



# Is Electronic Signature Legal in the Philippines?

**BLOCKCHAIN-POWERED ELECTRONIC SIGNATURE:  
THE KEY TO A FULLY-DIGITAL ECONOMY**

FAQ's on Legality of Electronic Signatures in the Philippines  
+ How Twala Complies with the Law  
+ Benefits of Using Electronic Signatures for Business

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



twala

Enabling trust for a frictionless digital future



# BLOCKCHAIN-POWERED ELECTRONIC SIGNATURE: THE KEY TO A FULLY-DIGITAL ECONOMY

FAQs on the Legality of Electronic Signatures in the Philippines

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

# **BLOCKCHAIN-POWERED ELECTRONIC SIGNATURES: THE KEY TO A FULLY-DIGITAL ECONOMY**

Atty. Herminio Bagro III, JD, MPA, Engr. Jeffrey Reyes, ECE, MTM, Atty. Emil Samaniego, JD  
*Email: [third.bagro@gmail.com](mailto:third.bagro@gmail.com), [jeffrey.reyes@twala.io](mailto:jeffrey.reyes@twala.io), [mr.emilsamaniego@gmail.com](mailto:mr.emilsamaniego@gmail.com)*

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.

Almost 25 years 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.

## **1. 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 document signing solution. It also outlines the current legal framework around electronic documents and signatures, how Twala complies with the applicable legal standards and the benefits of using electronic signatures.

## **2. Is an electronic signature the same as a digital signature?**

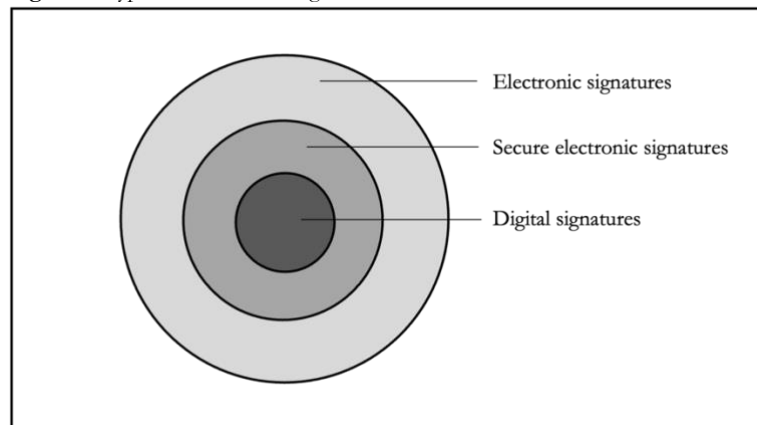
Although many people use the terms "electronic signature" and "digital signature" interchangeably, they are actually two distinct concepts. While a digital signature is a specific type of electronic signature, not all electronic signatures are digital signatures.

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



### Legal definitions to remember

- 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.<sup>i</sup>
- 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.<sup>ii</sup>
- A *digital signature*, 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.<sup>iii</sup>

### What distinguishes digital signatures?

The use of digital signatures presupposes the use of *asymmetric encryption*, also known as *public-key cryptography*. With this encryption, a message encrypted with someone's public key can only be deciphered by their private key, and vice versa. Asymmetric encryption solves the problem of sharing without secure communication by allowing parties to share their public keys and, using complex math, encrypt data so that an eavesdropper cannot decipher the message. Therefore, everyone can publicly share their public keys so that others can communicate with them securely.<sup>iv</sup>

There are many encryption systems used in asymmetric cryptography, such as ElGamal, digital signature algorithm (DSA), elliptic curve digital signature algorithm (ECDSA), Rivest-Shamir-Adleman (RSA), and public-Key cryptography standards (PKCS). The most popular and widely used asymmetric digital signature algorithm is the RSA, one of the first public-key cryptosystems. The RSA is widely used for secure data transmission on the web, particularly in Secure Socket Layer (SSL) and Transport Layer Security (TLS) protocols, which infuse web communications with integrity, security, and resilience against unauthorized tampering. RSA is the digital signature algorithm used by standard Public Key Infrastructure or PKI for X.509 digital certificates used in many internet protocols and also used in offline applications like electronic/digital signatures.

Since the introduction of SSL by Netscape in 1994, certificates for websites have typically used a public/private key pair based on the RSA algorithm. As the SSL specification evolved into TLS, support for different public key algorithms was added. One of these is the ECDSA, which provides a higher degree of security even with shorter key lengths, leading to efficiency in computing power. ECDSA became the digital signature scheme of choice for new cryptographic non-web applications, particularly in the finance industry -- most notably in blockchain technology. For example, every Bitcoin and Ethereum address is a cryptographic hash (like a digital fingerprint) of an ECDSA public key, where ownership is determined by who controls the ECDSA key.

As non-financial use for blockchain technology emerged, blockchain-based digital signatures that use ECDSA have been adopted by various applications in logistics, supply chains, digital identities, and document security.

### 3. What challenges do existing document signing systems such as PKI face?

Portable document format files (PDFs) were designed to easily share richly formatted documents with enterprises or individuals. It became an international standard in 2008 as Adobe and other companies added security features to PDFs.<sup>v</sup> These security features included password protection, digital signatures, and encryption.

Digital signatures were added to verify who created and encrypted a document. The most common standard used for this purpose is called X.509, which standard has become prevalent today, especially with the rise of remote work and online transactions.

