THE UNIVERSITY OF NAIROBI

COLLEGE OF BIOLOGICAL AND PHYSICAL SCIENCES

SCHOOL OF COMPUTING AND INFORMATICS

A PUBLIC KEY INFRASTRUCTURE MODEL FOR VERIFICATION OF COURT DOCUMENTS: THE JUDICIARY OF KENYA

HELLEN NYAMUIRU KABIRA

P53/86181/2016

SUPERVISOR: PROF. ROBERT OBOKO

Submitted in partial fulfillment of the requirements for the award of Master of Science in Distributed Computing Technology, 2021

DECLARATION

I Hellen Nyamuiru Kabira, do hereby declare that this research project is entirely my own work and where there is work or contributions of other individuals, it has been duly referenced as acknowledgement.

To the best of my knowledge, similar research has not been carried out before or previously presented to any other university.

Sign: Kabira Date: **20th August 2021**

Name: Hellen Nyamuiru Kabira

Reg. No: P53/86181/2016

This project has been submitted in partial fulfillment of the requirement for the Master of Science degree in Distributed Computing Technology at the University of Nairobi with my approval as the university supervisor.

Sign: -- Date: 27/08/2021 --

Name: Prof. Robert Oboko

School of Computing and Informatics

University of Nairobi.

DEDICATION

To my father; posthumously, you believed in me.

To my mother; you have been there all the way.

To my children; it can be done, go conquer!

ACKNOWLEDGEMENT

God has been faithful, I wouldn’t have if He didn’t will. He has sustained me through the cycle. I can’t thank Him enough.

I appreciate the push and drive from my able supervisor Prof. Robert Oboko. He was available and offered necessary support to see to the completion of this project. I am grateful for the privilege of having the School of Computing and Informatics vast resources that made this achievable.

I am thankful to my husband Kariuki, my children: Kamau, Kabira, Kinuthia and Wanjiru for being somewhere behind the scenes. I wouldn’t have been motivated enough if it wasn’t your presence in my life. Thank you.

Finally, I would like to thank other family members, colleagues and all the people that directly or indirectly supported and contributed to the realization of this research work.

ABSTRACT

Present day government is heavily investing in the provision of services over the internet. This comes with the benefits such as transparency, access to data and information and service availability at any time Inherently, the high dependence of data flow between the service providers and citizenry introduces the need to ensure security of this data due to the risks and challenges that come with online presence of these services. There is therefore need for the assurance of confidentiality, integrity, authentication, availability and non-repudiation in regards to data creation and transmission. A Public Key Infrastructure (PKI) is a set of roles, policies, and procedures needed to create, manage, distribute, use, store, and revoke digital certificates and manage public-key encryption.Technologies such as digital signatures and encryption are achieved through the PKI model. The research therefore set out to develop a model that uses digital signatures as one of the security measures in documents management for the Judiciary of Kenya. A qualitative research design is used to collect data that guides the development of a prototype as well as gather user feedback from the user tests. The design and create strategy of building information systems is used to come up with the prototype while following the waterfall model. The solution is used to generate all court related administrative and statutory documents as well as use their private key to digitally sign them. A verification mechanism was also built for the documents consumers. On hosting the system for testing, test case results and a post-implementation survey demonstrates that integrity, authenticity and non-repudiation is achieved.

Table of Contents

DECLARATION..2

DEDICATION...3

ACKNOWLEDGEMENT..4

ABSTRACT...5

Chapter 1: Introduction...13

1.1. Background Information..13

1.2. Problem Statement...15

1.3. Research Objectives..17

1.4. Research Questions...17

1.5. Justification..18

1.5.1. Importance to computer science...18

1.5.2. Importance to the Judiciary..18

1.5.3. Importance to the court users and the public...............................18

1.6. Scope of the study...19

Chapter 2: Literature Review...20

2.1. Introduction...20

2.2. Information security issues in e-government...20

2.3. Cryptography...21

2.3.1. Symmetric Key Cryptography..21

2.3.2. Asymmetric Key Cryptography..22

2.3.3. Public Key Infrastructure..24

2.3.4. Pretty Good Privacy (PGP)..28

2.4. The government of Kenya’s digitization journey...................................29

2.5. The Judiciary of Kenya..29

2.5.1. The court structure...30

2.5.2. Digitization of the Kenyan Judiciary..31

2.6. PKI Enabled e-government initiatives...36

2.6.1. PKI in Estonia..37

2.6.2. PKI in India..40

2.6.3. PKI in Rwanda...41

2.7. Current Status of PKI in Kenya...42

2.7.1. The Legal Framework in Kenya...42

2.8. Conceptual Model...44

Chapter 3: Research Methodology...45

3.1. Research Design...45

3.2. Data Collection...47

3.3. Location...47

3.4. Population..48

3.5. Sample Size..48

3.6. Software Methodology..48

3.6.1. Requirements Analysis...49

3.6.2. Data Analysis: Pre-Implementation Survey.....................................50

3.6.2.1. Current system usage to track litigation process.........50

3.6.2.2. System security confidence...52

3.6.2.3. Current court documents authenticity and validity.....54
3.6.2.4. New technologies adaptation for verification............... 55
3.6.2.5. Conclusion... 56
3.6.3. System Analysis and Design...57
3.6.3.1. System Architecture.. 57
3.6.3.2. Use Case diagram...59
3.6.3.3. System Flow Chart...60
3.6.3.4. Document verification sequence diagram..................... 63
3.6.3.5. Database Schema..64
3.6.4. System Implementation.. 65
3.6.4.1. Technology Stack..65
3.6.4.2. Key generation software.. 66
3.6.4.3. Key Pair Management.. 67
3.6.4.4. Court Document Creation...67
3.6.4.5. Document signing via MAYAN API.................................... 69
3.6.4.6. Public Facing verification module......................................70
3.6.5. Verification, testing and deployment..73
3.6.5.1. Unit Testing... 74
3.6.5.2. Integration Testing.. 75
3.6.6. Maintenance.. 75
Chapter 4: Results and Discussion.. 76
4.1. Results: Data Analysis...76
4.1.1. Objective 1: To identify security threats of e-government.... 76
4.1.2. Objective 2: To develop a prototype that uses Public Key Infrastructure in cryptography for verification of documents emanating from the courts...78
4.1.3. Objective 3: To evaluate court users satisfaction in the existence of a court documents verification mechanism.................. 80
4.1.3.1. System Availability...80
4.1.3.2. System Adoption.. 82
4.1.3.3. User experience..83
4.1.3.4. Accuracy...84

4.1.3.5. User satisfaction..86

4.2. Summary results and interpretation..88

4.3. Discussion...91

4.4. Challenges...92

Chapter 5: Conclusion and Recommendation...93

5.1. Summary..93

5.2. Recommendations...94

5.3. Further Research Areas...94

5.4. Conclusion...94

References...95

Appendices...100

Appendix A: Judicial Officers Pre-Implementation questionnaire.........100

Appendix B: Advocates Pre-Implementation questionnaire..................102

Appendix C: Judicial Officers Post-Implementation questionnaire.......104

Appendix D: Advocates Post-Implementation questionnaire................105

Appendix E: Sample Code...108

List of figures

Figure 1 : How Encryption works: symmetric Key Cryptography (Casey, 2020)........21
Figure 2 : Public Key Cryptography........23
Figure 3 : Public Key Infrastructure........25
Figure 4 : Interaction of entities within the PKI (Agangiba et al, 2013)........27
Figure 5 : Digital signatures design (Source: Choudhury et al., 2002 through Geoffrey, 2012)........28
Figure 6 : Structure of courts in Kenya........30
Figure 7 : The Judiciary Transformation Framework (2012-2016)........32
Figure 8 : Filing cabinet in the courts........34
Figure 9 : The Judiciary of Kenya Case Tracking System........35
Figure 10 : The Judiciary e-filing system in Kenya........36
Figure 11 : PKI for e-government (Agangiba et al, 2013)........37
Figure 12 : Estonia Information system architecture........38
Figure 13 : Applications of PKI in Rwanda........41
Figure 14 : An excerpt of the definition of the electronic signature in Kenya law (Kenya Gazette Supplement No. 26 (Acts No. 1), 2020)........43
Figure 16 *: The conceptual model*........44
Figure 17 : Waterfall model........49
Figure 18 : Advocates usage of system........51
Figure 19 : Best channel to receive documents........51
Figure 20 : JO’s usage of system........52
Figure 21 : Advocate security confidence........53
Figure 22 : JO CTS account security confidence........53
Figure 23 : Court documents transmission validity........54
Figure 24 : Court documents content validity........55
Figure 25 : Document alteration........55
Figure 26 : new technology trial........56
Figure 27 : Need to verify source and document author........56
Figure 28 : System Architecture........57

