHENTICATION, IT SHALL BE PRESUMED THAT: (RULE 6, SECTIONS 3-4)	ELECTRONIC SIGNATURE ⁴²	DIGITAL SIGNATURE
1	The electronic signature is that of the person to whom it correlates	●	●
2	The electronic signature was affixed by that person with the intention of authenticating or approving the electronic document to which it is related or to indicate such person's consent to the transaction embodied therein	●	●
3	The methods or processes utilized to affix or verify the electronic signature operated without error or fault	●	●
4	The information contained in a certificate is correct		●
5	The digital signature was created during the operational period of a certificate		●
6	No cause exists to render a certificate invalid or revocable		●
7	The message associated with a digital signature has not been altered from the time it was signed		●
8	A certificate had been issued by the certification authority indicated therein		●

NOTES

- 14 See discussion on Annotations on the E-Commerce Act Implementing Rules and Regulations by Jesus M. Disini, Jr. (September 2000), pp. 14–15 and 17–18.
- 15 ISO/IEC 14888–3:2018 – IT Security techniques — Digital signatures at <https://www.iso.org/standard/76382.html>.
- 16 ANSI X9.62–1998 – Public Key Cryptography For The Financial Services Industry: The Elliptic Curve Digital Signature Algorithm (ECDSA) at <https://webstore.ansi.org/standards/ascx9/ansix9621998>.
- 17 ASC X9 Issues New Standard for Public Key Cryptography/ECDSA at <https://x9.org/asc-x9-issues-new-standard-for-public-key-cryptography-ecdsa/>.
- 18 1363–2000 – IEEE Standard Specifications for Public-Key Cryptography at <https://ieeexplore.ieee.org/document/891000>.
- 19 FIPS 186–5 – Digital Signature Standard (DSS) at <https://csrc.nist.gov/publications/detail/fips/186/5/final>.
- 20 The FIDO Alliance is an open industry association launched in February 2013 whose stated mission is to develop and promote authentication standards that “help reduce the world’s over-reliance on passwords.” See <https://fidoalliance.org/>.
- 21 The World Wide Web Consortium is the main international standards organization for the World Wide Web. See <https://www.w3.org/>.
- 22 US National Institute of Standards and Technology – Digital Identity Guidelines. See <https://pages.nist.gov/800-63-3/>.
- 23 Section 7, penultimate paragraph.
- 24 Section 12.
- 25 The 1997 Rules of Civil Procedure As Amended, (April 8, 1997).
- 26 Article VIII Section 5(5) of the 1987 Philippine Constitution provides that the Supreme Court has the power to Promulgate rules concerning pleading, practice, and procedure in all courts, among others.
- 27 Administrative Matter No. 01–7–01–SC.
- 28 On September 24, 2002, the SC issued a resolution expanding the coverage of the REE to criminal cases. The amendment took effect on October 14, 2002 following its publication in the Manila Bulletin, a newspaper of general circulation. The Supreme Court, in a 2014 case, agreed with the trial court in admitting a text message as evidence against the accused, using as basis the September 2002. (*People v. Enojas y Hingpit*, G.R. No. 204894, [March 10, 2014])
- 29 REE, Rule 1, Section 1.
- 30 The general rule is that when the subject of inquiry in a legal proceeding is the contents of a document, writing, recording, photograph or other record, no evidence shall be admissible other than the original of the document itself. (Rule 130 (B) Section 3, The Revised Rules on Evidence, A.M. No. 19–08–15–SC [Resolution], August 10, 2019.)
- 31 Rules of Court, Rule 132 (B) Section 19. “For the purpose of their presentation evidence, documents are either public or private. Public documents are: (a) The written official acts, or records of the official acts of the sovereign authority, official bodies and tribunals, and public officers, whether of the Philippines, or of a foreign country; (b) Documents acknowledged before a notary public except last wills and testaments; and (c) Public records, kept in the Philippines, of private documents required by law to be entered therein. All other writings are private.”
- 32 Rules of Court, Rule 132 (B) Section 20.
- 33 REE, Rule 5, Section 1.
- 34 Recall that a digital signature differs from other electronic signatures in its use of asymmetric or public cryptography in the signing process. See footnote 4 for its full definition.

- 35 Recall that a secure electronic signature refers to an electronic signature created and verified through a security procedure or combination of procedures that ensure its uniqueness to the signer, its objective identification of the signer, its creation and attachment to the data message by the signer or through a means under the signer's sole control, and its linkage to the data message in a way that reveals any change in the message. See DTI-DOST Joint Department Administrative Order No. 2-2001, Sec. 3[p].
- 36 "[E]lectronic documents, electronic data messages and electronic signatures, shall be authenticated by demonstrating, substantiating and validating a claimed identity of a user, device, or another entity in an information or communication system, among other ways, as follows: a. The electronic signature shall be authenticated by proof that a letter, character, number or other symbol in electronic form representing the persons named in and attached to or logically associated with an electronic data message, electronic document, or that the appropriate methodology or security procedures, when applicable, were employed or adopted by a person and executed or adopted by such person, with the intention of authenticating or approving an electronic data message or electronic document; b. The electronic data message or electronic document shall be authenticated by proof that an appropriate security procedure, when applicable was adopted and employed for the purpose of verifying the originator of an electronic data message or electronic document, or detecting error or alteration in the communication, content or storage of an electronic document or electronic data message from a specific point, which, using algorithm or codes, identifying words or numbers, encryptions, answers back or acknowledgment procedures, or similar security devices."
- 37 See *RCBC Bankard Services Corporation vs. Moises Oracion, Jr. and Emily Oracion*, G.R. No. 223274 (June 19, 2019).
- 38 SC Approves Rules on Electronic Notarization: Advancing Digital Innovation and Access to Justice, <https://sc.judiciary.gov.ph/sc-approves-rules-on-electronic-notarization-advancing-digital-innovation-and-access-to-justice/>
- 39 Section 11, paragraph 3, RA 8792.
- 40 Rules of Court Rule 131, Section 3.
- 41 "Certificate" means an electronic document issued to support a digital signature which purports to confirm the identity or other significant characteristics of the person who holds a particular key pair. (REE, Rules 2, Section 1[c]) A digital ID is a type of a certificate.
- 42 Includes secure electronic signatures.