However, the use of X.509 certificates in signing PDF documents also poses several challenges that need to be addressed:

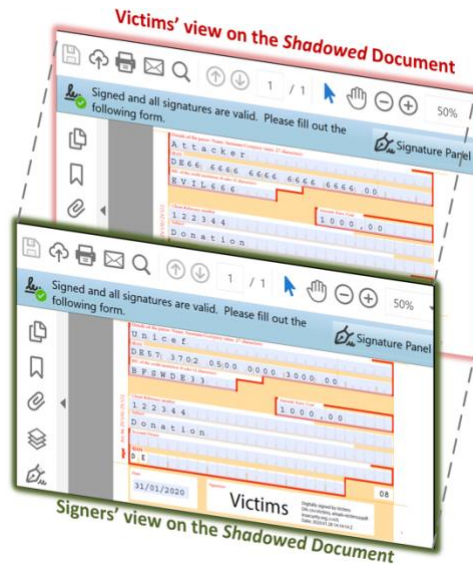
- *Trust.* Users need to ensure that the certificate they are using is valid, issued by a trusted certificate authority (CA), and has not been tampered with. Trust issues can also arise when a certificate is compromised or when a CA's root certificate is no longer trusted. This can lead to users losing confidence in the security of their signed documents.
- *Revocation of certificates.* When a certificate is compromised, lost, or revoked, the user must be notified immediately to prevent unauthorized access to their documents. However, revocation information is often not readily available, and the process of revoking a certificate can be complicated.
- *Key management.* The use of X.509 certificates requires proper key management to ensure that the private key is kept secure and confidential. Issues can arise when users forget their passwords or lose their private keys, leading to a loss of access to their signed documents.
- *Not compatible with other platforms.* Different software applications may have different requirements for digital signatures, making it difficult for users to sign documents across different platforms.
- *Hardware dependence.* X.509 certificates may also require specific hardware, such as smart cards or tokens, which can add to the cost and complexity of their use.
- *Costly digital certificates.* Obtaining individual digital certificates, particularly in the offline setting, poses a barrier to entry for some users. A privately issued digital certificate for document signing costs around \$300 to \$400 per individual per year.
- *Inefficient and not user-friendly.* PKI-certificate-based digital signatures only allow for sequential, one-at-a-time signing, as they are designed for offline signing. This means that each signer must wait for the previous signer to attach their digital signature before they can download and digitally sign the document, making parallel signing technically impossible. To illustrate, imagine a document that requires three signers. The first signer must sign the document on their laptop offline, and then send the digitally signed PDF to the second signer via email or another application. The second signer then needs to download the signed PDF, add their digital signature, and send it to the third signer. Finally, the third signer needs to download the document again and add their digital signature. As everything happens offline, the signers have no real-time status of the document, making it difficult to track.

- *Prone to security issues.* One of the recent issues with PKI technology is the PDF shadow attack. This attack exploits a vulnerability in the way PDF documents are structured and signed, allowing attackers to create a “shadow document” that looks like the original document but contains different content. The attacker can then use a legitimate digital signature to sign the shadow document, making it appear as if it is the original document. This can compromise the authenticity and integrity of electronically signed documents.

In February 2019, a team of security researchers from the Ruhr-University Bochum in Germany published details of vulnerabilities in the digital signing system of PDF viewers and online PDF digital signing services. They found that it is possible to change the document content and date/time stamp of a PDF document even after digitally signing and encrypting it, in a modus called the “Shadow Attack”<sup>vi</sup>.

Signed PDFs feature timestamps for when the file was created and updated. More often than not, signatures are added at the end of the document. The researchers found however that prior pages could be changed to reflect different content other than what the signer initially agreed to.

Figure 2. PDF Shadow Attack



With the evolution of technology, challenges in secure document signing have been addressed. Advancements in cloud computing, smartphone technology, and the widespread availability of the internet have made it easier to implement secure document signing. Among these technological solutions, blockchain stands out as a perfect fit for this use case.

#### 4. Why is blockchain useful for electronic documents and signatures?

Blockchain is a distributed ledger technology that provides a secure, decentralized way of recording and verifying transactions. It is a peer-to-peer network that enables the secure transfer of data without the need for intermediaries. Blockchain technology as a decentralized public key infrastructure (PKI) can help address the challenges associated with the use of X.509 digital certificates in document signing.

- *Trust and revocation issues solved.* One of the key benefits of using blockchain in signing PDF documents is that it eliminates the need for supposedly trusted intermediaries. This is possible because blockchain technology enables the creation of a tamper-proof, decentralized system where documents can be signed and verified without the need of X.509 digital certificates from a third party. This in turn provides a much higher level of security and eliminates process issues in determining whether the middleman-service provider can be trusted or not.

- *Digital banking-level key management.* With blockchain, private keys can be securely stored and accessed using custodial and non-custodial digital wallets. These digital wallets are protected by strong encryption and can be accessed using a password, passphrase, or biometric authentication, providing an additional layer of security.
- *Not hardware dependent.* Unlike PKI-based digital signatures that require a physical device to store and protect private keys, blockchain-based digital signatures use software algorithms to create and manage private keys. The private keys are securely stored in a distributed network, making it difficult for attackers to compromise them. This eliminates the need for expensive hardware devices, such as smart cards or tokens, and reduces the cost and complexity of using digital signatures.
- *Cost-effective.* Blockchain technology provides a transparent and decentralized system that enables secure and trustworthy digital signatures at a lower cost. Users can create and manage their own digital identities using public-key cryptography, eliminating the need to pay for expensive digital certificates. Users can sign documents on a blockchain without the need for costly hardware or software. This makes blockchain-based digital signatures accessible to a wider range of users, including individuals and small businesses.
- *Efficient and streamlined.* Another benefit of using blockchain in signing PDF documents is the ability to sign documents in parallel. With blockchain, multiple parties can sign a document simultaneously, reducing the time and effort required to sign a document. This provides a more efficient and streamlined signing process.
- *Secure and immune from shadow attacks.* Blockchain digital signatures are a type of digital signature that reside in the blockchain network, rather than in the object being signed, such as a PDF file. This key difference makes blockchain signatures more secure than traditional PKI-based signatures, as they are immune to shadow attacks. In a shadow attack, an attacker can create a malicious copy of a signed document and then replace the original with the forged copy, without altering the document's digital signature. However, with a blockchain-based signature, the signature resides on the blockchain network, making it extremely difficult for an attacker to modify the document without detection.

Furthermore, blockchain technology provides a decentralized, tamper-proof system for storing and verifying the authenticity and integrity of electronically signed documents. Each block in the chain is protected by a hash value, which acts as a digital fingerprint of the block's content. Any attempt to modify a block in the chain would change the hash value, rendering it invalid and alerting all network participants of the attempted tampering.

## 5. How does Twala use blockchain technology to secure electronic documents?

Twala is a digital signature solution that combines the above-mentioned benefits of blockchain technology and standard PKI technology to offer a more secure, privacy-preserving, and cost-efficient solution for document signing.