Figure 31 : Use Case Diagram.. 59
Figure 32 : Generate Key and store flow chart... 60
Figure 33 : Create and Sign Document Flow Chart 61
Figure 34 : Verification of Documents Flowchart..62
Figure 35 : Document verification sequence diagram... 63
Figure 36 : ERD...64
Figure 37 : Key generation software... 66
Figure 38 : Key Pair Management... 67
Figure 39 : Court Document Creation..68
Figure 40 : Signature details.. 69
Figure 41 : Signature in Mayan...69
Figure 42 : Verify document by code on e-filing...70
Figure 43 : Valid document details... 70
Figure 44 : Error: Wrong JO selected as document signer.................................71
Figure 45 : Error- document was altered...72
Figure 46 : Non-existent document.. 72
Figure 47 : Advocates responding to validity of court documents.................. 77
Figure 48 : Judicial officers response to whether document content gets to recipient as intended.. 77
Figure 49 : Document alteration...78
Figure 50 : showing that the purported document generator is not valid.....79
Figure 51 : showing a document whose content has been altered.................79
Figure 52 : A valid document... 80
Figure 53 : JOs login..81
Figure 54 : Advocates system usage.. 81
Figure 55 : Response to whether JOs would use system for doc generation82
Figure 56 : Are security features on documents satisfactory?..........................82
Figure 57 : JO System ease of use..83
Figure 58 : Advocate ease of system use..83
Figure 59 : JO system accuracy feedback.. 84
Figure 60 : Advocate system accuracy..84
Figure 61 : signature details visibility...85

Figure 62 : Valid vs fake documents 85
Figure 63 : Importance of verification..86
Figure 64 : user email feedback..86

List of Tables

Table 1 : Research Strategy.. 46
Table 2 : Data Collection..47
Table 3 : Technology stack.. 66
Table 4 : Test cases... 75
Table 5 : General user comments..87
Table 6 : Summary results and interpretation... 91

List of Abbreviations

Abbreviation	Description
PKI	Public Key Infrastructure
CMS	Case Management System
CTS	Case Tracking system
OTP	One Time Password
SMS	Short Message Service
HTML	Hyper Text Markup Language
CSS	Cascading Style Sheets
JO	Judicial Officer

Chapter 1: Introduction

1.1. Background Information

The quest by present day governments to provide online services to its citizenry has seen to the establishment of various initiatives to ensure the same. Various public sector institution have focused their efforts on providing their services online to allow availability of services from anywhere all the time.

With inherent computerization, options of interaction between the government, organizations and citizens have brought about dependency on information flow between them (Rasim Alguliyev & Farhad Yusifov, 2015). With the flow comes a need to ensure security of the data in and out of these systems where the lack of it may lead to disservice to the consumers. The main components of information security are confidentiality, integrity, authentication, availability and non-repudiation. Challenges and obstacles of e-government (Hwang, 2004) are classified as technical, political, cultural and legal. On the technical aspect, IT infrastructure, promotion of security mechanism, integrity and secure payment mechanisms are identified as pertinent to the success of e-government. Privacy (Alshehri, 2010) is also identified as an obstacle and its also stated that the government cannot guarantee its word without robust technical solutions and transparent procedures. Mohamed & Zaipuna, 2014 identifies a number of technical threats of e-government among them being unauthorized information access and integrity loss.

In order to make the citizenry trust the provided services, trust, protection and security of the information is required by application of high security mechanisms between the systems (Upadhyaya, 2012 through Tri Kuntoro, 2017). Tri Kuntoro, 2017 states that security is the focal point in determining success or failure of e-government. He also identifies *confidentiality, integrity, authentication, authorization, traceability* and *non-repudiation* as the main goals of information security within these environments. He recommends firewalls, Intrusion detection systems, encryption mechanisms and Public Key Infrastructure as some of the most indispensable security techniques.

A Public Key Infrastructure (PKI) is a set of roles, policies, and procedures needed to create, manage, distribute, use, store, and revoke digital certificates and manage public-key encryption. It facilitates a channel through which the secure electronic transfer of information for a range of network activities such as e-commerce, internet banking and confidential email is provided. Various governments have adopted the use of this technology to enhance security within their e-government models. Through PKI, technologies such as digital signatures and encryption are achieved.

Estonia is one of the countries that has successfully implemented the PKI atop which runs a data exchange layer (X-road) that enables communication between different government systems. With PKI they have managed to (AS Sertifitseerimiskeskus, 2003) integrate their Health Information Service and the Estonian Health Insurance Fund. The land register is also based on this infrastructure where transactions are enabled by use of digital signatures for documentation between buyers, sellers, notaries, land registrars and judges (Vali et al, 2014). Other countries that have extensively employed the use of PKI are the UK and the US, closer home is Rwanda. The courts in Malaysia also use the government PKI which also covers the cost for e-certification offered by the Certification Authority for their e-solutions (Heike et al, 2016)

The Kenya e-government strategy of 2004 (Cabinet Office of the President, 2004), outlines the process towards realization of online government services. Subsequently, the Judiciary of Kenya through the Judiciary Transformation Framework (2012-2016) and Sustaining the Judiciary

Transformation (2017-2021) establishes various automation initiatives one of which is introduction of e-filing of court documents. Heike et al, 2016, writing on good practices for courts identifies court automation as one of the key areas. Key success elements identified are electronic signatures and identity verification, E-file size limitations and appropriate e-storage capacities, e-file size limitations and appropriate e-storage capacities and linkage to e-payment systems.

This study will therefore explore the incorporation of Public Key Infrastructure as a security technology for e-government with the main case study being e-filing at the Judiciary of Kenya.

1.2. Problem Statement

With the potential benefits of e-government such as transparency, access to data and information and service availability at any time comes a number of risks and challenges with the online presence of these services. Mohamed and Zaipuna, 2014 identify implementation of security and privacy as the main challenge in these initiatives. Hany, 2008 in his study on Citizens' Readiness for E-government in Developing Countries, there are trust issues among the citizens when it comes to transmission of information between government portals and the end user clients. There are also security issues in regards to security of information in government owned databases. Concerns of unauthorized access and authentication are largely mentioned.

The Judiciary of Kenya is entirely dependent on paper information to initiate, process and dispose off cases. Exchange of information between the parties, advocates, the registry and the court is done using documents that are drawn by each of this players. The Judiciary has undertaken various initiatives to digitize court files that have really never taken off. However, in the wake of the Covid-19 pandemic, the Judiciary quickly adopted the use of electronically transmitted documents via the web based e-filing portal and email. Documents prepared by the courts are equally transmitted via these e-channels. With this quick adoption of technology for data transmission as opposed to in person submissions brings in the question of ***confidentiality, integrity, authentication*** and ***repudiation.***

1.3. **Research Objectives**

The study aims at investigating how various government entities and multi-stakeholder organizations manage the leap from physical files to digitized flow of information in a secure manner.

The main **objectives** of this research are:

i. To identify security threats of e-government.

ii. To develop a prototype that uses Public Key Infrastructure in cryptography for verification of documents emanating from the courts.

iii. To evaluate court users satisfaction in the existence of a court documents verification mechanism.

1.4. **Research Questions**

The research questions are:

i. What are the possible security threats to data transmitted electronically in and out of the Judiciary?

ii. How can we leverage of Public Key Infrastructure to ensure integrity, authenticity and non-repudiation in e-government systems?

iii. What are the confidence levels by the system users on incorporation of Public Key Infrastructure?

