ALDHABAAN & PARTNERS IN ASSOCIATION WITH EVERSHEDS SUTHERLAND (INTERNATIONAL) LLP

ACC Association of Corporate Counsel MIDDLE EAST

BY IN-HOUSE COUNSEL

FOR IN-HOUSE COUNSEL

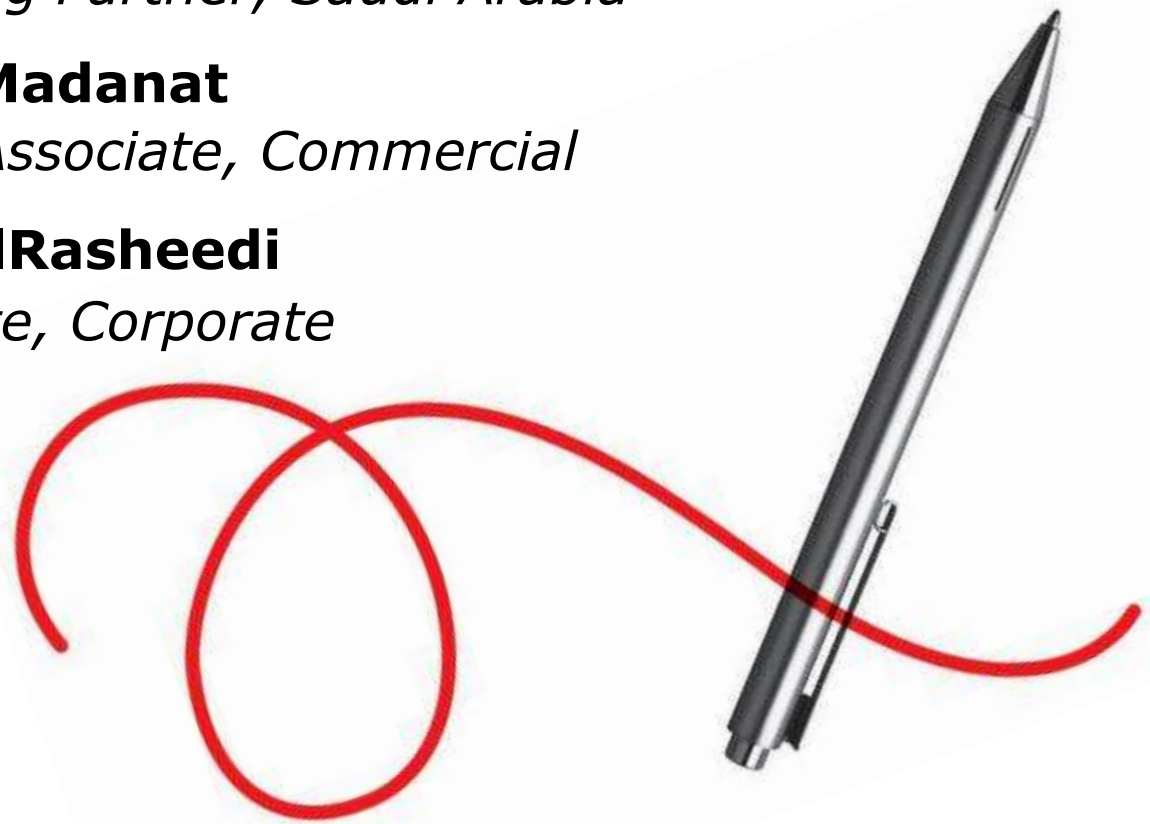
What you need to know about e-Signatures

The law and practice and remote public services in K.S.A.

Fahad AlDehais
Managing Partner, Saudi Arabia

Tareq Madanat
Senior Associate, Commercial

Sami AlRasheedi
Associate, Corporate



We will cover:

1. Law and Practice around E-signatures
2. Judicial Enforceability of E-signature

1. Law and practice around E-signatures

1. Law and practice around E-signatures

Electronic Transactions Law – introduction and background

- **Electronic Transactions Law of 2007 (1428H) (the "ETL")**
- **Implementing regulations of the ETL of 2008 (1429H)**
- Define and regulate electronic transactions and electronic signatures and apply to all electronic transaction and electronic signatures, save for:
  - dealings pertaining to personal status issues
  - issuance of title deeds pertaining to real property, except for real property with an area not exceeding 2,500 sqm
- Additionally, from a practical standpoint, notarizations are not currently enabled with e-signatures, such as POAs or the notarization of articles of association

1. Law and practice around E-signatures

Electronic Transactions - background

What is an "Electronic Transaction?"