Twala uses a decentralized public key infrastructure technology to secure documents. This means that document files are hashed, encrypted with the signer's digital or secure electronic signature, built into a hash (Merkle) tree<sup>vii</sup>, and mirrored or encoded across all nodes in the network. This ensures that the records are not altered or lost, and everyone in the ecosystem can keep a copy of the common system of record, but *without* having access to a copy of the documents, signatures, or metadata.

To further enhance the security, reliability, and scalability of its service, Twala uses a hybrid blockchain approach. The documents and audit trails are initially stored in a layer 2/ sidechain, and then recorded onto the public blockchain using a proprietary blockchain anchoring technology. This ensures that the data is secured and stored efficiently, while also reducing the load on the public blockchain network.

To cater to customers who prefer traditional PKI-based digital signatures and seals, Twala also supports the [Cloud Signature Consortium](#) standards on top of its blockchain security. This is especially useful for jurisdictions that only recognize PKI-based signatures. Cloud Signature Consortium is a global organization dedicated to promoting the adoption of cloud-based electronic signatures. Twala is a member of the Cloud Signature Consortium.

Recognizing the value of Twala's technology, the Philippine Department of Science and Technology awarded Twala a P4.6M grant in 2022 through the DOST Startup Grant Fund program to help it advance its research and development in the areas of distributed ledger technology or blockchain with applications in digital signatures and digital identity.<sup>viii</sup> In addition to the funding, the Philippine's Advanced Science and Technology Institute, an

attached agency of the DOST, signed a partnership with Twala to accelerate its blockchain research and development.<sup>ix</sup>

**6. How exactly does Twala work?**

*Step 1: Create an account and verify identity*

Twala users can create an account by either (1) providing their name and verified email address and/ **or** (2) verifying their government-approved ID via Twala ID. This allows them to sign documents using a secure electronic signature or digital signature that can be accessed via their email, Twala web account, or Twala ID mobile app.

*Step 2: Upload document*

Users can upload to the platform the document they need to get signed either in PDF or Word format.

*Step 3: Add signers*

Users can add all those who need to sign the documents, and assign the sequence of signing if needed. The signers are then notified with a signing request on their Twala dashboard and in their registered emails.

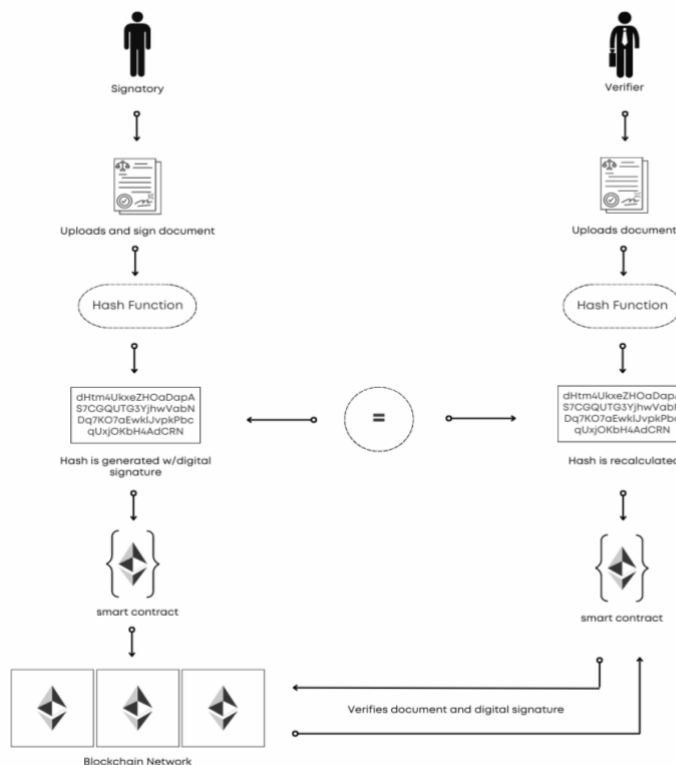
*Step 4: Sign*

Signers can create a signature by drawing, typing, or uploading an image of their handwritten signature. Every time a user signs a document, the document is first hashed using a secure cryptographic algorithm, creating a unique and irreversible fingerprint of the document. This hash is then signed using the user's private cryptographic key and/or business' digital seal. This process creates a digital signature unique to the user and the document. The completed transaction is then recorded on multiple blockchain networks, making an immutable and traceable record.

*Step 5: Verify*

Once the document is signed by all parties, a hash of the document is generated, encrypted with the signers' digital or secure electronic signatures, and recorded on the blockchain. Users can upload the signed document on Twala's verification page to check the document's authenticity. If the hash is the same as that of the hash generated at the time of signing, then the document will be validated. If the hash is not the same, it means that there was manipulation or alteration in the signed document. Alternatively, Twala users can verify the authenticity of their documents directly in the blockchain by using Twala's command line interface (CLI) verification system.

