Validity and Enforceability of Electronic and Digital Signatures

This legal brief examines the legal validity, enforceability, and practical recognition of electronic and digital signatures in Cambodia, with particular focus on the E-Commerce Law, Sub-Decree No. 246, and applicable technology and cybersecurity requirements in the banking and financial sector. It also considers key limitations on the use of electronic signatures, cloud-based signature arrangements, data residency issues, and current market and regulatory practice.

1. Summary

The Royal Government of Cambodia has issued the Sub-Decree No. 246 on Digital Signatures dated 27 December 2017 (“**Sub-Decree No. 246**”), which governs the use of digital signatures. Later in 2019, a new Law on Electronic Commerce (“**E-Commerce Law**”) was introduced, which includes provisions governing the legality and use of e-signatures, including digital signatures, in Cambodia.

Digital Signature and Electronic Signature are not completely distinguished from each other under the laws. Sub-Decree No. 246 defines “digital signature” as “any data attached to the electronic message certifying the digital signatory and verifying the authentication of such electronic message signed by the digital signatory”.

Whereas the E-Commerce Law generally defines “electronic signature” as “any signatures created by electronic means to identify the signatory, which includes digital signatures, biomass signatures, and other signatures”. Therefore, it can be interpreted that generally, an e-signature is regarded as a normal and ordinary electronic signature, and a digital signature is a category of the e-signature, rather than a completely different tool.

While electronic and digital signatures are generally recognised under Cambodian law, additional requirements apply in the banking and financial sector. The National Bank of Cambodia issued Technology and Cyber Risk Management Guidelines in 2026 (“**TCRMG**”) that require banking and financial institutions to implement security measures such as two-factor authentication (2FA), one-time passwords (OTP), and other cybersecurity controls when providing digital services. These measures are intended to help verify users' identities, protect online transactions, and enhance the reliability and enforceability of electronic and digital signatures.

2. Legal Validity

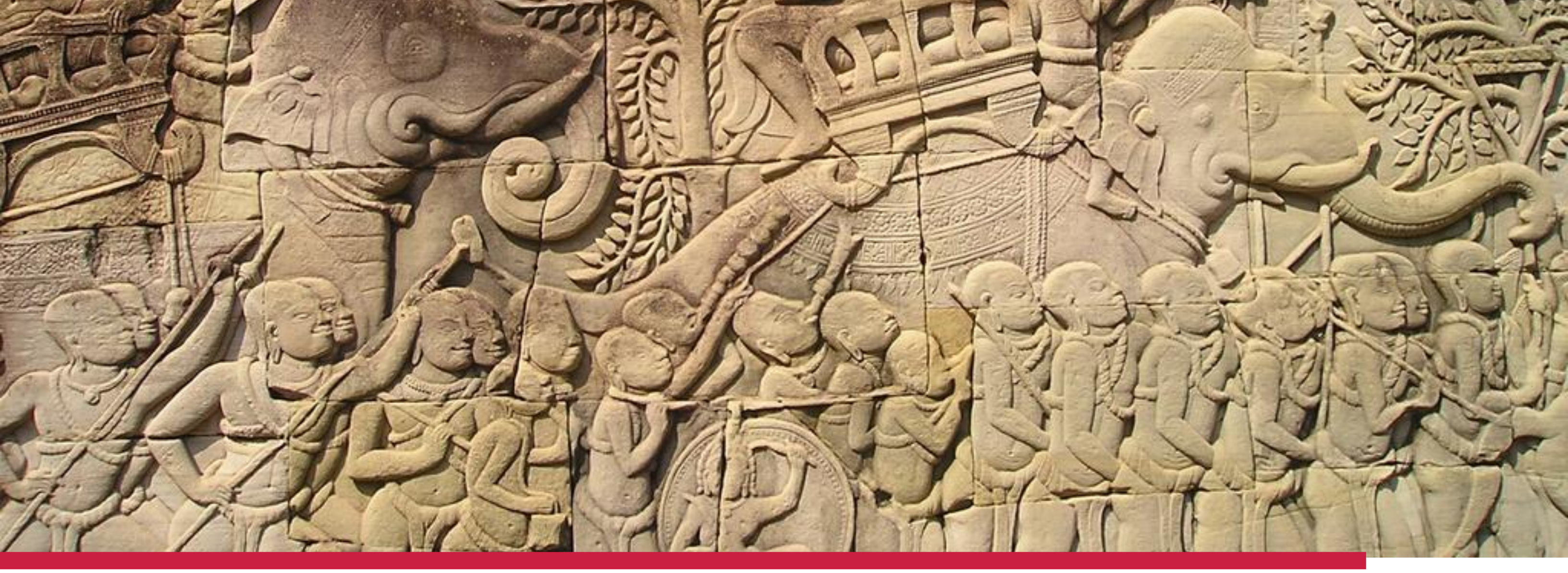
There is no admissibility difference between digital signatures and e-signatures. But for the enforceability requirement, under the E-Commerce Law, an e-signature is recognised as long as such signature (1) can identify the signatory and reflect the signatory's approval on the information contained in the message attached with such signature; and (2) is reliable.