- The ELT defines an "Electronic Transaction" as:

  "*Any exchange, communication, contract or other procedure, performed or executed, wholly or partially, by electronic means*"

- "Electronic" in this context, means technology based on using electrical, electromagnetic, optical or similar capabilities

Consent

- The ETL requires existence of express or implied consent to a an electronic transaction by private sector parties. Governmental bodies must consent to the electronic dealing explicitly, in all cases, an express contractual term providing for the parties' consent to the electronic nature and process of the relevant dealings would be prudent in contracts with both private and public sector counterparties, to ensure consent can be easily established
- When considering whether implied consent has been given, the court will consider applicable general principles of *Shariah*, for example, commencing performance

1. Law and practice around E-signatures

Electronic Transactions – background

When are Electronic Transactions captured by the ETL?

- The ETL will apply to any electronic transactions to which Saudi law applies, either by agreement of the parties, or by operation of law in cases where the relevant contract is silent, in accordance with applicable rules, including the nature of the of commercial transaction, the domicile of the contracting parties, and the jurisdiction of performance
- Parties are to ensure clear jurisdiction and governing law provisions are explicitly agreed to, in order to avoid conflict of laws issues or issues relating to the competent venue for disputes. These issues may be exacerbated by fully electronic dealings, especially where the parties are located in different jurisdictions or where the relevant obligations can be performed electronically without reference to a specific jurisdiction

1. Law and practice around E-signatures

State level: defining e-signatures

What is an Electronic Signature?

- The "**ETL**", defines "E-Signatures" as:

  "*Electronic Data included in, attached to, or logically associated with an Electronic Transaction, used to verify the identity and consent of the person signing it and to detect any change to said transaction after signing*."

- While, "Electronic Data" is defined as:

  "*data with electronic properties in the form of texts, codes, images, graphics, sounds or any other electronic form, whether combined or separate.*"

1. Law and practice around E-signatures

State level: defining e-signatures

- As such, an **electronic signature** can be defined:

Any text, code, images, graphics, sounds or other form of electronic data that attaches to, or is logically associated with an exchange, communication, contract or other procedure, performed or executed, wholly or partially, by technology means based on electrical, electromagnetic, optical or similar capabilities, used to verify the identity and consent of the person signing it and to detect any change to said transaction after signing

1. Law and practice around E-signatures

State level: defining e-signatures

Types of e-signatures

- Based on the foregoing, the definition of an e-signature under the ETL includes both:
  - basic electronic signatures, such as a scanned image of the person's ink signature, or a hand-signature created on a tablet by hand or using a stylus (referred to as “BESs”); and
  - secure electronic signatures, being electronic signatures secured by digital signature encryption technology used to verify the authenticity of an e-signature, such as cloud-based crypto tokens (referred to as “SESs”)
- The law assigns different evidentiary value to standard and secure electronic signatures respectively. These are addressed further along in the presentation (further explanation is provided in the coming slides)

Requirements/conditions of e-signatures

- E-signatures are deemed binding and their validity or enforceability may not be denied, nor their enforceability prevented for being completely or partially done electronically (*further information on the enforceability is provided in the coming slides*), provided that they are done according to applicable conditions, being:
  1. the e-signature must be linked to a digital certificate issued by a licensed digital certification service provider, or to a digital certificate adopted by the National Center for Digital Certification
  2. the digital certificate relating to the relevant must be valid at the time of signing
  3. maintaining the integrity of the signatory's identity data, and said data's compatibility with the contents of the digital certificate
  4. if the e-signature was made jointly with an electronic signature system (being an e-data system designed to work independently or with another e-data system, to generate an e-signature), the integrity of the logical and technical link between the electronic signature system and the relevant electronic data system (being one or more electronic devices or programs used to generate, retrieve, send, transmit, receive, store, display or process electronic data), and is free from technical defects that may affect the validity of the signature and its transmission