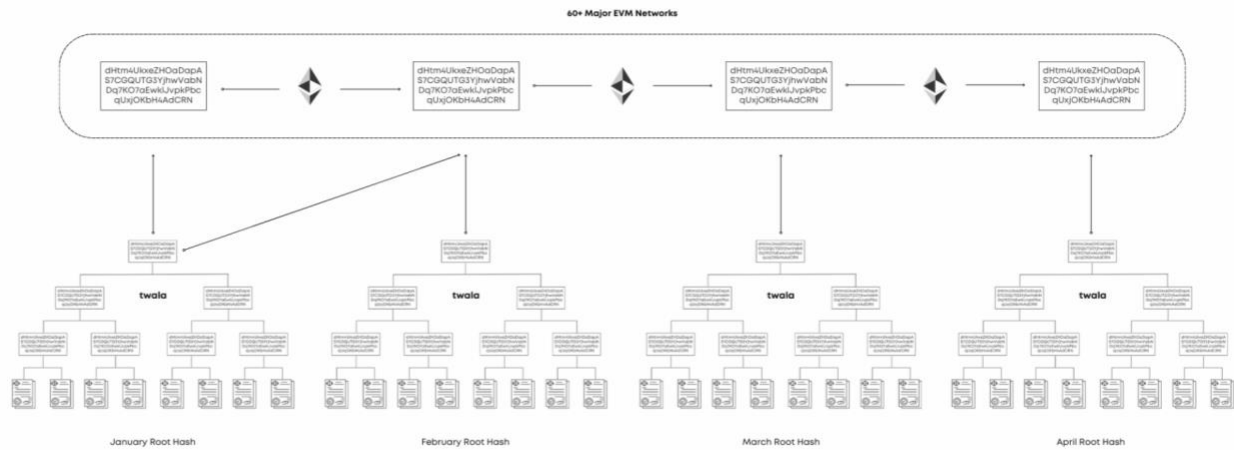
**Figure 3.** How Twalasin works





Twala is a hybrid blockchain solution that uses both private and public blockchains to secure documents. At the end of the month, all documents signed within Twala are consolidated through a Merkle Tree and the root hash is then anchored to Ethereum MainNet plus 60 other major blockchain networks. Every root hash is chained with the end objective of making it more difficult to alter any record as the chain continues.

Figure 4. Twala Chained Anchoring Technology



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

**Yes.** Twala uses technology, standards, and processes that comply with the laws and rules governing electronic documents and digital and secure electronic signatures in the Philippines. Twala is also designed to comply with e-signature laws in most jurisdictions globally such as the Electronic Signatures in Global and National Commerce Act (ESIGN) in the United States, the eIDAS (electronic IDentification, Authentication and trust Services) Regulation in the European Union, and the Electronic Transactions Act (ETA) in Singapore.

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 was made applicable 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 level of authenticity than what was provided under the UNCITRAL Model Law on Electronic Commerce.<sup>x</sup> 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:

<i>Requirements to Attain Functional Equivalence</i>		<i>How Twala Implements Requirement</i>
1	Integrity is maintained	Twala uses decentralized public key infrastructure powered by distributed ledger technology (DLT) or blockchain that uses an international standard in cryptographic technology (ECDSA) to make electronic documents tamper-proof.
2	Reliability is maintained	<p>Twala adheres to international standards and best practices in information security and data privacy to ensure the reliability of its system. These include:</p> <p><i>Web Application</i></p> <ul style="list-style-type: none"> <li>● Strict password requirements for user accounts</li> <li>● Opt-in secure login using self-sovereign digital identity (Twala ID) for multi-factor authentication</li> <li>● Web Application Firewall (WAF) policy to protect the web and server applications from known vulnerabilities such as OWASP Top 10 vulnerabilities and attacks</li> <li>● Regular vulnerability assessments and penetration testing (VAPT) to identify and remediate potential security weaknesses</li> <li>● Proper network segmentation for private and public-facing applications as well as development and production environment</li> <li>● Daily database and object storage encryption and backup</li> <li>● 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</li> <li>● Use of code analysis or Static Application Security Testing (SAST) tools such as Sonarqube and Snyk to ensure code-level security and up-to-date security</li> <li>● Proactive adoption of industry best practices and guidelines</li> <li>● Branch policies used for source control management, where the main branch is protected and code reviews, quality gates, and security gates are required</li> </ul>

		<p><i>Mobile Security Standards</i></p> <ul style="list-style-type: none"> <li>• Use of PIN delegation and opt-in biometrics features, such as fingerprint and Face ID, for multi-factor authentication and transaction validation</li> <li>• Encrypted local data storage on device, where secure key management systems such as EncryptedSharedPreferences for Android and KeyChain for IOS are used</li> <li>• Use of code obfuscation techniques to make it difficult for attackers to reverse engineer the app, extract sensitive information, or exploit vulnerabilities</li> <li>• Use of Firebase AppCheck 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</li> </ul>
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	<p>When a user signs a document in Twala, the document is first hashed using a secure cryptographic algorithm, creating a unique and irreversible fingerprint of the document. This hash is then signed using the user's private cryptographic key, which is securely stored on Twala's servers or the user's device. This process creates a digital signature that is unique to the user and the document. This transaction is then recorded in a blockchain network, ensuring that the document is complete, unalterable, and tamper-proof.</p> <p>In the case of secure electronic signatures, the document hash is signed by Twala's private key and/or the business' private key (digital seal).</p>
3.b	Document is reliable in light of the purpose for which it was generated and in the light of all relevant circumstances.	<p>Twala uses an internationally accepted digital signature algorithm standard used in digital signatures, smart contracts, and digital currencies around the world.</p> <p>This standard, called Elliptical Curve Digital Signature Algorithm (ECDSA) has been adopted by global standardization bodies such as:</p> <ul style="list-style-type: none"> <li>• The International Standards Organization (ISO 14888-3)<sup>xi</sup></li> <li>• The American National Standards Institute (ANSI X9.62)<sup>xii</sup></li> <li>• Accredited Standards Committee X9 Inc. (ECDSA. X9.142)<sup>xiii</sup></li> <li>• The Institute of Electrical and Electronic Engineers (IEEE 1363-2000)<sup>xiv</sup> and</li> <li>• The US Department of Commerce's Federal Information Processing Standards Publication (FIPS 186-4 and 186-5)<sup>xv</sup></li> </ul> <p>ECDSA is the digital signature algorithm used by the Twala Network, Ethereum, and Bitcoin blockchains to digitally sign transactions made in their network.</p> <p>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.</p> <p>Twala is also compatible with PKI-based digital signatures and seals based on the X.509 standard used by the Cloud Signature Consortium, an EU-based global organization that advocates for cloud-based electronic and digital signature standards. Twala is a member of this Consortium.</p>

<i>Requirements to Attain Functional Equivalence</i>		<i>How Twala Implements Requirement</i>
1	A prescribed procedure exists which is not alterable by the parties interested in the electronic document, under which:	<p>When a user signs a document in Twala, the document is first hashed using a secure cryptographic algorithm, creating a unique and irreversible fingerprint of the document. This hash is then signed using the user's private cryptographic key, which is securely stored on Twala's servers or the user's device. This process creates a digital signature that is unique to the user and the document. This transaction is then recorded in a blockchain network, ensuring that the document is complete, unalterable, and tamper-proof.</p> <p>In the case of secure electronic signatures, the document hash is signed by Twala's private key and/or the business' private key (digital seal).</p> <p>For signers using PKI-based signatures to secure their documents, Twala also has the capacity to integrate these on top of the DLT-based digital signature, while maintaining the above level of security.</p>