1.5. **Justification**

Security is one of the key success factors for e-government (Tri Kuntoro, 2017). Electronic signatures and identity verification which are implemented through public key cryptography is also identified as one on the good practices in courts automation and have been adopted by courts in Estonia, the United States, the United Kingdom, Malaysia, Singapore and Korea (Heike et al, 2016). This study will contribute to the ensuring of enhanced document security in and out of the courts using public key encryption ensuring *Confidentiality, Integrity, Authentication* and *Non-repudiation*.This can be scaled according to other areas of e-government.

1.5.1. Importance to computer science

The ability to use a software system to deal with factors that lead to possibilities of incorrect transmission of data from the courts will be a measure of success for this research. Given the diverse nature of perceived users of the system, ranging from possibility on illiterate, semi-illiterate and the elite, the system must have the ability to serve all these groups optimally. The research will aim at identifying the best platforms to avail the system.

1.5.2. Importance to the Judiciary

The judiciary having been tasked with delivery of justice requires public faith and confidence in the way they carry out the function of justice dispensation. The ability to verify the court documents by court users is key in ensuring that this is achieved.

1.5.3. Importance to the court users and the public

Some times documents from court stand between a person and their life or property. Case in point, court orders are issued every day to stop or authorize demolition of multi-million buildings. A judgment from children’s cases instructs on who the custodian of a child is hence forth. It is only right that the recipients of these documents are able to verify these documents as served.

1.6. Scope of the study

The study will be carried out in the courts in Nairobi that have already established e-filing for court operations. Once cascaded across the country the same will be adopted accordingly.

Chapter 2: Literature Review

2.1. Introduction

The introduction of digital government services comes with security challenges to do with information flowing between different stakeholders of the various systems. There is therefore need to establish ways in which various concepts of security management can be deployed for the success of e-government. This chapter will demystify issues pertaining to e-government, security issues and mitigation factors and the success achieved.

2.2. Information security issues in e-government

As a government avails its services over the internet it should ensure a balance of convenience, access availability and protection of all data affecting its citizens (S Benabdallah et al, 2002). They identify the use of PKI enabled services such as digital signatures and encryption and other security mechanisms such as firewalls, intrusion detection and network security protocols as the way to go. In their proposed e-government model, one of the tasks specially highlighted is the setting up of a PKI which includes the development of a secure Certificate Practice Statement, security auditing techniques and secure PKI platforms. It provides for security services such as confidentiality, authentication, integrity and non-repudiation.

Rasim & Farhad, 2015, state that with increased computerization, non-provision of security services may have negative effect on a people consuming e-government services. They reiterate on the need to ensure that all data is protected from unauthorized access and also mention five broad requirements of information security in e-government which are *confidentiality, integrity, availability, authenticity* and *accountability*

2.3. **Cryptography**

Cryptography is the science of keeping information secure by transforming it into a form in which unintended recipients cannot understand. Rao and Nayak (2014) define cryptography as the process in which a message originally intended to be deciphered by humans usually in *plaintext* is subjected to algorithms or mathematical operations and converted to non-human readable text known as *ciphertext.*

2.3.1. **Symmetric Key Cryptography**

This is also known as secret key cryptography in which users use a shared key to share encrypted data. It involves the following concepts: *Plaintext* which is the original message to be transmitted, the symmetric key *algorithm,* a *shared secret key* between the data sender and recipient and the *ciphertext* which is the encrypted message that can't be read.

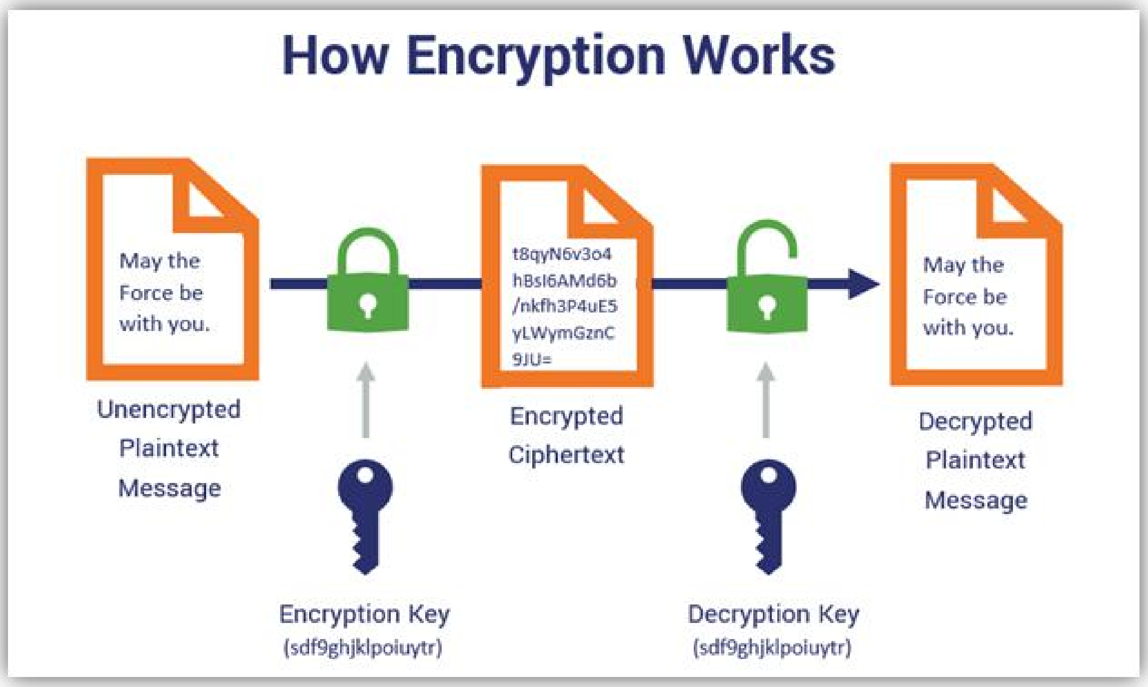

How Encryption Works
May the Force be with you.
Unencrypted Plaintext Message
t8qyN6v3o4 hBsI6AMd6b /nkfh3P4uE5 yLWymGznC 9JU=
Encrypted Ciphertext
May the Force be with you.
Decrypted Plaintext Message
Encryption Key (sdf9ghjklpoiuytr)
Decryption Key (sdf9ghjklpoiuytr)

Figure 1: How Encryption works: symmetric Key Cryptography (Casey, 2020)

Symmetric Key algorithms

Data Encryption Standard (DES) — It is a block cipher that encrypts data in 64-bit blocks and using a single key that is either either 64-bit, 128-bit and 192-bit in size. In each of these, 8 bits is a parity bit, meaning that a single-length key that's 64 bits is really like using a 56-bit key.Its since been deprecated and termed as insecure.

Triple Data Encryption Standard (TDEA/3DES) —It can use two or three keys, enabling it use multiple rounds of encryption (or, more accurate, a round of encryption, round of decryption, and another round of encryption). 3DES is more secure than DES.

Advanced Encryption Standard (AES) — This is the most commonly used in the internet. It is way secure and efficient than DES and 3DES with key options that are 128 bits, 192 bits and 256 bits.

The strength of these keys depends on the length of the key, the randomness of generation and the time taken to reverse the key to gather the original components.

The main challenge of symmetric key cryptography is key exchange since a similar key has to be known secretly by the sender and the recipient. Transmission of the key is susceptible to man-in-the-middle attack which has since been addressed by the adoption of asymmetric key exchange protocols like RSA and Diffie Hellman

2.3.2. Asymmetric Key Cryptography

This is also referred to as public key cryptography. These algorithms use key pairs: public keys which are known to everyone in the ecosystem and private keys which are only known to the owners.

Different keys are used for encryption and decryption of data. Public key cryptography is mainly applied in the following areas: **Encryption** whereby data is encrypted using an individual's public key and is decrypted with the their private key only. **Digital signatures** where data is signed using an individual's private key and can be verified using their public key.

How it works:

Each user generate a pair of keys where by the public key is placed on the public register for easy access by all. The private key is kept private.

If A wishes to send a message to B, it encrypts the message using B’s public key who when in turn receives is able to decrypt using their private key. Let the plaintext be X=[X1, X2, X3, …,Xm] where m is the number of letters in some finite alphabets.