1. Law and practice around E-signatures

E-signature requirements

5. the availability of a minimum of technical and administrative infrastructure, as well as related resources that achieves control over the e-signature procedures and that ensures confidentiality of data in accordance with the technical conditions contained in the digital certification procedures of the relevant digital certification services provider; and
6. the signatory must adhere to all conditions in the e-signatures certification procedures of the digital certification services provider in a manner that does not conflict with the ETL

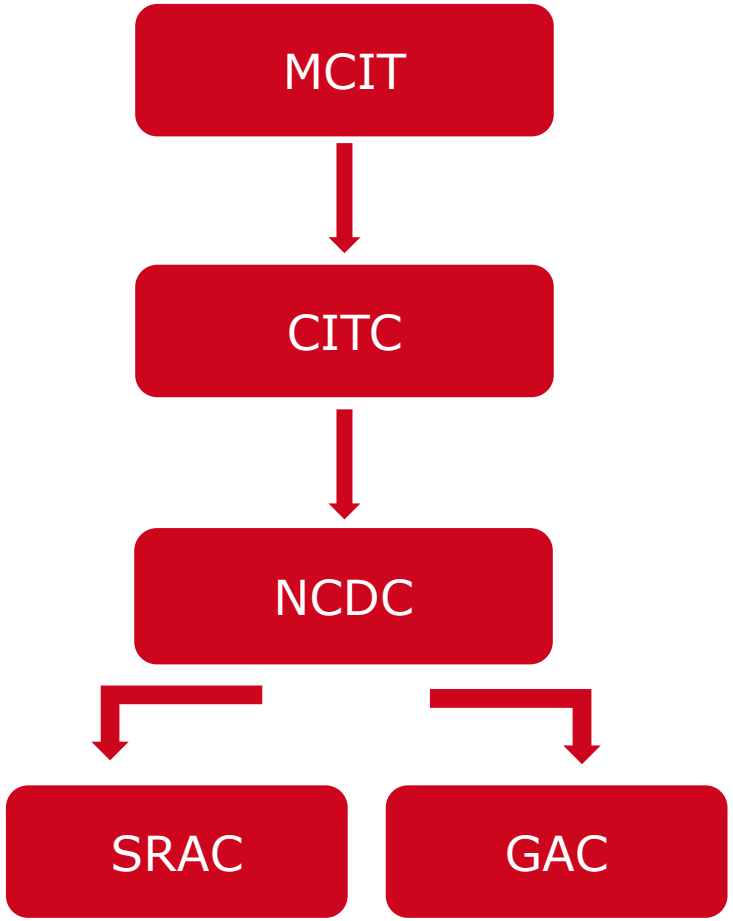
- As such, in order for an e-signature to have the weight of conclusive evidence, it must be a secure electronic signature, whereas a basic electronic signature may be used as presumptive evidence, along with other circumstantial matter. With respect to SESs, a signature interface provider employing best practices will also collect "process evidence" to establish what occurred at every stage of the signing process. Parties using e-signature certification services may care to check that the relevant e-signature solution used, caters for collection of such process evidence

1. Law and practice around E-signatures

E-Signatures – key players

Relevant Authorities

- MCIT: Ministry of Communications & Information Technology
- CITC: Communications & Information Technology Commission
- NCDC: National Center for Digital Certification
- SRAC: Saudi Root Authentication Center
- GAC: Government Authentication Center



1. Law and practice around E-signatures

E-Signatures – key players

- The CITC is the sector regulator and issues licenses to private sector digital certification service providers
- The NCDC was established by the MCIT to provides trust services to secure the exchange of information between key stakeholders, including government, citizens and the business sector. the NCDC operates as a closed business system model. Its scope includes the management and delivery of PKI policies and procedures, and the supervision of matters relating to digital certification, including the issuance of digital certificate certificates to licensed service providers
- Under the NCDC are the SRAC and GAC, responsible for the provision of PKI systems, and the management of digital certificates to government employees and governmental bodies, respectively