1.a	<p>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</p>	<p>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:</p> <ul style="list-style-type: none"> <li>● Email verification including via e-mail OTP, Open Authentication (OAuth), Single Sign On (SSO), and Active Directory (AD) standards</li> <li>● Mobile number verification via SMS One Time PIN (OTP)</li> <li>● Government-issued ID verification complemented by:                             <ul style="list-style-type: none"> <li>○ Optical character recognition (OCR) technology</li> <li>○ Facial/ biometric recognition technology</li> <li>○ Liveness test powered by artificial intelligence</li> <li>○ Manual verification</li> </ul> </li> </ul> <p>Only verified users will be given a Twala account and cryptographic key pairs to have access to the electronic document.</p> <p>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 Sign web page or TwalaID app) using their password or their phone’s biometric or facial authentication procedure.</p>
1.b	<p>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</p>	<p>Twala uses an internationally accepted digital signature algorithm standard used in digital signatures, smart contracts, and digital currencies around the world.</p> <p>This standard, called Elliptical Curve Digital Signature Algorithm (ECDSA) has been adopted by global standardization bodies such as:</p> <ul style="list-style-type: none"> <li>● The International Standards Organization (ISO 14888-3)</li> <li>● The American National Standards Institute (ANSI X9.62)</li> <li>● The Institute of Electrical and Electronic Engineers (IEEE 1363-2000), and</li> <li>● The US Department of Commerce’s Federal Information Processing Standards Publication (FIPS 186-2) (<i>Citations on Table 1</i>)</li> </ul> <p>ECDSA is the digital signature algorithm used by the Twala Network, Ethereum, and Bitcoin blockchains to digitally sign transactions made in their network.</p> <p>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.</p> <p>Twala is also compatible with PKI-based digital signatures and seals based on the X.509 standard used by the Cloud Signature Consortium, an EU-based global organization that advocates for cloud-based electronic and digital signature standards. Twala is a member of this Consortium.</p>
1.c	<p>The signer executes or provides the electronic signature in order to proceed further with the transaction, and</p>	<p>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:</p> <ul style="list-style-type: none"> <li>● 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;</li> <li>● Once the signer is satisfied, s/he must click on the “submit signature” button to create and attach his/her digital signature to the document.</li> </ul> <p>Twala deploys several layers of security to ensure that only verified users have access to their accounts and the digital signature creation device to sign electronic documents. These include but are not limited to:</p> <ul style="list-style-type: none"> <li>● Device PIN or Patterns</li> <li>● Device Biometric Key – Fingerprint</li> <li>● Device Biometric Key – Facial ID</li> <li>● Identity App – PIN</li> <li>● Email OTP or token</li> <li>● SMS OTP or token</li> <li>● Password</li> </ul> <p>Twala’s digital identity also complies with internal standards on authentication/digital ID such as Fast Identity Online (FIDO2)<sup>xvi</sup>, World Wide Web Consortium (W3C)<sup>xvii</sup> and the US National Institute of Standards and Technology Special Publication (NIST SP) 800-63<sup>xviii</sup>.</p>

1.d	The other party is authorized and enabled to verify the electronic signature and make the decision to proceed with the transaction authenticated by the same.	To verify the document, Twala uses public key cryptography to ensure that the digital signature is valid. The signature is decrypted using the signer’s public key, which is available to anyone who wants to verify the signature. If the decrypted signature matches the document’s hash, the signature is considered valid, and the document is verified. Twala Sign then anchors the hash of the signed document into an Ethereum smart contract, creating an immutable record of the document’s existence and integrity. This ensures that 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.”<sup>xxix</sup> 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.”<sup>xxx</sup>

However, while a particular piece of electronic document or signature may be admissible as evidence, actually presenting it to a judge to be considered in deciding a case requires compliance with the Rules of Court<sup>xxxi</sup>, issued by the Philippine Supreme Court<sup>xxxii</sup>, 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 Evidence<sup>xxxiii</sup> (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 criminal<sup>xxxiv</sup> and civil actions and proceedings, as well as quasi-judicial and administrative cases.<sup>xxxv</sup>

Under the Rules of Court, a document can only be presented in court as evidence, if (1) it is an original copy<sup>xxxvi</sup> and, (2) for private<sup>xxxvii</sup> documents, its due execution and authenticity is proven.<sup>xxxviii</sup> 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.<sup>xxxix</sup>

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

<i>Requirements</i>	<i>How Twala Addresses the Requirement</i>
1	<p><u>Must be an original copy.</u> 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)</p> <p>When a user signs a document in Twala, the document is first hashed using a secure cryptographic algorithm, creating a unique and irreversible fingerprint of the document. This hash is then signed using the user’s private cryptographic key, which is securely stored on Twala’s servers or the user’s device. This process creates a digital signature that is unique to the user and the document. This transaction is then recorded in multiple blockchain networks, ensuring that the original document is complete, unalterable, and tamper-proof.</p> <p>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:</p> <ol style="list-style-type: none"> <li>1. Name of the signer/s</li> <li>2. The digital ID of the signer/s</li> <li>3. Email of the signer/s</li> </ol>