■ 06

Is electronic notarization legal in the Philippines?

Yes, electronic notarization is now officially legal in the Philippines.

On February 4, 2025, the Supreme Court approved the Rules on Electronic Notarization under A.M. No. 24-10-14-SC, marking a significant step forward in modernizing legal processes in the country. These rules took effect on March 24, 2025, and introduced two modes of electronic notarization:

- **In-Person Electronic Notarization (IEN)** – The notary and signatories are physically present, but the notarization process is conducted electronically.
- **Remote Electronic Notarization (REN)** – The notary and signatories are in separate locations, and the notarization is performed via secure videoconferencing technology.

These forms of notarization require the use of tamper-proof electronic and digital signatures to ensure document integrity and authenticity. Such signatures are cryptographically secured, making them resistant to alteration and providing verifiable proof of identity and consent.

The rules also mandate multi-factor authentication methods—including facial recognition, biometrics, and one-time passwords—to verify the identities of parties involved. Additionally, notarized electronic documents must be in PDF or PDF/A format, and all records must be securely stored within compliant Electronic Notarization Facilities (ENFs) governed by the Data Privacy Act.

It is important to note that certain documents, such as notarial wills, depositions, and traditional paper documents with wet signatures, remain outside the scope of electronic notarization and are still governed by the 2004 Rules on Notarial Practice.

This legal framework enhances the accessibility, security, and efficiency of notarial services, particularly benefiting individuals in remote locations and Filipinos abroad.

Twala: a Supreme Court–accredited Electronic Notarization Facility

On August 5, 2026, the Supreme Court of the Philippines accredited Twala as an Electronic Notarization Facility (ENF) under the Rules on Electronic Notarization (A.M. No. 24–10–14–SC), one of the first three facilities accredited. The accreditation authorizes Twala to provide electronic notarization services nationwide. The platform incorporates essential features such as tamper-proof electronic signature, video conferencing, electronic Know Your Customer (e-KYC) mechanisms, multi-factor authentication, and liveness detection functionalities, ensuring secure and compliant electronic notarization processes, with every notarized document sealed and anchored through HashOrigin™. Twala’s commitment to these standards positions it as a reliable solution for modernizing notarial services in the country.

Aug 5, 2026

Supreme Court accreditation of Twala as an ENF

1 of 3

First facilities accredited under the 2025 Rules

Oct 19, 2026

The Philippines’ first two eNotarized documents, notarized on Twala

Twala made history: the Philippines’ first two eNotarized documents

On October 19, 2026, in Taguig City, electronic notarization officially launched in the Philippines, and the country’s first two electronically notarized documents were notarized on Twala. They were agreements with the Integrated Bar of the Philippines (IBP), supporting free legal aid under the Supreme Court’s Unified Legal Aid Service, and with the University of the Philippines College of Law, on legal technology and the responsible use of AI in legal practice.

The signing was witnessed by First Lady Louise Araneta-Marcos and Supreme Court Senior Associate Justice Marvic M.V.F. Leonen, the event’s Guest of Honor, together with representatives from government, the legal profession, business, banking, and real estate.

“Secure eNotarization removes geographical and physical barriers bringing legal protection to small players, safely and instantly.”

Senior Associate Justice Marvic M.V.F. Leonen, Supreme Court of the Philippines, at the October 19, 2026 launch

■ 07

Are electronic signature providers required to be accredited as such by any government agency to be valid and legally binding?

No. According to the ECA’s implementing rules and regulations issued by the Departments of Trade and Industry and Science and Technology,⁴³ accreditation is voluntary. So long as information certifiers⁴⁴ (like electronic signature providers) issue certificates “in accordance with commercially appropriate and internationally recognized standards, or where sufficient evidence indicates that the certificate accurately binds the secure electronic signature to the signer’s identity,” these certificates are valid and legal.

As discussed above, Twala deploys globally recognized technologies, standards, and processes in securing and processing electronic documents and digital signatures.

To date, no information certifier or certification authority⁴⁵ has been accredited by the government from among the existing private electronic signature providers, both foreign and domestic.

The role of the DTI as accrediting authority for certification authorities and digital signature providers

The power to accredit Certification Authorities (CAs) and regulate digital signature service providers is vested solely in the Department of Trade and Industry (DTI), as mandated by Executive Order No. 810, Series of 2009, and implemented through DTI Department Administrative Order (DAO) No. 10–09, Series of 2010⁴⁶.

While EO 810 outlines the national policy to institutionalize the use of digital signatures in government, and assigns the Department of Information and Communications Technology (DICT) the role of managing the Philippine National Public Key Infrastructure (PNPKI), it is the DTI that holds exclusive authority to accredit public Certification Authorities and digital signature providers.

DAO 10–09 specifically prescribes the rules governing the accreditation of CAs, ensuring compliance with security, reliability, and legal standards under the E-Commerce Act (RA 8792). Accreditation is intended to certify that a provider meets stringent requirements for trustworthiness and interoperability in both public and private sector transactions.

However, it is important to note that DTI has not accredited any Certification Authority or digital signature service provider since the issuance of DAO 10–09, as the accreditation process has remained voluntary and has not been actively implemented.

Recognizing that DAO 10–09 is now outdated and not aligned with current technologies and market practices, the DTI is currently in the process of revising its accreditation rules to make them more relevant, practical, and responsive to the evolving digital ecosystem.

Electronic notarization is different

While accreditation of electronic signature providers remains voluntary, electronic notarization may be performed only through Electronic Notarization Facilities accredited by the Supreme Court. Twala received this accreditation on August 5, 2026.

NOTES

- ⁴³ Implementing Rules and Regulations on Electronic Authentication and Electronic Signatures. DTI-DOST Joint Department Administrative Order (JDAO) No. 02 Series of 2001, issued on September 28, 2001.
- ⁴⁴ An information certifier is “any person who, or entity which, in the course of its business, issues certificates as a means of providing identification services and/or certifying information which are used to support the use of and trust in secure electronic signatures.” The term includes, but is not limited to, certification authorities. (Section 3[k], *ibid.*)
- ⁴⁵ “Certification authority” is a type of information certifier which, in the course of its business, engages in issuing certificates in relation to cryptographic keys used for the purposes of digital signatures. (Section 3[c], *ibid.*)
- ⁴⁶ DTI Department Administrative Order (DAO) No. 10–09, Series of 2010, Prescribing Rules Governing The Accreditation Of Certification Authorities For Digital Signatures

How does Twala ensure the security of its documents and network from cyber-attacks?