Suppose A wishes to send a message to B.

B generates a pair of keys: a public key KUb and a private key KRb. KRb is known only to B, whereas KUb is publicly available and therefore accessible by A.

With the message X and encryption key KUb as input, A forms the cipher text Y=[Y1, Y2, Y3, … Yn]., i.e., Y=E KUb(X)

The receiver can decrypt it using the private key KRb. i.e., X=D KRb(). The encrypted message serves as a digital signature. With this confidentiality is achieved as long as KRb is kept private to B. However; Authentication, integrity and Non repudiation are not guaranteed.

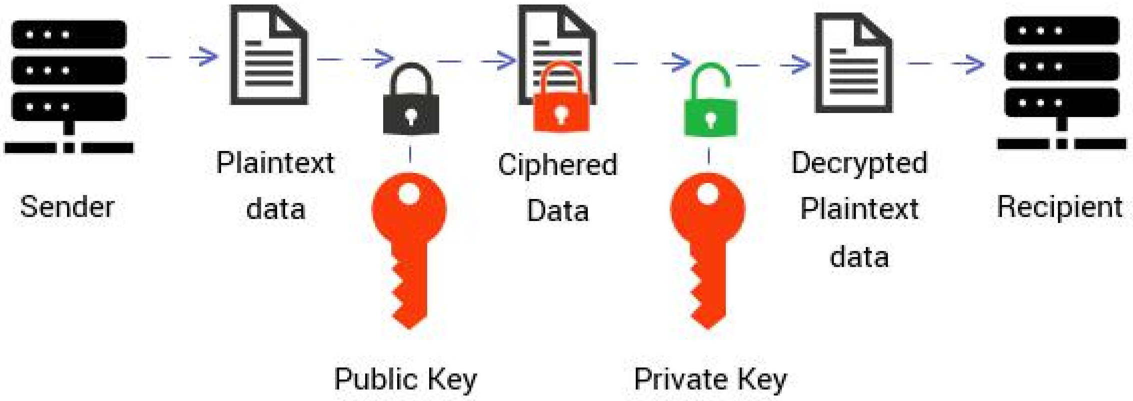


Figure 2: Public Key Cryptography

The following are the algorithms used in public key encryption:

i. **RSA** One of the first public-key schemes was developed in 1977 by Ron Rivest, AdiShamir, and Len Adleman.

ii. **Diffie-Hellman Key Agreement** The first published public-key algorithm appeared in the seminal paper by Diffie and Hellman that defined public key cryptography. The algorithm itself is limited to the exchange of the keys.

iii. **Digital Signature Standard The DSS**, published by the National Institute of Standards and Technology (NIST) makes use of SHA-1 and presents a new digital signature technique, the Digital Signature Algorithm (DSA). The DSS uses an algorithm that is designed to provide only the digital signature function. Unlike RSA, it cannot be used for encryption or key exchange.

iv. **Elliptic Curve Cryptography (ECC)** The principal attraction of ECC compared to RSA is that it appears to offer equal security for a far smaller bit size, thereby reducing processing overhead.

To ensure effectiveness of the use of these key pairs, it is important to have proof that the public key is authentic and hasn’t been tampered with. This is achieved by having a public Key Infrastructure whereby third parties know as *Certificate Authorities* as tasked with certification of key pairs

2.3.3. Public Key Infrastructure

This is a set of roles, policies, and procedures needed to create, manage, distribute, use, store and revoke digital certificates and manage public-key encryption. This regulates and controls secure operations of exchange of information based on asymmetric key cryptography

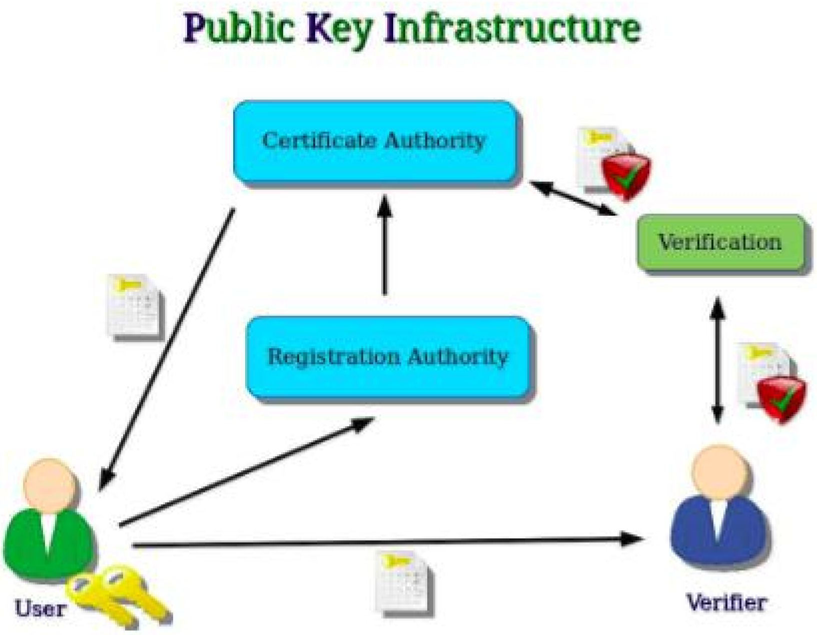


Figure 3: Public Key Infrastructure

Certificate Authorities (CA): This is a trusted third party that validates a person’s identity. The CA then generates a public, private key pair for them and associates an existing public key provided by the person to themselves. Upon validation of an identity, the CA issues a signed digital certificate. The digital certificate is used to verify a person associated with a public key when requested. The CA is also tasked with renewal and revocation of these certificates.

Registration Authority: This is an organization that receives and validates user requests for digital certificates. Upon reception of these requests,it verifies the identity using acceptable forms of identification like National ID or Driving License. The RA then contacts the CA in the PKI to issue a digital certificate and the key pair.

End users and devices: These are entities within the PKI that seek to attain or verify digital certificates.

Digital Certificates: It is important to guarantee the security of public keys. A mechanism is required which binds the public key with some globally trusted party that can ensure the identity and authenticity of the public key and should provide for establishment of the integrity of the public key and should also bind the public key and its associated information to the owner in a trusted manner. Digital certificates accomplish these goals. Certificates ensure that only the public key for a certificate that has been authenticated by a certifying authority works with the private key possessed by an entity. This eliminates the chance of impersonation.

A certificate includes the following elements: serial number of the certificate, digital signature of the CA, public key of the user to whom the certificate is issued, expiration date and the name of the CA that has issued the certificate.Upon obtaining the digital certificate,the entity can use it to communicate with recipients of information in the by:

i. The sender signs the message digitally with their private key to ensure message integrity and its own authenticity, sends the message to the recipient.

ii. The recipient, on message reception, verifies the digital signature with the subscribers public key and validates the senders digital certificate it by querying the global directory database

iii. The global directory database returns the status of the subscribers digital certificate to the recipient after which the transaction is completed if the certificate is valid.

The CA signs the digital certificates. To verify a signature, the CAs public key which is part of the CA’s digital certificate is needed. These certificates are usually pre-installed in web browsers. Upon issuance of a certificate, it is distributed to users and organizations by a Certificate Distribution System (CDS) or a repository.

Certificate Distribution System (CDS): It distributes certificates to users and organizations. Certificates can either be distributed by the user or distributed by a directory server that uses LDAP to query the user information stored in an X.500 compliant database. It is used to generate key pairs, certify validity of public keys by signing them, revoking expired or lost keys, publishing keys in the directory service server.

Certificate Revocation Lists: This is a list of digital certificates that have been revoked by the CA usually before they are expired. They therefore cannot be trusted. There are two states of revocation: *Revoked* and *Hold.* ***Revoked*** status is attained when the CA improperly issues a certificate or when a private key has been compromised or if the certificate owner violates stipulated CA's policy. ***Hold*** is attained temporarily when the user is not sure if the private is still private.The certificate can be reinstated if the key if found and no threat had gotten to it. These revocation lists are published periodically and are accompanied by the signature of the corresponding CA to ensure validity.