		<p>4. ID information such as type of ID and ID number if required by the document owner</p> <p>5. Digital timestamp of transactions related to the document/s (e.g. when the document has been sent, viewed, and signed).</p> <p>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.</p>
1.b	<p><u>Duplicate originals allowed.</u> 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 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)</p>	<p>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.</p> <p>But these too fall squarely within the definition of duplicate originals under this Section, as these documents are executed at the same time with identical contents.</p> <p>Either way, the legal effect is the same – that these electronic documents are all regarded as original.</p>
2	<p><u>Document must be authenticated.</u> Before any <b>private electronic document</b> offered as authentic is received in evidence, its authenticity must be proved by <i>any</i> of the following means:</p> <ul style="list-style-type: none"> <li>a. by evidence that it had been <i>digitally signed</i> by the person purported to have signed the same;</li> <li>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; <b>or</b></li> <li>c. by other evidence showing its integrity and reliability to the satisfaction of the Judge. (Rule 5, Section 2)</li> </ul>	<p>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 lists the data of the signers -- their digital ID, e-mail, mobile number, ID submitted during the sign-up process, IP address, geolocation, and digital timestamp.</p> <p>Twala’s electronic signature complies with the standards provided by the rules:</p> <ul style="list-style-type: none"> <li>o Its <i>digital signature</i><sup>xxx</sup> uses a public cryptosystem that ensures the transformation of the electronic document can be done only by using the signer’s private key that corresponds to his/her public key. 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 verification page, or directly through the blockchain by using Twala’s command line interface (CLI) verification system.</li> <li>o Its <i>secure electronic signature</i><sup>xxxi</sup> uses the same blockchain technology, identification and security procedures, and verification processes as the digital signature, except that the signer is not assigned a private key, a cryptographic digital seal is used instead. 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.</li> </ul>
3	<p><u>Signature must be authenticated.</u> An electronic signature may be authenticated in any of the following manner:</p> <ul style="list-style-type: none"> <li>a. By evidence that <i>a method or process was utilized to establish a digital signature and verify the same</i>;</li> <li>b. By any other means provided by law; <b>or</b></li> <li>c. By any other means satisfactory to the judge as establishing the genuineness of the electronic signature. (Rule 6, Section 2)</li> </ul>	<p>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:</p> <ul style="list-style-type: none"> <li>- A Twala-signed document includes a statement that it has been digitally or securely e-signed, and an electronic audit trail that lists the data of the signers -- their digital ID, e-mail, mobile number, ID submitted during the sign-up process, IP address, geolocation, and digital timestamp.</li> <li>- 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 verification page, or directly through the blockchain by using Twala’s command line interface (CLI) verification system. This provides a way to satisfactorily establish the genuineness of the electronic signature used.</li> <li>- For documents securely e-signed using Twala, we refer to Section 11<sup>xxxii</sup> of the ECA, which identifies the means to authenticate</li> </ul>

		electronic documents and electronic signatures. As mentioned above, secure electronic signature uses the same blockchain technology, identification and security procedures, and verification processes as the digital signature, except that the signer is not assigned a private key. A cryptographic digital seal is used instead. 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	<u>When authentication is not required.</u> A document electronically notarized in accordance with the rules promulgated by the SC shall be considered as a <b>public document</b> and proved as a notarial document under the Rules of Court. (Rule 5, Section 3)	The Supreme Court has yet to operationalize electronic notarization.  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.” <sup>xxxiii</sup>

Finally, the REE provides the method of proving electronic documents in court, i.e. through an affidavit of evidence<sup>xxxiv</sup>, presumably by a technical or IT personnel who is familiar with the procedure involved in preparing and signing the electronic document to be presented. In a recent case<sup>xxxv</sup>, the Supreme Court emphasized the importance of this requirement.

After an electronic document is presented, authenticated, and proven 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.<sup>xxxvi</sup> 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 certificate<sup>xxxvii</sup> or digital ID, as well as the reliability of the message associated with the digital signature, among others.

Upon authentication, it shall be presumed that: (Rule 6, Sections 3-4)		Electronic Signature <sup>xxxviii</sup>	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		✓

**8. Are electronic signature providers required to be accredited as such by any government agency?**

**No.** According to the ECA’s implementing rules and regulations issued by the Departments of Trade and Industry and Science and Technology,<sup>xxxix</sup> accreditation is voluntary. So long as information certifiers<sup>xl</sup> (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 authority<sup>xli</sup> has been accredited by the government from among the existing private electronic signature providers, both foreign and domestic.

## 9. 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.<sup>xlii</sup> 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 (SOC 1 Type II, SOC 2 Type I, and ISO 27001 - \*AWS Data Centers).
- *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 DICT-accredited 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 such as Sonarqube and Snyk 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 secure key management systems such as EncryptedSharedPreferences for Android and KeyChain for 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 Firebase AppCheck 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.

#### 10. 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)<sup>xliii</sup>, and the Philippines' Data Privacy Act of 2012<sup>xliiv</sup>. 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.

#### 11. 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.<sup>xlv</sup> In 2021, the Commission on Audit released the Guidelines on the Use of Electronic Documents, Electronic Signatures, and Digital Signatures in Government Transactions.<sup>xlvi</sup> 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."<sup>xlvii</sup>

The COA circular allows a government agency to use electronic signatures, secure electronic signatures, digital signatures, or a combination,<sup>xlviii</sup> 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."<sup>xlix</sup>

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 Department of Information and Communication Technology (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 signatures) (IV.D)*
  - When the officer opts to use an electronic signature other than a digital signature on an electronic document, the signed electronic document may be validly accepted provided the agency is able to establish that:
    - a. the electronic signature is that of the person to whom it correlates;
    - b. 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;
    - c. the methods or processes utilized to affix or verify the electronic signature, if any, operated without error or fault; and
    - d. the person whose e-signature was affixed, takes responsibility and assumes accountability that the document remained unchanged until it was submitted to the auditor.

## 12. Is blockchain technology recognized in practice 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.

- Electronic signature companies in the US, EU, and other countries are using blockchain-based signatures.
- China has implemented blockchain technology in its e-notary system<sup>i</sup>, and the European Union and South Korea plan to launch blockchain-powered services by 2024<sup>ii</sup>.
- The Archangel project is a research initiative funded by the EPSRC<sup>iii</sup> in the UK to investigate the use of blockchain technology for the digital preservation and archiving of cultural heritage.<sup>iii</sup>
- The entire European Union is transitioning PKI-based trust service providers to blockchain via the EIDAS Bridge for digital signature and other use cases.<sup>iv</sup>
- The EU accredited the world’s first blockchain-based trust services provider (TSP) in 2020, via the EU Trust List.<sup>v</sup>
- Estonia uses blockchain technology to enforce the integrity of government data and systems including the use of blockchain-based digital signatures.<sup>vi</sup>
- The Philippines has recognized blockchain technology through various initiatives such as:

