

Understanding the Enforceability and Admissibility of Electronic Signatures in Saudi Arabia's Evolving Legal System

Saudi's evolving legal system now allows companies and individuals to use electronic signatures in commercial transactions, reducing reliance on traditional wet ink signatures.

Electronic signatures have been legally recognized in the Kingdom of Saudi Arabia (KSA) since the issuance of the Electronic Transactions Law promulgated by Royal Decree No. M/18 on March 27, 2007 (the Electronic Transactions Law) and the Evidence Law promulgated by Royal Decree No. M/43 on July 8, 2022 (the Evidence Law), subject to certain conditions detailed below. In 2023, the Electronic Transactions Law was amended to establish new authorities responsible for its implementation, and new implementing regulations were issued in 2024. This update is crucial for commercial transactions, as it impacts the legal framework governing electronic signatures. Understanding these changes is important for ensuring compliance and leveraging the benefits of electronic transactions in the KSA.

The use of electronic signatures is generally permitted, except in certain scenarios outlined in KSA legislation, such as deeds related to real estate or documents concerning civil status, and the [underlying regulatory framework](#) is advanced. Nonetheless, with the rapid pace of change as a result of digitization, this area of law and the list of licensed entities remain under constant development in KSA. Moreover, while the E-Commerce Law, promulgated by Royal Decree No. M/126 on July 10, 2019, does not directly regulate electronic signatures, it provides that in instances in which the E-Commerce Law is silent, e-commerce shall be subject to the provisions of the Electronic Transactions Law. As the landscape continues to develop in light of the mass digitization taking place in the KSA, companies are advised to stay informed about regulatory updates and ensure that their use of electronic signatures complies with the latest legal requirements to facilitate smooth and legally sound transactions.

What Are the Key Definitions of Electronic Signatures in the KSA?

Pursuant to the Electronic Transactions Law, an electronic signature is defined as electronic data included in, attached to, or logically associated with an electronic transaction used to verify the identity and approval of the signatory and to detect any change to said transaction after signature.

Certain certification services providers use certain features of the signatory, including their email address, name, and identity, to ensure that the electronic data provided by the signatory through its platform is logically associated with the relevant transaction. Therefore, both of these products would qualify as

electronic signatures under KSA laws and offer features that could potentially align with the requirements of the Electronic Transactions Law.

What Are the Licensing and Certification Requirements?

Under the Electronic Transactions Law, the Digital Government Authority (DGA) is responsible for licensing certification services providers that issue and store digital certification certificates as well as monitoring the activities of such certification services providers. The DGA also approves digital certification certificates issued by foreign entities outside the KSA. The implementing regulations of the Electronic Transactions Law delegate to the National Information Centre (NIC), which operates as part of the Saudi Data and Artificial Intelligence Authority (SDAIA), the supervision over issuance and management of digital certificates by certification services providers, and setting policies and procedures for secure digital certification. Previously, the licenses were issued by the Communications, Space, and Technology Commission, and the National Center for Digital Certification was responsible for issuing authentication procedures.

To qualify as a certification services provider, an entity must obtain a license from the DGA and ensure that certificates meet security and protection standards as set by the NIC. Certification services providers are responsible for issuing, delivering, and preserving digital certificates in compliance with the license and regulatory procedures, using reliable methods to protect against forgery, fraud, and damage.

How Are Electronic Signatures Valid and Admissible in the KSA?

Under the Electronic Transactions Law's implementing regulations, an electronic signature is considered binding under KSA law if it meets several key conditions, including that it be linked to a digital certificate issued by the NIC or a certification services provider licensed by the DGA, and this certificate must be valid at the time of signing.

Regardless of whether an entity is officially licensed, the general provisions of the Electronic Transactions Law still permit the use of electronic signatures and recognize electronic records as admissible evidence, with the following key elements important to consider:

- Approval and agreement to contracts can be expressed through electronic means, and such contracts are considered valid as long as they comply with the Electronic Transactions Law.
- An electronic record is regarded as an original if created and maintained in a manner that ensures the integrity of the information from the time the record is finalized, and if such record can provide the necessary information upon request.
- Electronic transactions and signatures are admissible as evidence if their electronic records meet certain criteria. Even if they do not fully meet these criteria, they may still be considered as presumptive evidence.
- Electronic transactions, signatures, and records are generally deemed reliable evidence unless proven otherwise. When evaluating the reliability of an electronic transaction, consider the method of creating, storing, or communicating the record, the means of maintaining the integrity of the information, and the method of identifying the originator.

Under the Evidence Law, electronic signatures are classified as "digital evidence," which can be either official or unofficial and is admissible under certain conditions. For instance, unofficial digital evidence is considered valid against transaction parties unless proven otherwise, with the burden of proof on the

party challenging its validity. This applies if the evidence is produced in accordance with the Electronic Transactions Law or E-Commerce Law, through an electronic method agreed upon by the parties in the agreement, or via an authenticated or publicly recognized platform.

In essence, if a signature is contested as not being a valid electronic signature under the Electronic Transactions Law, the metadata associated with the signature can be used as evidence of a party's intent to be bound by the document.

Next Steps

The evolving framework for electronic signatures in KSA marks a significant advancement in the regulation of digital transactions within the region.

Latham & Watkins will continue to monitor developments related to electronic signatures in the Middle East, including any forthcoming rules and regulations, and will provide further guidance to ensure compliance and effective use of electronic signatures in transactions.

The authors would like to thank Shahad Mohamed AITurki and Abdulmohsen AISaleh for their contribution to this Client Alert.

If you have questions about this Client Alert, please contact one of the authors listed below or the Latham lawyer with whom you normally consult:

[Abdullah A. Alasaheed](#)

abdullah.alasaheed@lw.com
+966.11.207.2518
Riyadh

[Omar Ali Al-Qazlan](#)

omar.al-qazlan@lw.com
+966.11.207.2521
Riyadh

You Might Also Be Interested In

[Saudi Arabia Practice – Latham & Watkins](#)

Client Alert is published by Latham & Watkins as a news reporting service to clients and other friends. The information contained in this publication should not be construed as legal advice. Should further analysis or explanation of the subject matter be required, please contact the lawyer with whom you normally consult. The invitation to contact is not a solicitation for legal work under the laws of any jurisdiction in which Latham lawyers are not authorized to practice. A complete list of Latham's Client Alerts can be found at www.lw.com. If you wish to update your contact details or customize the information you receive from Latham, [visit our subscriber page](#).