Twala is a secure platform that adheres to international standards and best practices for information security and data privacy, including the International Organization for Standardization's ISO 27001, the world's best-known standard for information security management systems and their requirements.⁴⁷ By implementing these requirements, Twala ensures the confidentiality, integrity, and availability of its users' data.

- **Information security policy and objectives.** Twala has established information security policy and goals that outline the company's commitment to security and assigns roles and responsibilities for security-related tasks.
- **Risk assessment and management.** Twala conducts regular risk assessments to identify and mitigate potential security threats and vulnerabilities. Twala uses a risk-based approach to prioritize its security controls and allocate resources effectively.
- **Asset management.** Twala maintains an inventory of its information assets and applies appropriate security controls to protect those assets.
- **Access control.** Twala implements access controls to restrict access to sensitive information based on job roles and responsibilities. Twala uses strong authentication methods and monitors user activity to prevent unauthorized access to its systems.
- **Cryptography.** Twala uses encryption to protect sensitive information in transit and at rest. Twala uses industry-standard encryption protocols such as SSL/TLS and AES to protect data.
- **Physical and environmental security.** Twala implements physical and environmental security controls to protect its systems and data centers from physical threats such as theft, fire, and natural disasters.
- **Operations security.** Twala maintains secure operations by implementing secure configuration management practices, conducting regular vulnerability assessments and penetration testing, and maintaining backups of critical data and systems.
- **Communications security.** Twala implements secure communication protocols such as SSL/TLS to protect data in transit.
- **System acquisition, development, and maintenance.** Twala follows secure software development practices, conducts code reviews and static code analysis to identify and fix security vulnerabilities in its software development process, and implements secure configuration management practices to ensure that system configurations are secure and maintained in a consistent manner.
- **Supplier relationships.** Twala applies appropriate security controls to its suppliers to ensure that they meet Twala's security requirements.
- **Information security incident management.** Twala has an incident response plan in place that outlines the steps to be taken in the event of a security incident, including reporting the incident, containing the impact, and conducting a post-incident review to identify lessons learned and opportunities for improvement.
- **Business continuity management.** Twala maintains a business continuity plan to protect its operations in the event of a security incident.
- **Compliance with legal and regulatory requirements.** Twala complies with various laws and regulations, such as the Data Privacy Act and the Anti-Cybercrime Law.

- **Security organization and management.** Twala has partnered with an information security firm in implementing and maintaining the company's information security program.

For its web application, Twala uses the following security mechanisms:

- Strict password requirements for user accounts and opt-in secure login using self-sovereign digital identity (Twala ID) for multi-factor authentication
- Web Application Firewall (WAF) policy to protect the web and server applications from known vulnerabilities such as OWASP Top 10 vulnerabilities and attacks
- Regular vulnerability assessments and penetration testing (VAPT) to identify and remediate potential security weaknesses provided by a Department of Information and Communications Technology (DICT)-recognized cyber security firm
- Proper network segmentation for private and public-facing applications as well as development and production environment
- Daily database and object storage encryption and backup, and encryption in transit and at rest for sensitive data using protocols such as SSL/TLS for transport layer encryption and AES for data at rest
- Use of code analysis or Static Application Security Testing (SAST) tools to ensure code-level security and up-to-date security, and
- Proactive adoption of industry best practices and guidelines, and branch policies used for source control management where the main branch is protected and code reviews, quality gates, and security gates are required.

Twala likewise implements the following security standards for its mobile application:

- Use of PIN delegation and opt-in biometrics features such as fingerprint and Face ID for multi-factor authentication and transaction validation
- Encrypted local data storage on the device using the secure key management systems native to Android and iOS
- Use of code obfuscation techniques to make it difficult for attackers to reverse engineer the app, extract sensitive information, or exploit vulnerabilities, and
- Use of app attestation and certificate pinning to help protect access to the backend server and prevent man-in-the-middle attacks, by attesting that the incoming traffic is coming from the app and blocking traffic that doesn't have valid credentials.

NOTES

- ⁴⁷ See International Organization for Standardization, <https://www.iso.org/isoiec-27001-information-security.html>.

How does Twala protect users' data privacy?

Twala recognizes and respects the importance of data privacy and is committed to adhering to global privacy standards, such as the European Union's General Data Protection Regulation (GDPR)⁴⁸, and the Philippines' Data Privacy Act of 2012⁴⁹. As a registered company with the National Privacy Commission, Twala has implemented various measures to ensure the protection of personal data, including obtaining explicit consent from users before collecting and processing any personal data, limiting access to personal data to authorized personnel

only, and implementing appropriate technical and organizational measures to ensure the confidentiality, integrity, and availability of personal data. Additionally, Twala regularly conducts privacy impact assessments and data protection impact assessments to identify and address potential risks to personal data. Twala also provides users the ability to access, rectify, erase, and restrict the processing of their personal data, in compliance with applicable privacy regulations.

NOTES

- 48 The General Data Protection Regulation (GDPR) is the European Union's privacy and security law, <https://gdpr.eu/what-is-gdpr/>
- 49 An Act Protecting Individual Personal Information and Communications Systems in the Government and the Private Sector, Creating for this Purpose a National Privacy Commission, and for Other Purposes, Republic Act No. 10173, August 15, 2012.

■ 10

Can government offices use Twala as a digital signing platform?