- the Bangko Sentral ng Pilipinas’ Pioneer Regulatory Framework for Virtual Currency Exchanges,<sup>lvii</sup>
- the Securities and Exchange Commission’s Draft of Digital Asset Exchange,<sup>lviii</sup>
- The charter of the Bataan freeport zone<sup>lix</sup> introduced the term “cryptocurrency,” the underlying value of which is blockchain technology,
- the Cagayan economic zone’s “Crypto Valley of Asia” initiative<sup>lx</sup>,
- Union Bank’s project i2i<sup>lxi</sup>, and the Philippine Bureau of the Treasury’s application for the distribution of government bonds enabled by blockchain technology<sup>lxii</sup>,
- the Department of Information and Communications Technology spearheading a national blockchain summit in Bataan<sup>lxiii</sup>, and lastly,
- the Department of Science and Technology training their researchers in blockchain technology.<sup>lxiv</sup>

**13. What are the benefits of using electronic signatures for your business?**

Electronic signatures have become increasingly popular in recent years as more and more businesses are switching to digital processes. The use of electronic signatures has many benefits that make them a more convenient and efficient way to sign documents. Here are some of the benefits of using electronic signatures:

**Convenience:** One of the primary benefits of electronic signatures is their convenience. With electronic signatures, you can sign documents from anywhere, at any time, without the need for physical paperwork. This means you can sign contracts, agreements, and other documents without having to be in the same location as the other party.

**Efficiency and Scalability:** Electronic signatures are also more efficient than traditional paper signatures. They eliminate the need for printing, mailing, and manually signing documents, which can take a lot of time and resources. With electronic signatures, the signing process can be completed in a matter of minutes, saving you time and increasing productivity.

**Security and Risk Reduction:** Electronic signatures are also more secure than traditional signatures. They can be encrypted, password protected, and tracked, providing an extra layer of security to your documents. Additionally, electronic signatures can help prevent fraud, as they can be verified using various authentication methods.

**Cost-effective:** Electronic signatures are a cost-effective solution for signing documents. They eliminate the need for paper, ink, printing, and mailing, reducing the overall cost of the signing process. This makes them an ideal solution for businesses of all sizes, from small startups to large corporations.

**Environmentally friendly:** Electronic signatures are a more environmentally friendly option than traditional signatures. They reduce the amount of paper waste and carbon emissions associated with printing, mailing, and storing physical documents.

Electronic signatures are a convenient, efficient, secure, cost-effective, and environmentally friendly way to sign documents. As more businesses adopt digital processes, electronic signatures will continue to become more prevalent and replace traditional signatures as the preferred way of signing documents.

**Conclusion**

Blockchain-based electronic signatures are an essential building block for a fully digital economy. They provide a tamper-proof and secure method for signing and authenticating digital documents, making them legally binding and court-admissible. Twala’s platform offers a reliable, secure, and legal solution for individuals, businesses, and government agencies to digitize their processes, allowing them to take advantage of the high levels of security and transparency that blockchain technology provides.

Moreover, Twala’s platform offers end-to-end document management -- from preparation, routing, signing, tracking, storage, and archiving -- so that workflows are further streamlined, costs are reduced, and efficiencies are achieved.

As more businesses adopt blockchain-based electronic signatures, we can expect to see a transformation toward a society less reliant on paper. This transformation has far-reaching benefits that have the potential to unlock

enormous economic value, help achieve our environmental goals, and revolutionize the way we transact with each other, making it easier, faster, more transparent, and more secure -- a frictionless digital future.

---

### ***About the Authors***

#### **Atty. Herminio Bagro III, JD, MPA**

Atty. Third Bagro has served the public sector for 13 years across three governments.

He began his career in service as a student leader in high school, until he was elected University of the Philippines Student Council Chairperson in 2008 during the University's centennial. As a law student, he worked as a legal assistant at the National Labor Relations Commission. While waiting for the bar examination results, he joined the team of former Senator MAR Roxas as legislative staff. After placing 8th in the 2009 bar exams, he joined the government under the late President Benigno S. Aquino III, first as Director and later as Undersecretary and Deputy Head to Presidential Management Staff Secretary Julia R. Abad. In 2016, he returned to the legislative branch, serving as chief-of-staff and counsel to three-term Senator Francis N. Pangilinan. Most recently, he served as Undersecretary and legal counsel to Department of Trade and Industry Secretary Alfredo E. Pascual.

Third Bagro graduated from UP with degrees in Philosophy, cum laude, and Juris Doctor. He obtained his Master's in Public Administration from the Maxwell School of Citizenship and Public Affairs in New York State as a Fulbright scholar. He co-founded Twala, a technology startup offering digital solutions for secure electronic signing and notarization. He also teaches part-time at the UP College of Law.

#### **Engr. Jeffrey V. Reyes, ECE, MTM**

Jeffrey Reyes is currently the Chief Executive Officer of Twala, a digital identity and digital signature solutions company supported by the Department of Science and Technology through the Startup Grant Fund Program. Jeffrey has more than 13 years of IT experience in systems and software development and have worked for global companies in the Philippines, the United States, Singapore, and the European Union. He also served as an IT consultant to the Philippine Consulate in Dublin, Ireland.

He is a licensed electronics and communications engineer and a member of Institute of Electronics Engineers of the Philippines (IECEP). He obtained his Master's in Technology Management from UP Diliman and his Bachelor of Science in Electronics and Communications Engineering degree from PUP - Manila. His technology research interests are in the fields of distributed ledger technology, digital signature, digital identity, cryptography and advanced authentication technologies.

#### **Atty. Emil Samaniego, JD**

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.

<sup>i</sup> Republic Act No. 8792, Electronic Commerce Act, Section 5(5)(e).

<sup>ii</sup> DTI-DOST Joint Department Administrative Order No. 2-2001, Sec. 3(p).

<sup>iii</sup> Supreme Court Rules on Electronic Evidence (SC REE), Sec. 1(e), and DTI-DOST Joint Department Administrative Order No. 2-2001, Sec. 3(d).

<sup>iv</sup> Thomas W. Edgar, David O. Manz, in Research Methods for Cyber Security, 2017.

<sup>v</sup> Adobe Systems Incorporated (November 2006). "PDF Reference" (PDF). 1.7 (6th ed.). Archived from the original (PDF) on October 1, 2008. Retrieved January 12, 2023.