Below is an illustration of interaction of various players within the public key infrastructure:

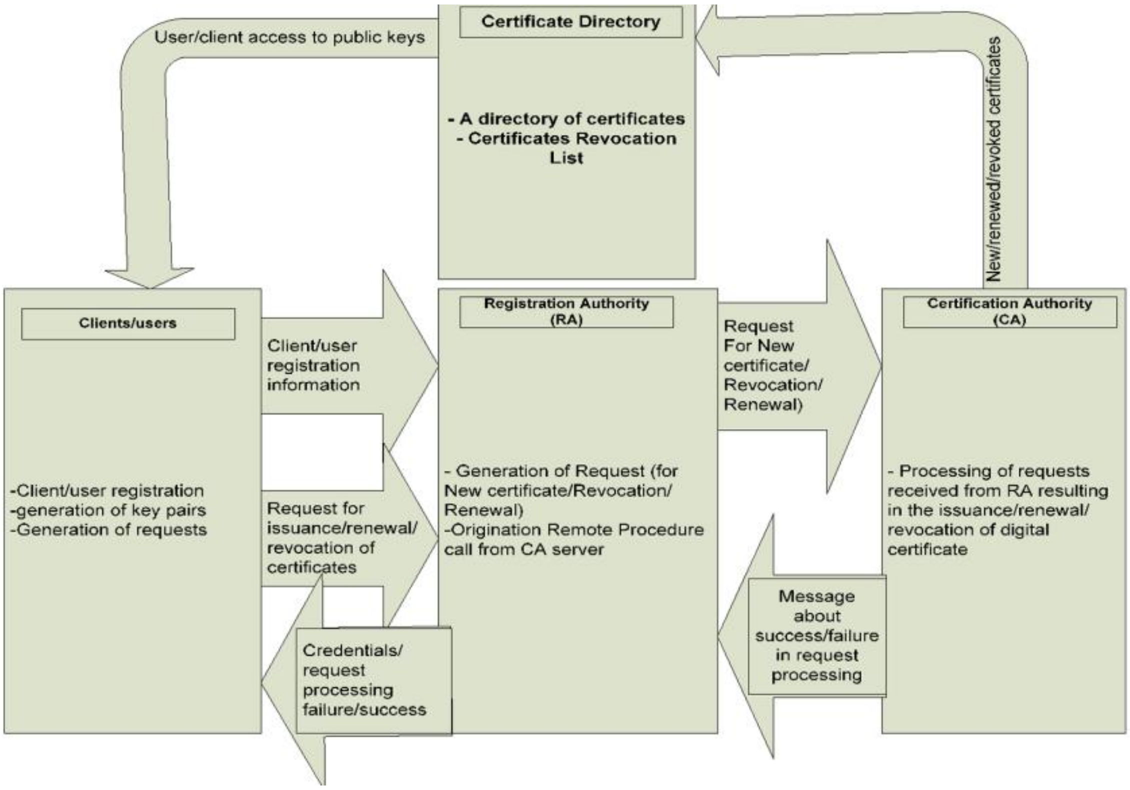

User/client access to public keys
Certificate Directory
- A directory of certificates
- Certificates Revocation List
New/renewed/revoked certificates
Clients/users
-Client/user registration
-generation of key pairs
-Generation of requests
Client/user registration information
Request for issuance/renewal/ revocation of certificates
Credentials/ request processing failure/success
Registration Authority (RA)
- Generation of Request (for New certificate/Revocation/ Renewal)
-Origination Remote Procedure call from CA server
Request For New certificate/ Revocation/ Renewal)
Message about success/failure in request processing
Certification Authority (CA)
- Processing of requests received from RA resulting in the issuance/renewal/ revocation of digital certificate

Figure 4: Interaction of entities within the PKI (Agangiba et al, 2013)

The key reasons for adoption of PKI are:

i. **Confidentiality**: Unauthorized access of data is prevented by use of ***encryption***

ii. **Integrity**: Data should not be modified during storage or transmission. This is achieved through ***hashing*** which is a process in which a message digest based on the entire message is generated. If the original data is changed, the digest changes hence modification can easily be detected.

iii. **Authentication**: genuine users are identified by the ***digital certificates*** issued by certificate authorities

iv. **Non-repudiation**: A user cannot later deny being the origin of a message. This is achieved by use of ***digital signatures.***

While public key solves the problem of key passing, by the possession of the 2 keys (private and public), it is slow in computation and there is difficulty in ascertaining the real ownership of the public key hence prone to impersonation attacks. However this is solved the the involvement of a third party in the CA which issues and verifies the keys.

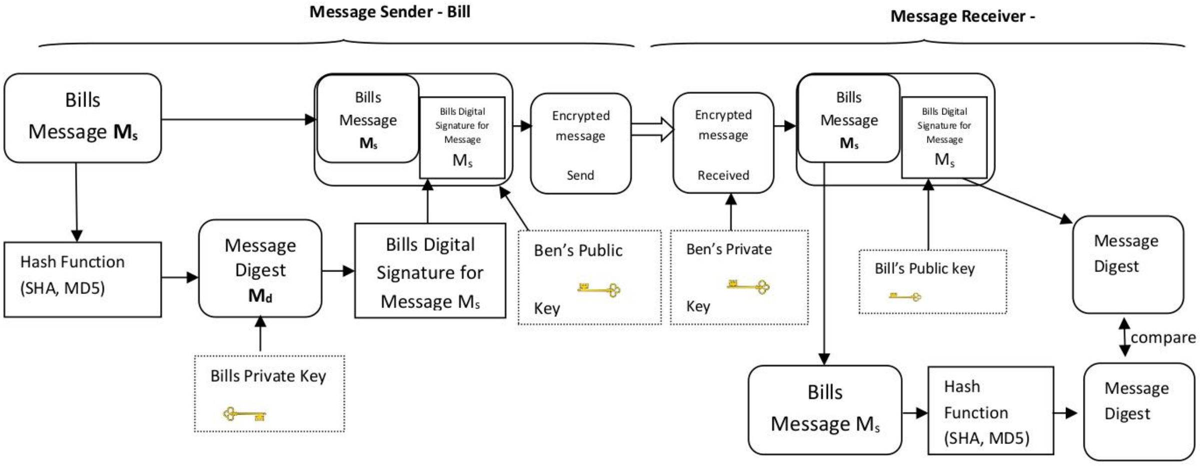


Figure 5: Digital signatures design (Source: Choudhury et al., 2002 through Geoffrey, 2012)

2.3.4. Pretty Good Privacy (PGP)

Pretty Good Privacy is an encryption program that provides cryptographic privacy and authentication for data communication. It is used for signing, encrypting, decryption of texts, e-mails, files, directories and whole disk partitions. It is also used to increase the security of e-mail communications.

In relation to digital signatures, PGP supports message authentication and checking of integrity. Integrity check are used to determine if any alteration of the original message has been done, while authentication is done to determine whether the message was actually sent by the person who claimed to be the sender by way of digital signature. Since the message is is encrypted, changes in the message will fail the decryption with the appropriate key. The sender uses PGP to create a digital signature for the message with either the RSA or DSA algorithms. To create a digital signature, PGP computes a message digest from the original plain text and then creates the digital signature from that hash using the sender's private key.

2.4. The government of Kenya’s digitization journey

In the Kenya e-government strategy of 2004 (Cabinet Office of the President, 2004), an outline of objectives and processes for the modernization of Government is well articulated. The plan was to leverage on the use of internet to enhance transparency, accountability and good governance making the Government more result oriented, efficient and citizen centred. The outlined processes would also enable citizens and business to access Government Services and Information as efficiently and as effectively as possible. Kenya envisioned to roll out as many functions online some of which are digitized records management like registration of persons via the Integrated Population Registration Service, Lands and Motor Vehicle registration. Services like automated government returns and claims, e-procurement, land search and registration, motor vehicle inspection booking and driving licence management have since taken shape. All these are linked to e-payment gateways to facilitate online payments that is convenient.