1. Law and practice around E-signatures

E-Signatures – key players

- The NCDC is also the competent authority to approve (adopt) digital certificates issued by foreign parties outside the Kingdom. Said certificates shall be considered equal to those issued in the Kingdom, in accordance with certain conditions and procedures specified in the ETL Implementing Regulations. The Regulations refer to certain general principles to be carted for when approving a foreign-issued digital certificate (such the consistency of licensing conditions for service providers with national standards), but defer to a specific "Mutual Certification Policy" to govern the applicable procedures, which policy has not yet been made available
- Further, the NCDC is to issue a list of approved foreign digital certification providers. Such a list has not yet been made available

Licensed Digital Certificate Services Providers

– The following two entities are currently the only two entities licensed to issue Digital Certificates for the private section in Saudi Arabia:

1. BAUD Telecom Company (BTC) – offered under the branded service "emdha": https://www.emdha.sa/; and

2. Arabian Internet and Communications Services Co Ltd (STC Solution) – offered under the branded service "Sayen": https://www.stc.com.sa/wps/wcm/connect/english/business/iot/managedservices/digital-signature-service-sayen

2. Judicial Enforceability of E-Signatures

2. Judicial Enforceability of E-signatures

E-Signatures – evidentiary weight

Effect and evidentiary weight of an e-signature

- An e-signature that is compliant with ETL has the same weight as a 'wet' signature
- If an e-signature (that is compliance with applicable requirements – *as shown in the previous slides*) is provided in any legal procedure, the following shall be deemed true, unless proven otherwise or the concerned parties agree to the contrary:
  - the e-signature belongs to the person identified in the relevant digital certificate
  - the e-signature was provided by the person identified in the relevant digital certificate for the purpose specified therein; and
  - the relevant electronic transaction has not been altered since the electronic signature was affixed thereto

1. Law and practice around E-signatures

E-Signatures – evidentiary weight

Admissibility into evidence

- Electronic transactions and/or e-signatures shall be admissible as evidence if their Electronic Records satisfy the requirements set forth in the ETL and its Implementing Regulations
- Electronic transactions and/or e-signatures may be admissible as **presumptive evidence** even if their Electronic Records do not satisfy the requirements set forth in the ETL (although, please see next slide on relevant considerations under the Commercial Courts Law in force)
- The ETL defines an "Electronic Record" as "*data generated, communicated, received, or stored by electronic means, and retrievable in perceivable form.*"
- Electronic transactions, e-signatures and records are deemed by the ETL to be reliable evidence in transactions, and shall be deemed intact unless proven otherwise

2. Judicial Enforceability of E-signatures

E-Signatures – evidentiary weight

Commercial Courts Law

- The newly enacted Commercial Courts Law of 2020 also recognizes electronic evidence as having evidentiary weight, and lists electronic transcripts, electronic media, means of communication, email, and electronic records as types of electronic evidence. The law defers to the Law's implementing regulation to stipulate the types of electronic evidence, means for verification of electronic evidence and the procedures for its submission as evidence. The implementing regulations of the Commercial Courts Law have not yet been issued, and so it remains to be seen if or how the newly enacted law will affect the legal status of BESs and SECs under Saudi law

Judicial Guidance

- The General Assembly of the Supreme Court has also recognized digital evidence as having evidentiary weight barring manifest error, ruling the admissibility into evidence of digital evidence, the strength or weakness of which shall be "*decided based on the relevant* occurrence*, related circumstances and other related evidence*"

