EMERGING ISSUES IN DIGITAL ID PART 4

DIGITAL SIGNATURES

A Use Case and Issue Brief
Prepared by CIPIT

Strathmore University

Centre for Intellectual Property and Information Technology Law

01

BACKGROUND

Precautions being put in place in light of the COVID-19 pandemic include mandatory orders or recommendations for persons to work from home. With many non-essential businesses working remotely, the authentication or execution of documents with handwritten signatures can be cumbersome. In these circumstances, digital signatures are an ideal solution to this problem.

Laws in different jurisdictions impose different requirements in relation to the validity, use or authentication of digital signatures. Countries such as Nigeria, Cameroon, Egypt, South Africa, Kenya, and others have passed laws to make electronic signatures, which include digital signatures, legally binding.

As digital signature programs cannot link digital signatures to specific persons, they make use of certificate-based digital ID to identify and authenticate signers. This is made possible by third party Certification Authorities (CAs), alias certification service providers, who validate the identity of persons before issuing digital certificates which outline certain attributes of individuals.

JUSTIFICATIONS FOR THE USE CASE

1. Digital ID for digital signatures is required for the identification of signers.
2. Completion of transactions without the need of face to face interactions.
3. Continued and efficient operation of organizations.

DATA INVOLVED IN THE USE CASE

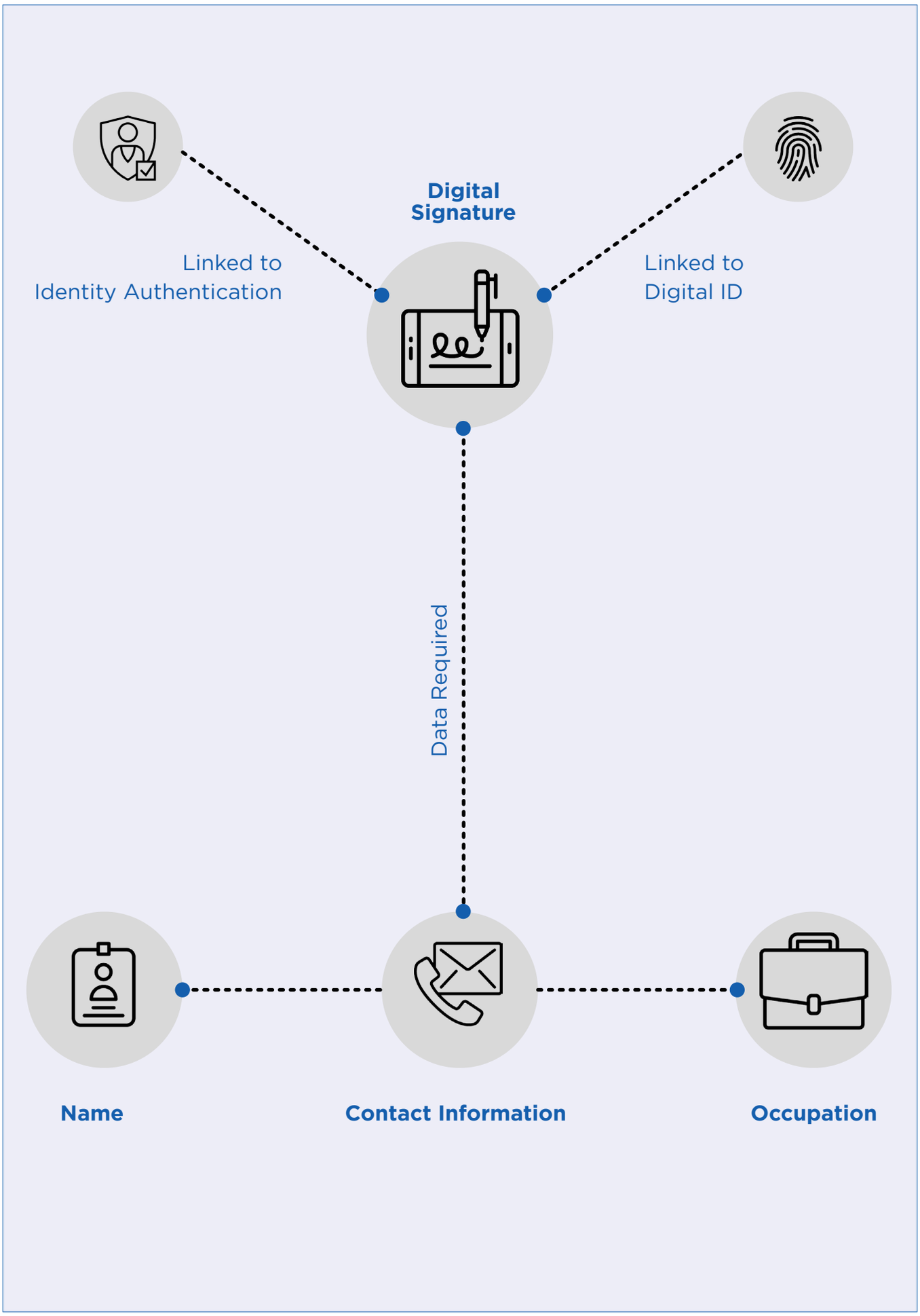
Data collected for Digital ID in the use case include:

1. Names.
2. Contact information i.e. email addresses and telephone numbers.
3. Job titles

RISKS INVOLVED IN THE USE CASE

Risks associated with Digital ID in the use case include:

1. Fraud.
2. Identity Theft.
3. Privacy Breaches.
4. Man-in-the middle attacks
5. Eavesdropping attacks
6. Malware attacks.