2.5. The Judiciary of Kenya

The Judiciary of Kenya is one of the arms of government established under chapter 10, article 159 of the constitution of Kenya. As such, it is mandated with a number of functions that are:

i. Administration of justice

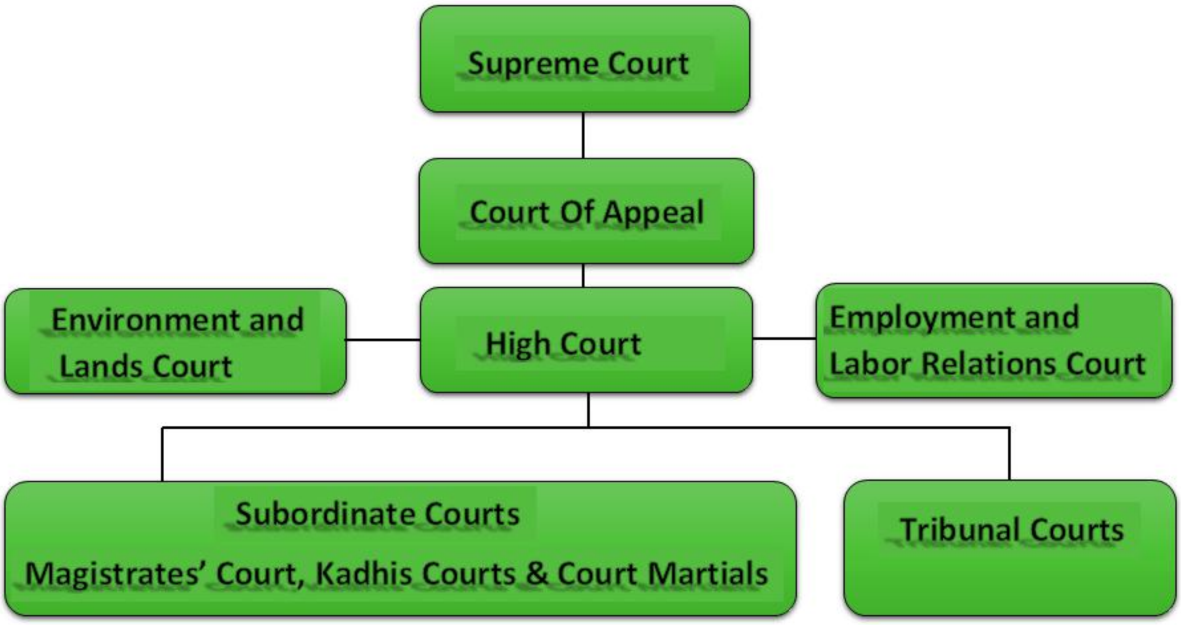
ii. Formulation and implementation of judicial policies

iii. Compilation and dissemination of case law and other legal information for the effective administration of justice

The Judiciary as is known to the citizenry of a country is an institution in which disputes that need interpretation or application of the preset laws of a country are handled and justice meted out to the parties involved in the case.

2.5.1. The court structure

The judiciary comprises of various courts of different ranks, some of which offer specialized litigation. Below is a diagram that shows the courts ranking in Kenya:



Supreme Court
Court Of Appeal
Environment and Lands Court
High Court
Employment and Labor Relations Court
Subordinate Courts
Magistrates' Court, Kadhis Courts & Court Martials
Tribunal Courts

Figure 6: Structure of courts in Kenya

The supreme Court handles presidential election petitions, advisory opinions related to matters on county governments and appeals from the Court of Appeal and special tribunals as is defined by the law.

The court of appeal handles matters arising from decisions made by High Court judges and tribunals.

The High Court is tasked with handling all civil and criminal cases as well as appeals from the magistrate courts. Matters are handled based on the following divisions: Family, Commercial and Tax, Criminal, Civil, Constitution and Human Rights, Judicial Review, Anti-corruption and economic crimes.

The Environment and Lands Court handles matters related to land and environment while Employment and Labour Relations Court deals with matters related to employee rights and conditions.

Magistrates Court deals with the majority of matters in the country. They listen to all criminal matters except treason, murder and crimes under international criminal law. They also handle all civil cases for which they have jurisdiction.

Kadhis Courts deal with cases such as family and succession, cases on marriage, divorce and inheritance where those involved are Muslims

Court Martial deals with cases whose parties are people serving in the military

Tribunals are bodies established by various acts of parliament to supplement the courts in justice administration. Examples are Rent Restriction Tribunal, Sports Disputes Tribunal etc.

2.5.2. Digitization of the Kenyan Judiciary

In the same breath as the national strategy of moving towards e-solutions, The Judiciary of Kenya that is one of the arms of government published the Judiciary Transformation Framework (JTF) (2012-2016). This is a document that outlines the strategy put in place to transform a then ailing Judiciary. It outlined four pillars whereby the fourth one is *Harnessing Technology as an enabler for Justice* and sought to achieve the following:

Establish an electronic Case Management System with SMS capability for case status search

Digitization of court records

Install teleconferencing facilities.

Mainstream the use of electronic billboards in the courts.

Establish an integrated personnel and payroll system.

Digital recording of proceedings and transcription.

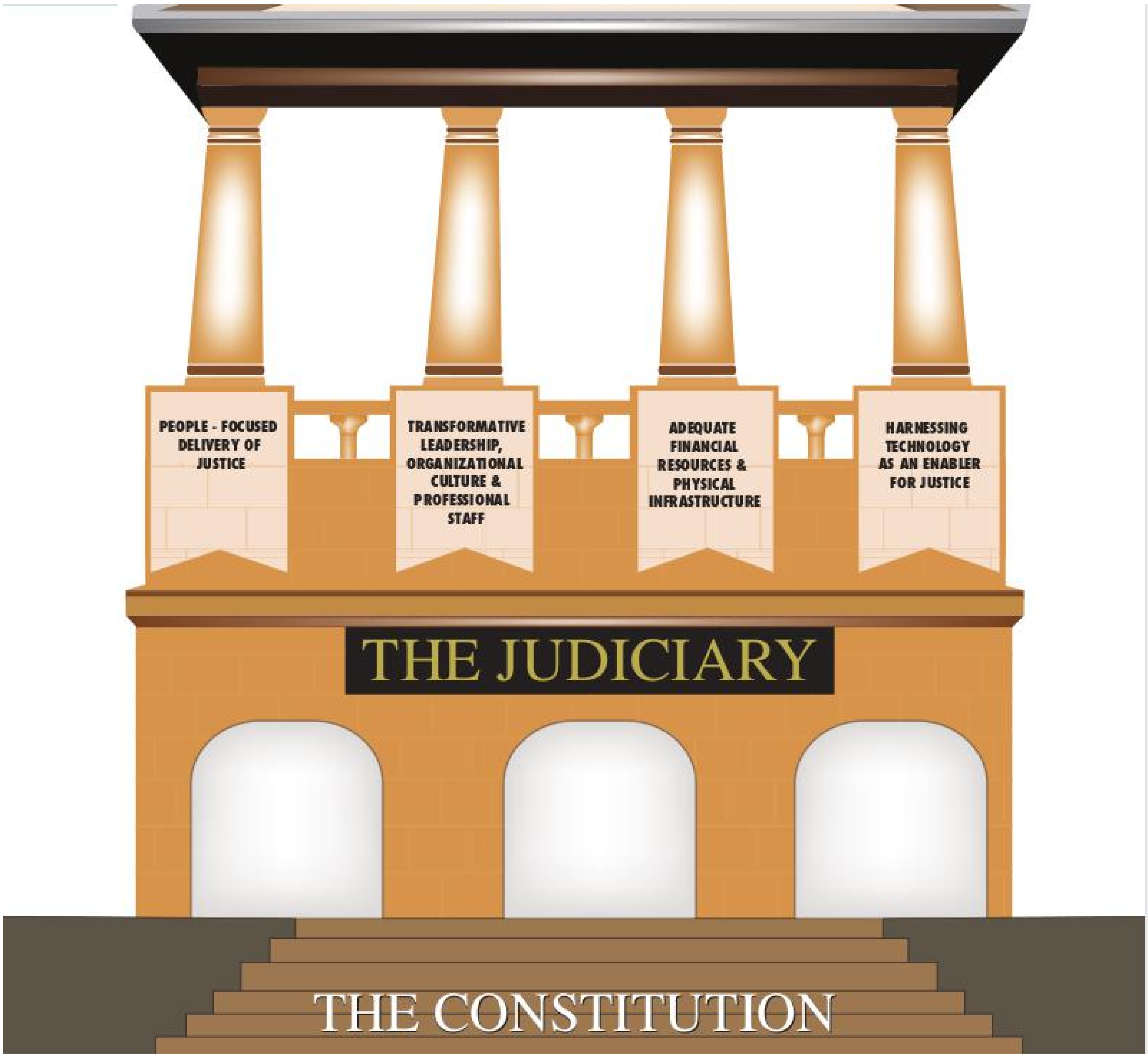

PEOPLE - FOCUSED DELIVERY OF JUSTICE
TRANSFORMATIVE LEADERSHIP, ORGANIZATIONAL CULTURE & PROFESSIONAL STAFF
ADEQUATE FINANCIAL RESOURCES & PHYSICAL INFRASTRUCTURE
HARNESSING TECHNOLOGY AS AN ENABLER FOR JUSTICE
THE JUDICIARY
THE CONSTITUTION

Figure 7: The Judiciary Transformation Framework (2012-2016)

The need to automate was clearly spelt out in the document. This laid the foundation for automation which aptly began in 2016 with the Case Tracking System.