Whereas a digital signature is required to have the corresponding digital signature certificate issued by a licensed certified authority, in order to be enforceable. To be valid, digital signatures must be issued by a certified authority, who is a legal entity that has obtained a Digital Signature License from the Ministry of Posts and Telecommunications. Further, Sub-Decree No. 246 does not specifically limit other government agencies or other service providers from being a certified authority. According to Sub-Decree No. 246, all online financial transactions shall use a digital signature, unless stipulated otherwise by the inter-ministerial decision.

In the financial sector, the National Bank of Cambodia's Technology and Cyber Risk Management Guidelines (2026) have established security and authentication requirements for digital financial services, including internet banking, mobile banking, e-wallets, payment processing services, and other online banking activities. In order for electronic signatures to be valid and enforceable, electronic banking and financial institutions are required to implement measures such as two-factor authentication, one-time password (OTP) controls with limited validity periods, cryptography, web application firewall protection, secure handling of sensitive information, and additional application security controls including input validation, CAPTCHA, or random token mechanisms.

3. Legal Requirements and Obligations

Laws and Regulations	Legal Requirements
E-Commerce Law	For e-signature, according to the E-Commerce Law, in order to be valid, it must: • Be able to identify the signatory, and reflect of approval of the signatory on the information or record containing in the communication attached with the e-signature; and • Be reliable, according to the characteristics, purposes, and circumstances whereby the communication is made or communicated.



Laws and Regulations	Legal Requirements
Sub-Decree No. 246	As for a digital signature, to be considered valid, it must meet the following requirements imposed by Sub-Decree No. 246: Certify the accurate and specific the signatory’s identity; • Certify the authenticity of the message attached with such digital signature; • Certify the time and date of the signing of the digital signature; and • Satisfy any other conditions required by the Ministry of Posts and Telecommunications. • In addition, according to Sub-Decree No. 246, the holder of a Digital Signature shall comply with the following obligations: • Keep the creation key of Digital Signature confidential and secure; and • Immediately notify the Certified Authority and the data receiver regarding the sent data when the creation key of the Digital Signature has been stolen, lost or leaked.
Technology and Cyber Risk Management Guidelines	In order to be considered valid and enforceability of online transaction, it must meet the following requirements as provided under TCRMG: • Implement two-factor authentication to validate customers' identities at each login session before allowing them to conduct any online transaction; • Ensure the secure authentication, such as one-time password (OTP), has a limited validity period for each financial transaction; • Implement web application firewall (WAF) to protect against Denial of Service (DoS) attacks; • Shall not store sensitive information in HTML hidden fields, cookies, or any other client-side storage; • Implement input validation, CAPTCHA, or random token to secure the internet banking web application; or • Use cryptography to provide authentication and authorisation.

4. Limitations on the Use of Electronic and Digital Signatures

Under the E-Commerce Law, an e-signature may not be used for activities, documents, and transactions related to:

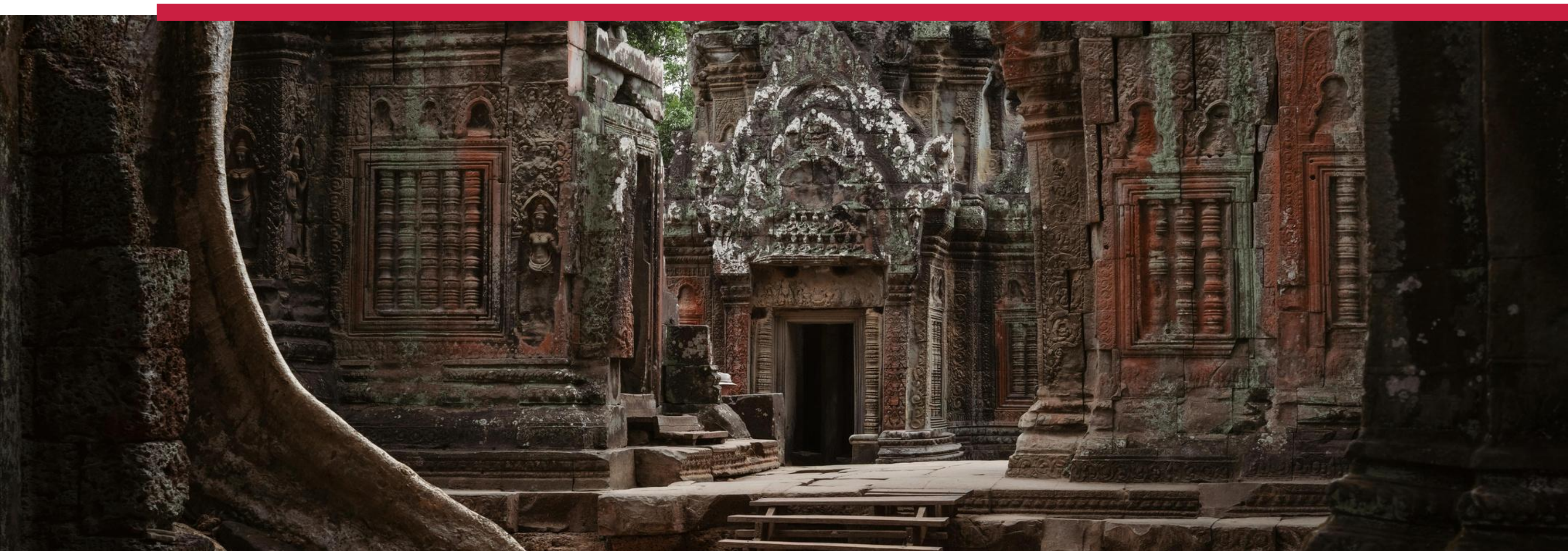
- Creation and enforcement of power of attorney;
- Creation and signing on wills, codicils, or other matters related to succession;
- Any contract on sale, transfer, or relinquishment of rights over immovable properties and other benefits of such properties;
- Transfer of immovable properties or any benefits related to such properties; and
- Any other cases deemed as exceptions, as determined by a sub-decree.