Digital Signature
Linked to Identity Authentication
Linked to Digital ID
Data Required
Name
Contact Information
Occupation

02

ANALYSIS

Digital signatures, like handwritten signatures, are meant to authenticate the source of signed messages, to assure their integrity in transit and to prevent signers from disclaiming signed messages. Thus, in many countries digital signatures are legally equivalent to hand-written signatures.

Certificate authorities are trusted to protect personal and business information from being accessed by unauthorized persons. Vulnerabilities in the security of Digital ID managed by Certification authorities may be exploited by hackers to partake in illicit activities like economic fraud, malware diffusion among other cyberattacks. Persons whose digital certificates are stolen may suffer identity theft. As digital signatures accompanied with valid digital certificates are required for the installation of certain software, cybercriminals may steal or intercept legitimate digital certificates and use them to sign malware, purporting to be legitimately certified individuals. Cybercriminals can also abuse digital certificates to divert resources or funds elsewhere.

Allowance of, or reliance on, digital signatures can be somewhat controversial for various reasons. For example, Kenyan law provides that the Communications Authority of Kenya (CA, the government regulator for ICT) is empowered to approve certification authorities, but the CA has not yet approved any authorities. Thus, digital signatures in Kenya can currently only be authenticated by foreign authorities, a practice which may be frowned upon or untrusted. Furthermore, the law is only one factor determining the uptake of digital signatures, but may be insufficient in view of culture. Digital signatures may be refused even where the law specifically or generally allows them, especially where the technology is not understood or not trusted, and in cultures that place a high value on trust based on personal interactions.