In the succeeding document that is Sustaining Judiciary Transformation (SJT) (2017-2021), the automation agenda is maintained in chapter 5 which is *The Digital Strategy.* It seeks to measure the automation quick wins outline by the JTF and proposes on scaling of the initiated projects. Case in point was rolling out of the Case Tracking System (CTS) and e-fling system in the Commercial and Tax Division of Milimani High Court. This has since been achieved with the establishment of the CTS in all courts and e-filing in all Nairobi Courts.

In the wake of SARS-CoV-2 (COVID-19), accelerated adoption of the internet to transmit documents to and from the Judiciary. With this comes threats on integrity and authenticity of data. It is therefore imperative that this institution must embrace security mechanisms to ensure data security. Litigants must be sure that court orders, judgments and rulings and other court documents are valid and can be trusted.

Establishment of a public Key Infrastructure model to enable encryption and the use of digital signatures is considered very effective in creating a web of trust in all players within a data transmission ecosystem

Electronic Case Management

In order to present matters before the court for litigation, parties through their advocates or through self are required to present standard documents to the court. This is done at registries spread across all court stations in the country. Here, requisite fees by document are assessed and corresponding physical court files opened upon payment. These files are then presented to the Judicial Officers (Judges and Magistrates) for hearing and determination. Subsequent filing of documents may be done by the litigants by request of the court or as moved by the parties as the case progresses. The court also appends its own documents which are proceedings (parties, advocates and witnesses counts as captured the judicial officers in court that are initially handwritten and eventually typed), orders, rulings, judgments etc. The files are then stored in large cabinets and are retrieved based on the court calendar.

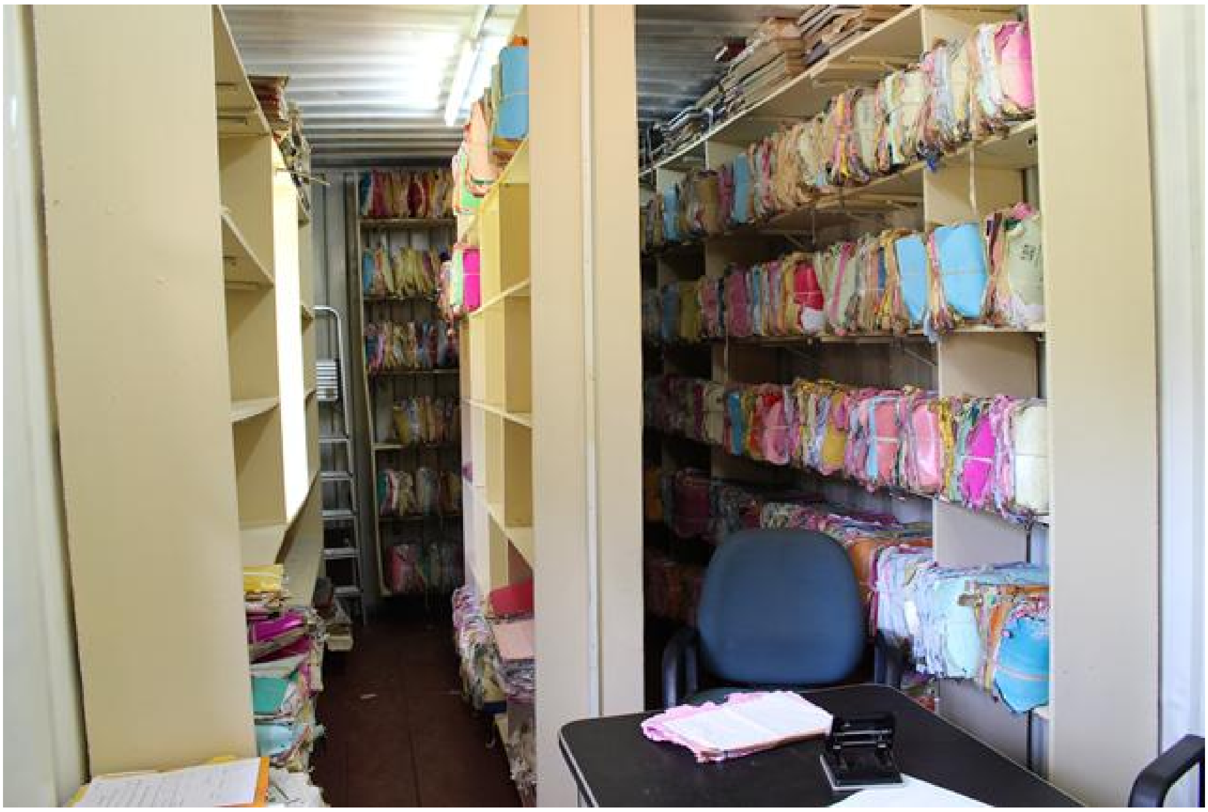
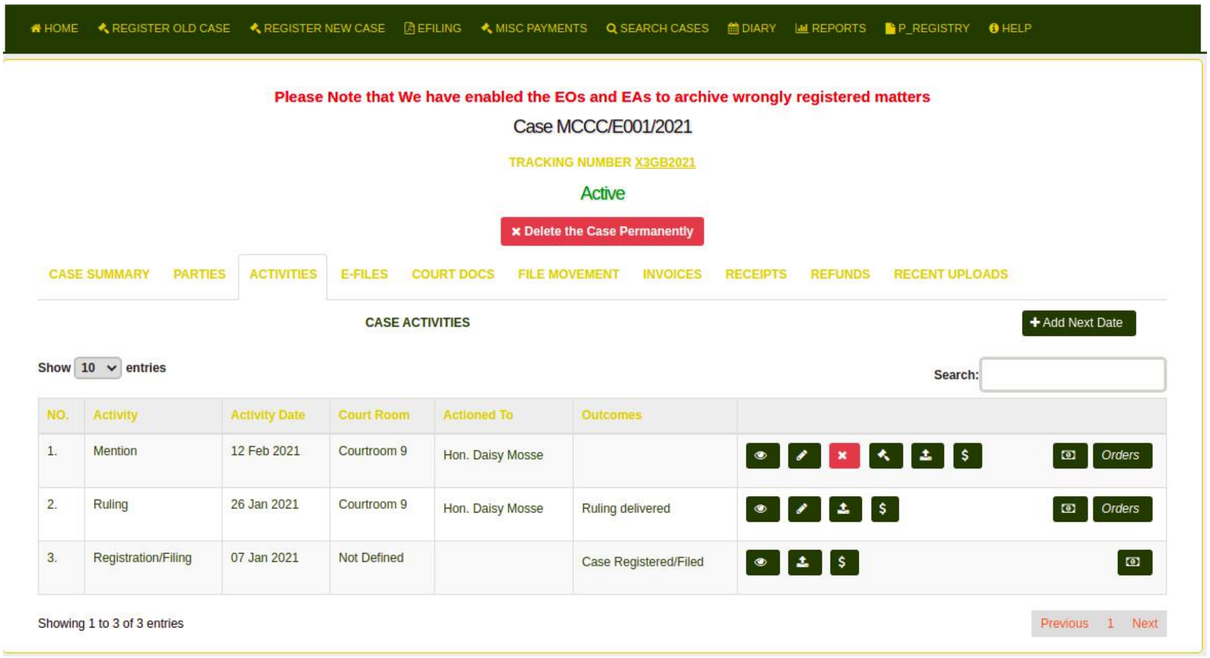