2. Judicial Enforceability of E-signatures

E-Signatures – evidentiary weight

BES vs SEC

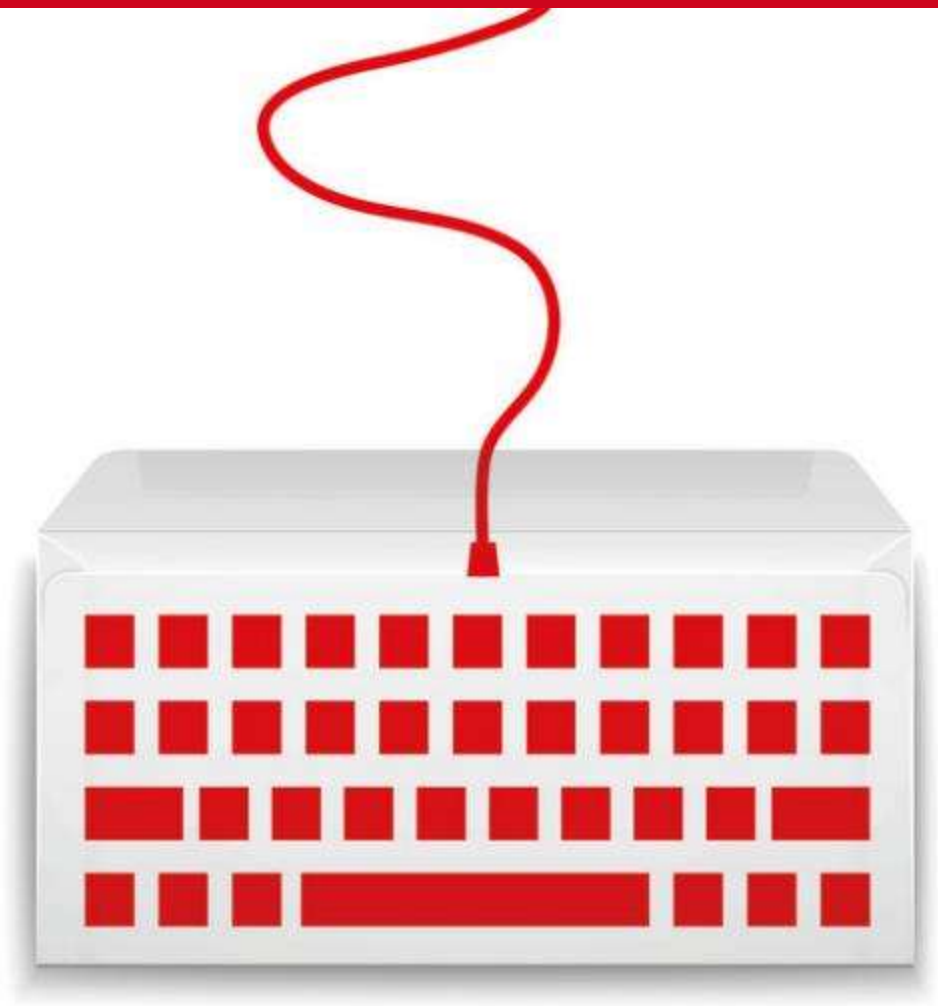
- Despite carrying the status of presumptive as opposed to conclusive evidence, a BES can still have the same evidentiary effect as a SES depending on the circumstances surrounding execution and other evidence provided. In cases where a service provider collects and provides "process evidence" in accordance with best practices it should be able to furnish compelling evidence as to the authenticity of an e-signature. In such cases the court will want to satisfy itself that the processes and practices employed in collecting, retaining, and disseminating any such electronic records is in compliance with applicable standards and requirements

1. Law and practice around E-signatures

Practical considerations

Things to keep in mind

- Express consent to electronic nature of transaction/signature is prudent practice
- Amendments to a contract executed by the e-signature must be accompanied by another e-signature
- Difference between BES and SES
- Conclusive evidence vs presumptive evidence
- The need to collect process evidence when using BES
- Sufficient indemnities in relationship with service provider



Any Questions?

ALDHABAAN & PARTNERS IN ASSOCIATION WITH EVERSHEDS SUTHERLAND (INTERNATIONAL) LLP

Fahad AlDehais
Managing Partner, Saudi Arabia

T: +966 11 277 9811
M: +966 50 442 8520
AlDehais@aldhabaan-es.com

Tareq Madanat
Senior Associate, Saudi Arabia

T: +966 11 484 4448
M: +966 542 118477
SamiAlRasheedi@aldhabaan-es.com

Sami AlRasheedi
Associate, Saudi Arabia

T: +966 11 484 4448
M: +966 55 507 9117
tareqmadanat@aldhabaan-es.com

aldhabaan-es.com