Yes. Since the year 2000, it has been the state's objective to promote the universal use of electronic transactions in the "government and by the general public".⁵⁰ In fact, the Philippine Development Plan 2023–2028, the country's overall blueprint for development planning, describes the digitalization as the very first strategy in the nation's transformation, saying: "Digital transformation of government will result in more efficient and faster service delivery to the people, more transparency, and fewer opportunities for corruption at various levels."⁵¹

In 2021, the Commission on Audit released the Guidelines on the Use of Electronic Documents, Electronic Signatures, and Digital Signatures in Government Transactions.⁵² These rules "apply when the audited agency submits electronic documents to the auditor in lieu of paper documents, where the signature of an authorized signatory is required."⁵³

The COA circular allows a government agency to use electronic signatures, secure electronic signatures, digital signatures, or a combination,⁵⁴ in securing their electronic documents "such as but not limited to, procurement-related documents, disbursement vouchers, requisition and issuance slips, purchase orders, contracts, and memoranda, among others."⁵⁵

Below is a summary of the key provisions of the COA Circular:

General principles and guidelines (IV.A)

- Submission of electronic documents with electronic signatures (including digital signatures) shall mean sufficient compliance to the requirement of submission of a duly signed document used in government transactions.
- When under existing rules a document requires a signature, the use of electronic signature (including digital signature) shall be an accepted alternative and shall be equivalent to the wet signature of a person on a document.
- Private parties transacting with the government, "may use other types of electronic signature, subject to the controls implemented by the transacting government entity."

Responsibilities of management in using electronic documents (IV.B)

- “All government entities that elect to use and/or implement a system using digital signature or other types of electronic signature on electronic documents under this Circular shall issue internal rules in the adoption of the same, including sanctions for unauthorized and illegal use of digital certificates or electronic signatures.”
- “They shall submit a Management Representation or Policy Statement on the use of signatures on electronic documents in their operations to their respective Auditors, together with the approved internal rules.” Note: A standard template of the Management Representation is annexed to the circular, making compliance easier for government agencies.

Specific rules on the use of digital signatures (IV.C)

- All officials and employees designated/authorized to sign documents using digital signature shall apply with the DICT where they shall undergo identity verification and training.
- Alternatively, they may apply for their individual certificates from any other service provider accredited or recognized by the Department of Trade and Industry – Philippine Accreditation Bureau (DTI-PAB) to issue digital certificates to be used in government transactions.
- To ensure digitally-signed documents can be verified, these shall be maintained in its original form and submitted electronically. Print-outs of documents are considered duplicates or secondary copies and shall have a notation (footer) or disclosure “The original of this document is in digital format” or other similar language.

Specific rules on the use of electronic signatures (other than digital signature) (IV.D)

When the officer opts to use an electronic signature other than a digital signature (provided by the DICT) on an electronic document, the signed electronic document may be validly accepted provided the agency is able to establish that:

- the electronic signature is that of the person to whom it correlates;
- the electronic signature was affixed by that person with the intention of authenticating or approving the electronic document to which it is related or to indicate such person’s consent to the transaction embodied therein;
- the methods or processes utilized to affix or verify the electronic signature, if any, operated without error or fault; and
- the person whose e-signature was affixed, takes responsibility and assumes accountability that the document remained unchanged until it was submitted to the auditor.

The COA Circular No. 2021-006, Section IV.D, explicitly allows government agencies to adopt alternative electronic technologies or solutions—such as Twala—provided they meet the prescribed requirements for legality, security, and integrity. This gives agencies the flexibility to use modern platforms that comply with COA standards for digital transactions, signatures, and document management.

In 2020, the Anti-Red Tape Authority (ARTA) released Memorandum Circular No. 2020-06, a landmark directive aimed at streamlining government processes and accelerating the country’s shift toward digital governance. The circular directed all government agencies to recognize and adopt the use of electronic and digital signatures in official transactions, including those issued by private providers that comply with the standards set by the Department of Information and Communications Technology (DICT) and the Electronic Commerce Act. Specifically, agencies were encouraged to utilize the Philippine National Public Key Infrastructure (PNPKI) of the DICT for digitally signing documents, while also allowing for alternative compliant solutions from the private

sector (e.g. Twala). This policy laid the groundwork for modernizing public service delivery through secure, efficient, and legally recognized digital tools.⁵⁶

Twala, a Philippine startup providing intelligent document and digital signature solutions, meets all requirements set forth by ARTA, DICT, the Commission on Audit (COA), the Department of Trade and Industry (DTI), and the Supreme Court, positioning itself as a key enabler in the government's digital transformation efforts.

Twala and DICT Philippine National Public Key Infrastructure (PNPKI) compatibility

For government agencies that require or prefer the use of digital certificates issued by the Department of Information and Communications Technology (DICT), Twala provides full compatibility and enhanced flexibility.

Twala's platform supports both Public Key Infrastructure (PKI) and blockchain-based digital signatures, making it fully interoperable with the DICT's Philippine National Public Key Infrastructure (PNPKI). This means that government personnel can use their X.509 digital certificates issued by PNPki to digitally sign documents directly within the Twala platform.

By using their DICT-issued certificates into Twala, agencies can enable secure online and remote digital signing, automate document routing and approval workflows, and manage files via encrypted cloud storage. The platform also includes built-in features for audit trails, timestamping, role-based access, and compliance with COA, ARTA, and Data Privacy Act requirements, ensuring that all digital transactions meet national standards for trust and security.

Whether for internal approvals, citizen-facing services, or inter-agency coordination, Twala empowers government offices to shift from manual paperwork to digitally signed, legally compliant, and efficient e-documents—all while using the credentials already issued by the DICT.

Twala and the eGovPH Super App

Twala is integrated with the eGovPH Super App, the government's one-stop app for public services, making electronic notarization easier to access through a platform already used by millions of Filipinos. The integration brings Twala's Supreme Court-accredited eNotarization closer to citizens, and complements Twala's verification of the Philippine National ID against the national registry, so that government services and the documents they require can move online together.

From announcement to integration

Twala announced its eGovPH Super App integration at the official launch of electronic notarization on October 19, 2026. Today, citizens can reach Twala's eNotarization services through the eGovPH Super App, alongside the other public services it brings together.

NOTES

⁵⁰ Section 3, ECA.

⁵¹ P. 14, Philippine Development Plan 2023–2028. Accessed at <https://pdp.neda.gov.ph/philippine-development-plan-2023-2028/>.

⁵² COA Circular 2021–006, dated September 6, 2021. See https://coa.gov.ph/wpfd_file/coa-circular-no-2021-006-september-6-2021/.