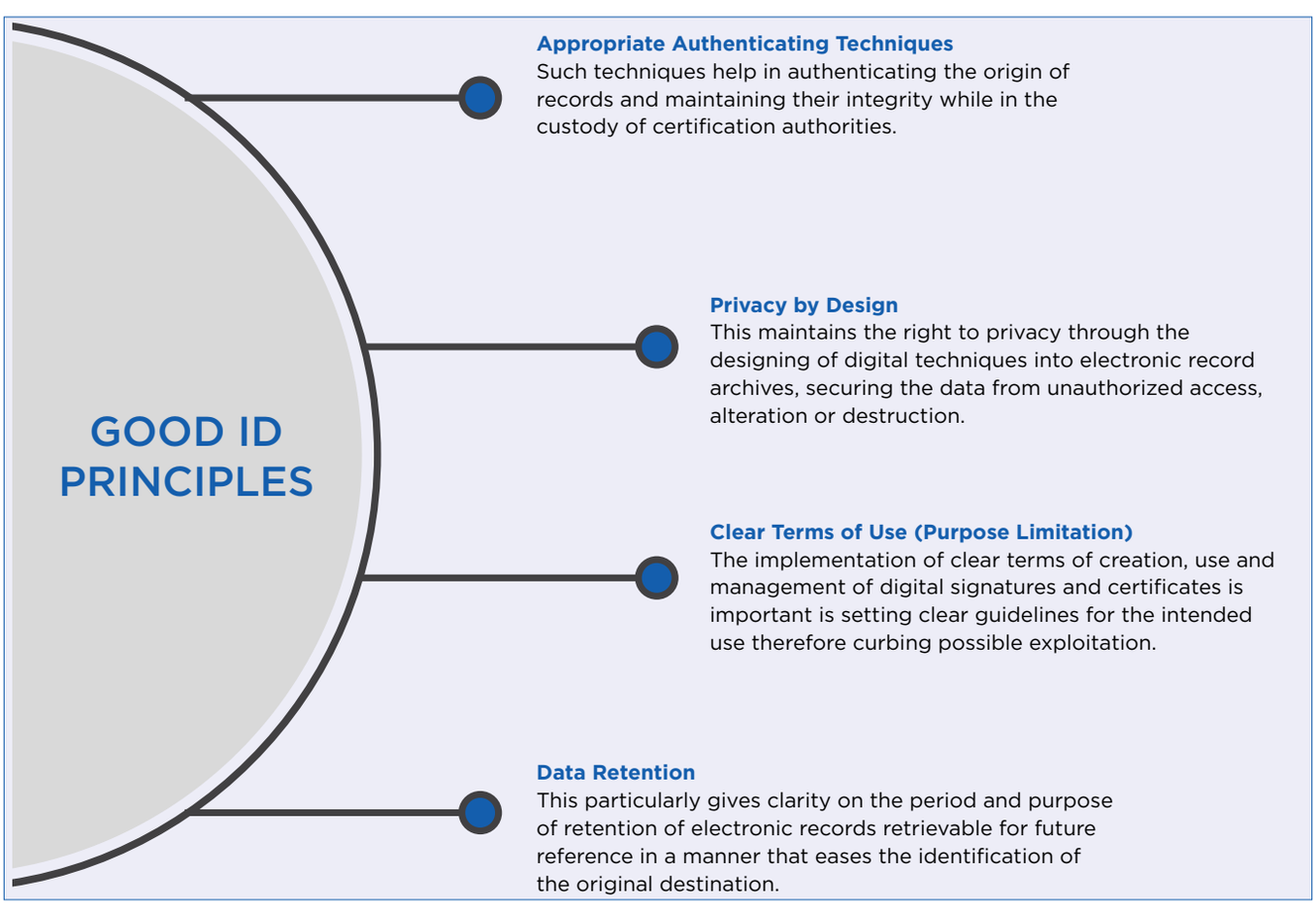
03

CONCLUSION

In light of social distancing and stay-at-home orders issued by governments to curb the spread of COVID-19, digital signatures could ease business transactions by enabling virtual signing. If not properly secured, the Digital ID based in the digital certificates that link digital signatures to the identities of signers could expose signers to various cyber breaches. Thus, data management systems that keep the involved Digital ID safe are essential.

GOOD ID PRINCIPLES

1) Adoption of appropriate techniques for authenticating the origin of records and for maintaining their integrity while they remain in the custody of certification authorities.
2) Designing digital techniques into electronic record archives to secure retained data from unauthorized access, alteration or destruction.
3) Implementation of standards for the creation, use, and management of records that contain digital signatures and digital certificates.
4) Retention of electronic records for a specified period so that they are retrievable for future reference; and in format that can ease the identification of the original destination, date and time of dispatch or receipt.



04

ADDENDUM: KENYA AS A CASE STUDY

In Kenya, the Business Law (Amendment) Act, enacted into law on 18 March 2020 is one of various laws that regulate electronic signatures in Kenya. Even before the recently assented Act, electronic signatures were, and still are, recognised, under Kenya Information and Communications Act (KICA), as equal to written signatures. Under Section 83G of the KICA, a matter that should be in writing is also satisfied if the matter is made available in an electronic form, and remains accessible so as to be usable for a subsequent reference. Additionally, an offer and acceptance of an offer in the formation of contracts expressed by means of electronic messages is valid and enforceable under the Act. Advanced electronic signatures –synonymous with digital signatures – are defined in the Act as electronic signatures that are: "uniquely linked to the signatory; capable of identifying the signatory; created using means that the signatory can maintain under his sole control; and linked to the data to which it relates in such a manner that any subsequent change to the data is detectable".

Under the Evidence Act, to prove that an electronic signature is that of an alleged signer, certification service providers may be required to produce an electronic signature certificate. Certification services providers are to be licensed by the Communications Authority of Kenya (CAK) to issue digital certificates. The creation and publication of digital certificates for fraudulent or unlawful purposes is an offence under KICA. Currently, there is only one certification service provider licenced by the CAK: KENET Certification Authority.

According to Section 83H of KICA, electronic records are to be retained in the format in which they were originally generated, sent or received and contain details which will facilitate identification of the original destination, date and time of dispatch or receipt of such an electronic record. The Kenya Information and Communications (Electronic Certification and Domain Name Administration) Regulations gives further detail on the electronic records that certification service providers are to retain. These include digital certificates which are to be preserved for a period of not less than seven years.

RECENT AMENDMENTS

The Business Law(Amendment)Act makes significant amendments to certain Acts of Parliament, expanding the use of electronic signatures in transactions.

Whereas the Law of Contract Act previously only provided for handwritten signatures, the definition of signing in the Business Law Act now incorporates signing by way of an advanced electronic signatures.

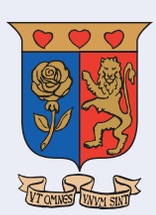
The Registration of Documents Act is amended to permit the use of electronic signatures and advanced electronic signatures in signing documents presented for registration at the Registrar of Documents, which may also be filled and maintained electronically.

The Survey Act is similarly amended to include electronic signatures and advanced electronic signatures as valid forms of signatures.

The Land Registration Act (LRA) has also been amended to provide for use of electronic signatures and advanced electronic signatures. The Act further permits the electronic processing and execution of instruments under the Act. Before this amendment, dispositions of land interests according to the LRA, the Law of Contract Act and the Land Act were expected to be in writing, physically executed and attested.

KICA previously prohibited electronic transactions in 3 instances: in the execution of wills, in negotiable instruments and in documents of title. The Business Law Act amends this by allowing for the execution of documents of title using electronic signatures.

These amendments could ease business transactions in the wake of the COVID-19 pandemic as movement has been restricted in certain towns in Kenya and working from home is encouraged by the government.



Ole Sangale Rd, Madaraka Estate.
PO Box 59857 00200, Nairobi, Kenya | Tel +254 (0)703 034 612
Email: cipit@strathmore.edu | Website: https://cipit.strathmore.edu