<sup>vi</sup> Attacks on PDF Signatures, <https://pdf-insecurity.org/signature/shadow-attacks.html>.

<sup>vii</sup> In cryptography and computer science, a hash tree or Merkle tree is a tree in which every "leaf" (node) is labelled with the cryptographic hash of a data block, and every node that is not a leaf (called a branch, inner node, or inode) is labelled with the cryptographic hash of the labels of its child nodes. A hash tree allows efficient and secure verification of the contents of a large data structure.

<sup>viii</sup> DoST grants funding to blockchain startup Twala for its digital signature innovation, The Manila Times, <https://www.manilatimes.net/2022/08/10/public-square/dost-grants-funding-to-blockchain-startup-twala-for-its-digital-signature-innovation/1854114>

<sup>ix</sup> DOST-ASTI CSD signs MOU w/ Partners to support, promote IoT, Blockchain, AI Tech, <https://asti.dost.gov.ph/communications/dost-asti-csd-signs-mou-w-partners-to-support-promote-iot-blockchain-ai-tech/>

<sup>x</sup> 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.

<sup>xi</sup> ISO/IEC 14888-3:2018 -IT Security techniques — Digital signatures at <https://www.iso.org/standard/76382.html>.

<sup>xii</sup> 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>.

<sup>xiii</sup> ASC X9 Issues New Standard for Public Key Cryptography/ECDSA at <https://x9.org/asc-x9-issues-new-standard-for-public-key-cryptography-ecdsa/>.

<sup>xiv</sup> 1363-2000 - IEEE Standard Specifications for Public-Key Cryptography at <https://ieeexplore.ieee.org/document/891000>.

<sup>xv</sup> FIPS 186-5 - Digital Signature Standard (DSS) at <https://csrc.nist.gov/publications/detail/fips/186/5/final>.

<sup>xvi</sup> 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/>.

<sup>xvii</sup> The World Wide Web Consortium is the main international standards organization for the World Wide Web. See <https://www.w3.org/>.

<sup>xviii</sup> US National Institute of Standards and Technology - Digital Identity Guidelines. See <https://pages.nist.gov/800-63-3/>.

<sup>xix</sup> Section 7, penultimate paragraph.

<sup>xx</sup> Section 12.

<sup>xxi</sup> The 1997 Rules of Civil Procedure As Amended, (April 8, 1997).

<sup>xxii</sup> 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.

<sup>xxiii</sup> Administrative Matter No. 01-7-01-SC.

<sup>xxiv</sup> 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])

<sup>xxv</sup> REE, Rule 1, Section 1.

<sup>xxvi</sup> 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.)

<sup>xxvii</sup> 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."

<sup>xxviii</sup> Rules of Court, Rule 132 (B) Section 20.

<sup>xxix</sup> REE, Rule 5, Section 1.

<sup>xxx</sup> 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.

<sup>xxxi</sup> 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. (DTI-DOST Joint Department Administrative Order No. 2-2001, Sec. 3[p])

<sup>xxxii</sup> "[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."

<sup>xxxiii</sup> Section 11, paragraph 3, RA 8792.

<sup>xxxiv</sup> Rule 9, Section 1.

<sup>xxxv</sup> RCBC Bankard Services Corp. v. Oracion, Jr., G.R. No. 223274, (June 19, 2019)

<sup>xxxvi</sup> Rules of Court Rule 131, Section 3.

<sup>xxxvii</sup> “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.

<sup>xxxviii</sup> Includes secure electronic signatures.

<sup>xxxix</sup> 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.

<sup>xl</sup> 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.*)

<sup>xli</sup> “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.*)

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

<sup>xliii</sup> The General Data Protection Regulation (GDPR) is the European Union’s privacy and security law, <https://gdpr.eu/what-is-gdpr/>

<sup>xliv</sup> 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.

<sup>xlv</sup> Section 3, ECA.

<sup>xlvi</sup> COA Circular 2021-006, dated September 6, 2021. See [https://coa.gov.ph/wpfd\\_file/coa-circular-no-2021-006-september-6-2021/](https://coa.gov.ph/wpfd_file/coa-circular-no-2021-006-september-6-2021/).

<sup>xlvii</sup> Rule II, Scope and Coverage, *id.*

<sup>xlviii</sup> Note 3 of Annex A, *id.*

<sup>xlix</sup> Rule IV.A.2, *id.*

<sup>l</sup> Notary office in Shanghai applies blockchain technology with success, [http://en.moj.gov.cn/2020-11/04/c\\_560984.htm](http://en.moj.gov.cn/2020-11/04/c_560984.htm)

<sup>li</sup> 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>

<sup>lii</sup> 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.

<sup>liii</sup> ARCHANGEL - Trusted Archives of Digital Public Records, <https://www.archangel.ac.uk/>

<sup>liiv</sup> About SSI eIDAS Bridge, <https://joinup.ec.europa.eu/collection/ssi-eidas-bridge/about>

<sup>liv</sup> 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>

<sup>lvi</sup> Estonian blockchain technology, <https://e-estonia.com/solutions/cyber-security/ksi-blockchain/>

<sup>lvii</sup> Circular No. 1108 - Bangko Sentral ng Pilipinas, <https://www.bsp.gov.ph/Regulations/Issuances/2021/1108.pdf>

<sup>lviii</sup> 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/>

<sup>lix</sup> 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.

<sup>lx</sup> CEZA host blockchain, fintech webinar, <https://ceza.gov.ph/ceza-hosts-blockchain-fintech-webinar/>.

<sup>lxi</sup> 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>

<sup>lxii</sup> 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>


<sup>lxiii</sup> The promise of blockchain, <https://mb.com.ph/2022/11/01/the-promise-of-blockchain/>

<sup>lxiv</sup> 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>

# twala

 [www.twala.io](http://www.twala.io)

 [info@twala.io](mailto:info@twala.io)

 12th floor The Trade and Financial Tower  
32nd St. Cor. 7th Avenue, Bonifacio Global City  
Taguig, Philippines 1634

 DEPARTMENT OF SCIENCE  
& TECHNOLOGY  
Supported by

 CLOUD  
SIGNATURE  
CONSORTIUM  
Member