⁵³ Rule II, Scope and Coverage, id.

⁵⁴ Note 3 of Annex A, id.

⁵⁵ Rule IV.A.2, id.

⁵⁶ ARTA affirms thru COA validity of electronic/digital signatures and online payments in gov't transactions, <https://arta.gov.ph/press-releases/arta-affirms-thru-coa-validity-of-electronic-digital-signatures-and-online-payments-in-govt-transactions>

Does the Philippine government encourage the general public to use electronic documents and signatures?

Yes. Apart from the law and rules mentioned above, various other laws and instruments have highlighted the government's continued push for the use of electronic documents and signatures.

- **Tax Reform for Acceleration and Inclusion (TRAIN), Republic Act No. 10963, (December 19, 2017).** The law provides that within five (5) years, and upon the setup of a system capable of storing and processing the required data, the Bureau of Internal Revenue (BIR) shall require taxpayers engaged in the export of goods and services, taxpayers engaged in e-commerce, and taxpayers under the jurisdiction of the Large Taxpayers Service to issue electronic receipts or sales or commercial invoices in lieu of manual receipts or sales or commercial invoices. It added that taxpayers not covered by said mandate may issue electronic receipts or sales or commercial invoices, in lieu of manual receipts, and sales and commercial invoices.⁵⁷ Implementing the above law, the BIR on June 30, 2022 issued Revenue Regulations No. 8-2022 and prescribed the requirements on the issuance of e-Receipts and/or e-Invoices in lieu of the manual receipts or sales/commercial invoices and on the electronic reporting of these sales data to the BIR.
- **Ease of Doing Business and Efficient Government Service Delivery Act of 2018, Republic Act No. 11032, (May 28, 2018).** Section 9 (e) of the law provides that electronic signatures or pre-signed licenses, clearances, permits, certifications or authorizations with adequate security and control mechanisms may be used by government offices and agencies including local government units (LGUs), government-owned or -controlled corporations and other government instrumentalities, whether located in the Philippines or abroad, that provide services covering business and nonbusiness related transactions. Per Section 11 (c), cities/municipalities are also mandated to automate their business permitting and licensing system or set up an electronic business one-stop shop (BOSS) within a period of three (3) years upon the law's effectivity.

Implementing the above provisions, the Anti-Red Tape Authority (ARTA), the DTI, Department of Interior and Local Government (DILG), and the DICT, issued on April 13, 2021 the Guidelines for Processing Business Permits, Related Clearances and Licenses in All Cities and Municipalities.⁵⁸

- LGUs were mandated to use authenticated digital signatures or electronic signatures in the business permit that will be issued to the applicants for business permits. LGUs were also directed to "avail of and recognize the use of the Philippine National Public Key Infrastructure (PNPKI) of the DICT or utilize other secured available means of digitally signing official documents such as offered by private entities, in accordance with issuances by the DICT."⁵⁹
- The head of the LGU was also tasked to issue the appropriate inter-office memorandum stating the rules on controls for the use of the digital signatures as well as proper identification and delegation of authority to alternate signatories in the absence of the regular signatory.⁶⁰
- **ASEAN Agreement on Electronic Commerce (January 22, 2019).** Under Article 7 of this Agreement, member states shall not deny the legal validity of a signature solely on the basis that the signature is in electronic form.⁶¹
- **Revised Corporation Code of the Philippines, Republic Act No. 11232, (February 20, 2019).** This law allows the filing of a corporation's articles of incorporation and applications for amendments thereon with the Securities and Exchange Commission (SEC) in the form of an electronic document, in accordance with SEC rules and regulations.⁶² The SEC was also tasked to develop and implement an electronic filing and monitoring system and to promulgate rules to facilitate and expedite, among others, corporate name

reservation and registration, incorporation, submission of reports, notices, and documents required under this Code, and sharing of pertinent information with other government agencies.⁶³

- **United Nations Convention on the Use of Electronic Communications in International Contract (Ratified by the Philippines on July 12, 2022; entered into force on February 1, 2023).** The Electronic Communications Convention aims to enhance legal certainty and commercial predictability where electronic communications are used in international contracts. It provides criteria for establishing functional equivalence between electronic communications and paper documents with respect to legal requirements such as “writing”, “original” and “signature”, building upon legal principles and provisions contained in other United Nations Commission on International Trade Law (UNCITRAL) texts on electronic commerce, such as the UNCITRAL Model Law on Electronic Commerce, already adopted in some 160 jurisdictions across more than 80 countries.⁶⁴
- **Bangko Sentral ng Pilipinas (BSP) Circular No. 1163 (December 14, 2022).** The BSP amended Section 276 of the Manual of Regulations for Banks (MORB) and explicitly recognized the acceptability of electronic signatures pursuant to Section 8 of the ECA. Section 1 of the Circular provides:

“For opening any type of deposit account/establishing relationship under the true and full name of the depositor, all banking institutions are required to obtain a minimum of three (3) specimen signatures, simultaneously executed by the depositor, either wet or electronic, or biometrics (such as fingerprints, iris scans, or facial recognition images) from their depositors and to update the same, as applicable, based on risk and materiality. Banks may, at their option, require their depositors to submit clear ID photos.

“Electronic signatures shall be accepted pursuant to the provisions of Section 8 of R.A. No. 8792 or the Electronic Commerce Act of 2000.”

- **Ease of Paying Taxes Act, Republic Act No. 11976, (January 5, 2024).** The law explicitly allowed the various tax processes -- from registration to filing of returns on all types of taxes -- to be done electronically. To improve service delivery, Section 43 of the law mandates the BIR to adopt an integrated digitalization strategy by providing automated end-to-end solutions for the benefit of taxpayers, through, among others, taking measures to set up electronic and online systems that will make the means of exchanging data and information secure, efficient, and seamless, and streamlining procedures by adopting automation and digitalization of BIR services to minimize face to face transactions. Note that previously, the BIR issued Revenue Memorandum Circular No. 29–2021 (February 26, 2021) prescribing the policies and guidelines for the use of electronic signatures only on a few BIR Forms/Certificates⁶⁵. The withholding agents or duly authorized representatives of the withholding agents who issue said BIR Forms/Certificates have the option (without need of BIR pre-approval) to use e-signatures, which shall serve as the functional equivalent of his/her manual signature.