Aside from the exceptions as mentioned in point (a) above, there is no limitation on the use of an e-signature (including a digital signature) in specific processes or workflows. However, it is worth noting that the use of such signatures varies depending on actual practice. For instance, in court proceedings, it is not practical to validate the documents used in relation to the proceeding by using either a handwritten or electronic signature (thumbprint is preferred); although the existing Cambodian laws do not prohibit such usage.

5. Cloud-Based Signature and Data Residency

Currently, there is no law or regulation that specifically stipulates the acceptability of cloud-based (or remote) electronic signatures in Cambodia. However, according to the Sub-Decree No.246, it is worth noting that any publication of another person's private key and the act of storing or using another person's private key without written authorisation from the owner of a Certificate of Digital Signature is prohibited. Owing to such stipulation, in relation to the private key, it cannot be stored anywhere unless there is written authorisation from the owner of a Certificate of Digital Signature.

Furthermore, there is no specific law or regulation stipulating data residency requirements in general as well as in regard to storage and processing of electronic signature data outside of Cambodia.



6. Use And Recognition of Electronic and Digital Signatures

Digital signatures are not widely used in Cambodia due to the limited knowledge on the practical and legal aspects of the signature. Whereas for ordinary electronic signatures, despite being low, the usage of e-signature is generating larger demand because of various restrictions on physical signing due to COVID-19's impacts; and businesses are increasingly shifting online and considering the possible usage of e-signatures.

However, judges or magistrates are not acquainted with the implementation or enforcement of the electronic signatures or digital signatures. In practice, they still prefer the conventional handwritten signature.

According to the E-Commerce Law, state institutions are permitted to use electronic communication (including e-signature) for the following activities and operations:

- The receipt of registration of a document, or the fulfilment of a requirement for the creation or record of documents;
- The issuance of a license or permit;
- The determination of means and methods of payment; or
- Other activities as determined by the institutions.

Other activities as determined by the institutions.

If the institutions decide to use electronic communication for the above-mentioned activities or operations, the institution may specify:

- The method and form in which the information in the communication is registered, created, stored, or published;
- The type of signature required to be affixed in such communication;
- The method and form in which such signature is attached in the communication;
- Appropriate management processes and procedures to ensure accuracy, security, and confidentiality of communication or payment; and
- Other requirements rendering equivalent value between a document or payment in electronic form and a document or payment in written form.

AUTHORS

Vanseka Sok
Managing Partner
vanseka.sok@kinstellarsea.com

Sophanara DET
Junior Associate
sophanara.det@kinstellarsea.com

Kinstellar Southeast Asia (Cambodia) in association with Sok Siphana Sethalay was born from the recent combination of SokSiphana & Associates' and Sethalay Law Office's expertise and resources. As one of Cambodia's leading law firms, we offer comprehensive corporate and commercial legal services to a wide-ranging clientele – from multinational corporations to fast-growing local businesses.

With our sister law firm in Vietnam - Kinstellar Southeast Asia (Vietnam) - we are proud to be part of Kinstellar Southeast Asia's platform. Kinstellar is a leading law firm dedicated to delivering the highest quality advice and assistance to clients across Central and Eastern Europe, Southeast Europe and Central Asia. In addition to Southeast Asia, Kinstellar has operations in 12 countries with more than 400 lawyers: Austria, Bulgaria, Croatia, Czech Republic, Hungary, Kazakhstan, Romania, Serbia, Slovakia, Ukraine, Turkey, and Uzbekistan.

Vanseka Sok

Managing Partner, Sok Siphana Sethalay Law Office
vanseka.sok@kinstellarsea.com

Roman Hamala

International Partner, Kinstellar Southeast Asia
roman.hamala@kinstellarsea.com

Sok Siphana Sethalay Law Office

+855 23999878
info@kinstellarsea.com

GIA Tower, Floor 33A, Sopheak Mongkul Street, Koh Pich, 120101, Phnom Penh, Cambodia