NOTES

⁵⁷ See Section 237 (Issuance of Receipts or Sales or Commercial Invoices).

⁵⁸ ARTA-DTI-DILG-DICT Joint Memorandum Circular No. 01, S. 2021.

⁵⁹ Section 8.6.2, id.

⁶⁰ Section 8.6.3, id.

⁶¹ Accessed at <https://agreement.asean.org/media/download/20190306035048.pdf> on February 12, 2024.

⁶² Section 13, Revised Corporation Code of the Philippines, Republic Act No. 11232, (February 20, 2019).

⁶³ Section 180, id.

⁶⁴ “The Philippines ratifies the UN Electronic Communications Convention”, accessed at <https://unis.unvienna.org/unis/en/pressrels/2022/unisl332.html>.

⁶⁵ BIR Forms 2304 (Certificate of Income Payment Not Subject to Withholding Tax [Excluding Compensation Income]), 2306 (Certificate of Final Tax Withheld at Source), 2307 (Certificate of Creditable Tax Withheld at Source), and 2316 (Certificate of Compensation Payment/Tax Withheld).

■ 12

Is blockchain a recognized technology in securing electronic documents, electronic signatures, and other digital transactions here in the Philippines and the rest of the world?

Yes. Blockchain technology is internationally and locally recognized for its superiority in terms of security, integrity, and reliability.

Blockchain technology has emerged as a robust solution for securing digital documents, ensuring their integrity and authenticity. Notably, the first use case of blockchain—nearly two decades before Bitcoin—was to secure electronic documents. In their 1991 paper, *How to Time-Stamp a Digital Document*, Stuart Haber and W. Scott Stornetta introduced the use of cryptographic hashes to link digital records into an immutable chain, effectively establishing the foundational principles of blockchain technology. This early innovation laid the groundwork for blockchain's evolution from document security to more complex applications like cryptocurrencies. Since then, blockchain has gained international recognition for its security, integrity, and reliability in safeguarding electronic documents, digital signatures, and various digital transactions.⁶⁶

The principles established by Haber and Stornetta have been instrumental in various applications beyond cryptocurrencies. For instance, in the healthcare sector, blockchain is being explored to secure Electronic Health Records (EHRs), ensuring that patient data remains unaltered and accessible only to authorized individuals. By leveraging a decentralized ledger, healthcare providers can maintain a tamper-proof record of patient information, enhancing trust and compliance with data protection regulations.⁶⁷

Today, blockchain is globally and locally recognized as a superior technology for securing electronic documents, electronic signatures, and digital trust services.

- Electronic signature companies in the US, EU, and other countries are using blockchain-based signatures.
- China has implemented blockchain technology in its e-notary system⁶⁸, and the European Union and South Korea plan to launch blockchain-powered services by 2024⁶⁹.
- The Archangel project is a research initiative funded by the EPSRC⁷⁰ in the UK to investigate the use of blockchain technology for the digital preservation and archiving of cultural heritage.⁷¹
- The entire European Union is transitioning PKI-based trust service providers to blockchain via the EIDAS Bridge for digital signature and other use cases.⁷²
- The EU accredited the world's first blockchain-based trust services provider (TSP) in 2020, via the EU Trust List.⁷³
- Estonia uses blockchain technology to enforce the integrity of government data and systems including the use of blockchain-based digital signatures.⁷⁴
- Statistics Canada uses blockchain and embedded digital signatures to authenticate official documents, ensuring they remain genuine and tamper-proof since publication.⁷⁵
- The Philippines has recognized blockchain technology through various initiatives such as:
 - the Bangko Sentral ng Pilipinas' Pioneer Regulatory Framework for Virtual Currency Exchanges,⁷⁶
 - the Securities and Exchange Commission's Draft of Digital Asset Exchange,⁷⁷
 - The charter of the Bataan freeport zone⁷⁸ of Bataan introduced the term "cryptocurrency," the underlying value of which is blockchain technology,

- the Cagayan economic zones “Crypto Valley of Asia” initiative⁷⁹,
- Union Bank’s project i2i⁸⁰, and the Philippine Bureau of the Treasury’s application for the distribution of government bonds enabled by blockchain technology⁸¹,
- The Department of Information and Communications Technology spearheading a national blockchain summit in Bataan⁸², and lastly,
- The Department of Science and Technology training their researchers in blockchain technology.⁸³

NOTES

- 66 Haber, S., & Stornetta, W. S. (1991). How to time-stamp a digital document. *Journal of Cryptology*, 3(2), 99–111. <https://doi.org/10.1007/BF00196791>
- 67 Casado-Vara, R., Prieto, J., De la Prieta, F., & Corchado, J. M. (2019). How blockchain improves the security and transparency of digital documents. SSRN. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=5181147
- 68 Notary office in Shanghai applies blockchain technology with success, http://en.moj.gov.cn/2020-11/04/c_560984.htm
- 69 South Korea Aims to Boost Economy With Digital ID on Blockchain, <https://www.bloomberg.com/news/articles/2022-10-16/south-korea-aims-to-boost-economy-with-digital-id-on-blockchain>
- 70 The Engineering and Physical Sciences Research Council (EPSRC) is a British Research Council that provides government funding for grants to undertake research and postgraduate degrees in engineering and the physical sciences.
- 71 ARCHANGEL - Trusted Archives of Digital Public Records, <https://www.archangel.ac.uk/>
- 72 About SSI eIDAS Bridge, <https://joinup.ec.europa.eu/collection/ssi-eidas-bridge/about>
- 73 Guardtime offers world’s first EU-eIDAS accredited blockchain-based trust service, <https://guardtime.com/blog/guardtime-offers-first-eu-e-eidas-accredited-blockchain-based-trust-service>
- 74 Estonian blockchain technology, <https://e-estonia.com/solutions/cyber-security/ksi-blockchain/>
- 75 Statistics Canada. (2022). Authenticating official documents using blockchain technology. Retrieved from <https://www150.statcan.gc.ca/n1/pub/11-633-x/11-633-x2022007-eng.htm>
- 76 Circular No. 1108 - Bangko Sentral ng Pilipinas, <https://www.bsp.gov.ph/Regulations/Issuances/2021/1108.pdf>
- 77 SEC releases draft rules on digital asset trades, <https://www.bworldonline.com/editors-picks/2019/07/17/242481/sec-releases-draft-rules-on-digital-asset-trades/>
- 78 Republic Act No. 11453 or “An Act Further Strengthening the Powers and Functions of the Authority of the Freeport Area of Bataan (AFAB), Amending for this Purpose Republic Act No. 9728, Otherwise Known as the “Freeport Area of Bataan (FAB) Act of 2009,” August 30, 2019.
- 79 CEZA host blockchain, fintech webinar, <https://ceza.gov.ph/ceza-hosts-blockchain-fintech-webinar/>.
- 80 UnionBank’s blockchain-based i2i network powers financial inclusion in PH, <https://www.bloomberg.com/press-releases/2019-10-29/unionbank-s-blockchain-based-i2i-network-powers-financial-inclus>.
- 81 Philippine Treasury is Asia Pioneer in Leveraging Distributed Ledger Technology (Blockchain) for Treasury Bonds, <https://business.inquirer.net/303055/philippine-treasury-is-asia-pioneer-in-leveraging-distributed-ledger-technology-blockchain-for-treasury-bonds>.
- 82 The promise of blockchain, <https://mb.com.ph/2022/11/01/the-promise-of-blockchain/>.
- 83 DOST starts blockchain technology training for in-house technologists, <https://www.philstar.com/headlines/2022/05/28/2184309/dost-starts-blockchain-technology-training-house-technologists>.

CONCLUSION

Conclusion

Tamper-proof electronic signatures are essential to building a secure and fully digital economy, ensuring the integrity, authenticity, and legal validity of digital documents. Twala makes this vision a reality through its intelligent document solutions platform, offering secure electronic signatures, e-notary services, digital identity verification, and AI-powered document processing. These tools empower individuals, businesses, and government agencies to streamline workflows and digitize operations with confidence.

By leveraging both traditional Public Key Infrastructure (PKI) and decentralized ledger technology (blockchain) through HashOrigin™, Twala provides verifiable, tamper-proof signatures that meet the highest standards of security, transparency, and compliance. Its end-to-end document management system — from preparation and routing to signing, tracking, and archiving — boosts efficiency and cuts operational costs.

As a Supreme Court–accredited Electronic Notarization Facility, the platform on which the Philippines’ first two eNotarized documents were notarized, and a partner of the eGovPH Super App, Twala carries this trust from the signature to the notarial act and into public services.

As digital transformation accelerates, Twala stands at the forefront, enabling a paperless, secure, and trusted digital future for the Philippines and beyond.

■ THE AUTHORS

The authors

Atty. Herminio Bagro III, JD, MPA

For thirteen years, Atty. Herminio Bagro III served as public sector manager and legal counsel to members of the Cabinet and Senators across four administrations.

He started out as a legal assistant to the labor relations commission while taking up law, and after graduating, as staff to former Senator Mar Roxas in 2010. After ranking 8th in the 2009 bar examinations, he joined the government, first as Director, then as Undersecretary and Deputy Head of the Presidential Management Staff, during the term of late President Benigno S. Aquino III. In 2016, he crossed over to the legislative branch and served as chief-of-staff to three-term Senator Francis N. Pangilinan, who headed successively the Senate committees on agriculture and constitutional amendments. In 2022, he was appointed as Undersecretary for Legal and Legislative Affairs in the Department of Trade and Industry (DTI), serving under Secretary Fred Pascual.

Realizing the huge potential of technology in democratizing legal access in the country, he co-founded two startups: Twala, a blockchain-powered digital identity and signatures provider, and FLO Attorneys-at-Law, a firm offering tech-enabled legal services. He is currently the US-ASEAN Business Council's country representative in the Philippines.

He has served as a lecturer in constitutional law at the University of the Philippines (UP), where he graduated with degrees in Philosophy (cum laude) and Juris Doctor. It was also at UP that he understood the transformative potential of public service – as both a student and leader. In 2008, he was elected student council Chairman, during the University's 100th year. Herminio pursued public administration in academia and earned a Masters in Public Administration (MPA) from the Maxwell School at Syracuse University, New York as a Fulbright scholar.

Engr. Jeffrey Reyes, ECE, MTM

Engr. Jeffrey Reyes serves as the Co-founder and Chief Executive Officer of Twala, a pioneering document intelligence platform powered by AI and secured by PKI and blockchain technology. Twala offers secure and tamper-proof electronic signature, electronic notarization, digital identity, and intelligent document processing solutions, delivering end-to-end digital trust services for individuals and organizations. The company is supported by the Department of Science and Technology through the Startup Grant Fund Program and is a member of the Cloud Signature Consortium, a global organization of digital trust service providers. Twala is also a graduate of the IdeaSpace Foundation's Startup Acceleration Program and the winner of the first La French Tech Startup Competition in 2022, supported by the French Chamber of Commerce in the Philippines and the Government of France.

With more than 15 years of extensive experience in Information Technology, Engr. Reyes has held pivotal roles in systems and software development, IT product and project management, quality assurance, information security, and data privacy. His professional journey spans renowned multinational corporations in the Philippines, the United States, Singapore, and the European Union.

At Twala, Engr. Reyes leads research and development initiatives across various domains, including cryptography, distributed ledger technology (DLT), PKI, digital identity, digital signatures, electronic notarization, artificial intelligence, information security and privacy, and software engineering. He also serves as a volunteer IT consultant for the Philippine Consulate in Dublin, Ireland.

In recognition of his contributions to innovation and the startup ecosystem, Engr. Reyes was named to Esquire Magazine's Startup Trailblazer List of 2024, highlighting the most influential movers and shakers in the Philippine startup landscape.

He is a licensed Electronics and Communications Engineer by the Professional Regulation Commission (PRC) and a proud member of the Institute of Electronics Engineers of the Philippines (IECEP). Engr. Reyes earned his Master's degree in Technology Management from the University of the Philippines - Diliman and a Bachelor of Science in Electronics and Communications Engineering from the Polytechnic University of the Philippines - Manila. He further enriched his academic credentials through a specialized program on education policies at the International Academy for Leadership in Gummersbach, Germany.

Atty. Emil Samaniego, JD

Atty. Emil L. Samaniego is a junior associate from Sarmiento Loriga Law Office. His practice areas include litigation, technology, competition and trade law. He has worked on projects involving Virtual Assets Service Providers (VASP) license application from Bangko Sentral ng Pilipinas (BSP). He also renders legal assistance and advisories to start-ups and corporations from pre-incorporation to restructuring, merger and acquisition (M&A). He is currently part of a team working on a major constitutional litigation case in the Supreme Court. He obtained his Juris Doctor degree in San Beda University.

■ ABOUT

About Twala

Twala is a Philippine-based technology company that offers a secure and intelligent document platform for digital signatures, electronic notary, identity verification, and AI-powered document lifecycle management. It empowers individuals, professionals, and organizations to execute and manage legally binding documents electronically, with the highest standards of security, integrity, and compliance.

Built on blockchain and public key infrastructure (PKI) technologies, Twala enables tamper-evident, cryptographically verifiable digital transactions through its HashOrigin™ technology. Its platform serves high-trust use cases across government, legal, enterprise, and financial sectors.

A multi-awarded technology startup, Twala is backed by the Department of Science and Technology (DOST) and Philippine Council for Industry, Energy, and Emerging Technology Research and Development (DOST-PCIEERD) through its Startup Grant Fund Program and maintains active R&D partnerships with DOST-ASTI. Twala has also collaborated with key public institutions such as the DICT, the Senate, and the Anti-Red Tape Authority (ARTA).

Importantly, Twala collaborated with the Supreme Court of the Philippines on the drafting of the 2025 Rules on Electronic Notarization, lending its technical expertise in digital signature infrastructure and e-notarization technology to help shape the regulatory framework. On August 5, 2026, the Supreme Court accredited Twala as an Electronic Notarization Facility, and on October 19, 2026, the Philippines' first two eNotarized documents were notarized on Twala. Twala is also integrated with the eGovPH Super App, bringing eNotarization to a platform already used by millions of Filipinos. These milestones reflect Twala's ongoing commitment to modernizing legal systems and improving access to trusted digital services in the country.

Twala's recognitions

Twala's innovations have earned national and international acclaim, including:

- **Supreme Court-accredited Electronic Notarization Facility** – Accredited on August 5, 2026 under the 2025 Rules on Electronic Notarization (A.M. No. 24-10-14-SC), one of the first three facilities accredited
- **The Philippines' first two eNotarized documents** – Notarized on Twala on October 19, 2026, at the official launch of electronic notarization
- **Startup Grant Recipient** – Department of Science and Technology – Philippine Council for Industry, Energy and Emerging Technology Research and Development (DOST-PCIEERD)
- **Grand Champion** – La French Tech Startup Competition 2022, supported by the French Chamber of Commerce and Industry
- **Top 3 – Ideaspace Startup Acceleration Program** – Recognized for outstanding innovation and potential in one of the Philippines' premier tech acceleration programs
- **Top LegalTech Startup** – Featured by multiple innovation forums and industry publications
- **Esquire Philippines 2024 Trailblazers List** – Recognized for its leadership in secure digital transformation and contributions to national legal innovation
- **Ease of Doing Business Champion of 2024** – Awarded by the Anti-Red Tape Authority (ARTA) for its pivotal role in enabling digital trust services that promote regulatory efficiency and innovation in public service
- **Cloud Signature Consortium Member** – Participates in global standard-setting for cloud-based digital signatures

- **Trusted Partner of the Supreme Court and other government agencies** for digital identity, e-signature, and e-notarization reform
- **Selected LegalTech Exhibitor** – Featured at SAASCON PH, Philippine Startup Week Top 100 Startups, and Singapore Echelon 100

These recognitions affirm Twala's position as a leading force in legal innovation, digital identity, and secure electronic transactions—both in the Philippines and across the broader legal tech landscape.

Twala as an Electronic Notarization Facility (ENF)

Twala is an Electronic Notarization Facility (ENF) accredited by the Supreme Court on August 5, 2026 under the 2025 Rules on Electronic Notarization. As defined under the Rules, an ENF is a secure, standards-based system that enables Electronic Notaries Public (ENPs) to perform notarial acts electronically—either in person or remotely—while ensuring authenticity, reliability, and legal enforceability.

Twala's platform provides all the core components of a compliant ENF, including:

- Support for In-Person Electronic Notarization (IEN) and Remote Electronic Notarization (REN)
- Real-time identity verification through biometrics, facial recognition, e-KYC, and multi-factor authentication
- Integration of secure electronic signatures and digital signatures backed by cryptographic standards
- Generation of electronic notarial records, audit trails, and video logs in accordance with the Rules
- Secure document handling using HashOrigin™ tamper-evident sealing and blockchain anchoring, and long-term archiving standards
- Access through the eGovPH Super App, bringing eNotarization to a platform already used by millions of Filipinos

Twala is also integrated with global digital signature ecosystems, including the Cloud Signature Consortium (CSC) and the Adobe Approved Trust List (AATL), allowing users to execute and verify trusted digital signatures that are interoperable across platforms and jurisdictions.

By aligning with both Philippine regulatory standards and international best practices, Twala is leading the digital transformation of notarial and legal services—bridging the gap between legal tradition and technological innovation.

■ CONTACT

Published by Twala, 12th Floor, The Trade & Financial Tower, Unit 1206, 32nd Street, 7th Avenue, Bonifacio Global City, Taguig City 1634, Metro Manila, Philippines. Email info@twala.ai or visit twala.ai.

Book a demo, explore pricing, or verify a Twala document at twala.ai. Technical details of HashOrigin™ are at hashorigin.io.

This white paper is provided for general information only and does not constitute legal advice. Twala is a technology provider; notarial acts are performed by commissioned Electronic Notaries Public. HashOrigin™ is a trademark of Ohelio Inc. Other names are the property of their respective owners. Twala © 2026.