Figure 8: Filing cabinet in the courts

In 2017, the Judiciary set out to automate the registry process of case registration, fees assessment, court calendaring, documents digitization and reporting. A web based application referred to as the "*Case Tracking System (CTS)"* was developed handle this laid out functionality. CTS is a registry (back office) operated system that eases the work of the registry. The system however was an under-utilized feature that is the handling of documents that are brought to court and those generated by the registry and the court. Lack of a clear legal framework around the format in which documents were submitted to court contributed to this hiccup. The law then did not obligate people seeking litigation to submit their documents in soft copy format. It was very difficult for the judiciary staff therefore to scan and upload the documents as presented. Efforts however were made through rapid results initiatives and outsourcing of the digitization but given the magnitude of files over the years, this was hardly adequate. There are plans to keep digitizing until 100% digitization is achieved.



Please Note that We have enabled the EOs and EAs to archive wrongly registered matters

Case MCCC/E001/2021

TRACKING NUMBER X3GB2021

Active

CASE ACTIVITIES

Show 10 entries

Search:

NO.	Activity	Activity Date	Court Room	Actioned To	Outcomes
1.	Mention	12 Feb 2021	Courtroom 9	Hon. Daisy Mosse	
2.	Ruling	26 Jan 2021	Courtroom 9	Hon. Daisy Mosse	Ruling delivered
3.	Registration/Filing	07 Jan 2021	Not Defined		Case Registered/Filed

Showing 1 to 3 of 3 entries

Figure 9: The Judiciary of Kenya Case Tracking System

Following the success of the internal case management system, a public facing portal of CTS was developed and referred to as the *"e-filing system" and is available at efiling.court.go.ke* . This system was first piloted in the High court at Nairobi's Commercial and Tax Division in 2018 with 5 law firms and eventually for everyone filing in that division. The system ran successfully until February 2020.

In the wake of SARS-CoV-2 (COVID-19) that was announced in Kenya on 13th March of 2020 (Ministry of Health, 2020), the Judiciary through a press statement (The Judiciary, 2020) by the Chief Justice of Kenya, Hon. Justice David Maraga scaled down operations within the court premises. All in person operations were halted which included manual filing of documents. This necessitated the scaling up of the e-filing system which was eventually rolled out for all Nairobi courts which are: The Supreme Court, The Court of Appeal, Milimani High Court, The Environment and Lands Court at Nairobi, The Employment and Labour Relations Court at Nairobi, Milimani Magistrates and Milimani Chief Magistrates Court, Kibera Law Court and Makadara Law Court. Other courts in all other parts of the country were also only expected to receive their documents in soft copy via designated email addresses. The e-filing system offers the following services:

electronic filing and electronic service of court documents

electronic case search

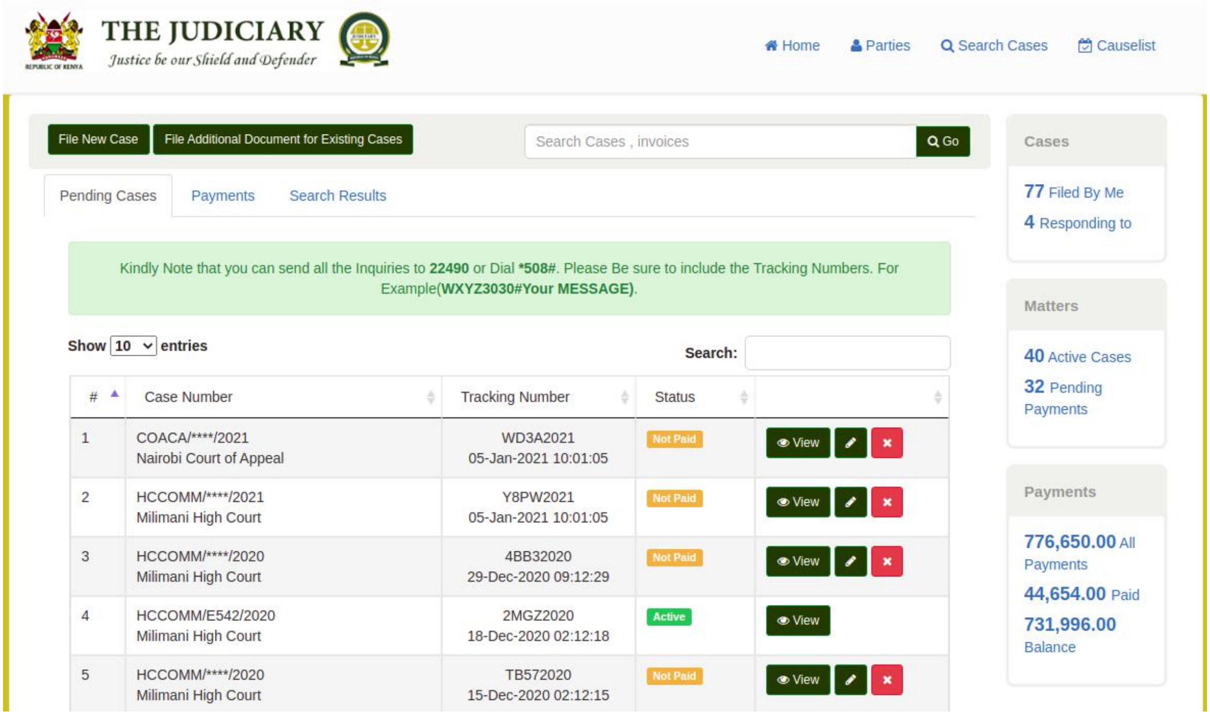
electronic diary

electronic case tracking system

electronic payment and receipting

electronic stamping

exchange of electronic documents, including pleadings and statements



THE JUDICIARY
Justice be our Shield and Defender

Home | Parties | Search Cases | Causelist

File New Case | File Additional Document for Existing Cases | Search Cases , invoices | Go

Pending Cases | Payments | Search Results

Kindly Note that you can send all the Inquiries to **22490** or Dial ***508#**. Please Be sure to include the Tracking Numbers. For Example(**WXYZ3030#Your MESSAGE)**.

Show 10 **entries** **Search:**

#	Case Number	Tracking Number	Status	
1	COACA/****/2021 Nairobi Court of Appeal	WD3A2021 05-Jan-2021 10:01:05	Not Paid	View
2	HCCOMM/****/2021 Milimani High Court	Y8PW2021 05-Jan-2021 10:01:05	Not Paid	View
3	HCCOMM/****/2020 Milimani High Court	4BB32020 29-Dec-2020 09:12:29	Not Paid	View
4	HCCOMM/E542/2020 Milimani High Court	2MGZ2020 18-Dec-2020 02:12:18	Active	View
5	HCCOMM/****/2020 Milimani High Court	TB572020 15-Dec-2020 02:12:15	Not Paid	View

Cases
77 Filed By Me
4 Responding to

Matters
40 Active Cases
32 Pending Payments

Payments
776,650.00 All Payments
44,654.00 Paid
731,996.00 Balance

Figure 10: The Judiciary e-filing system in Kenya

2.6. **PKI Enabled e-government initiatives**

The term e-Government is described as the use of ICTs to provide services online. It is aimed at increasing efficiency and effectiveness in service delivery. On these initiatives, interaction between the government, the public, businesses, organizations and institutions is made possible via the digital space. According to Agangiba et al, 2013, three major aspects enforced by the e-model of government are automation of routine government tasks, enabling government functions on web to allow direct citizen access and improving government processes to enhance openness, accountability, effectiveness

In the application of these ICTs, the questions of digital threats to data transmitted across entities come along (Agangiba et al, 2013). Cryptography has therefore been adopted to provide the much needed security model for data to achieve data validity. Below is a diagram that shows the access of data through the PKI.

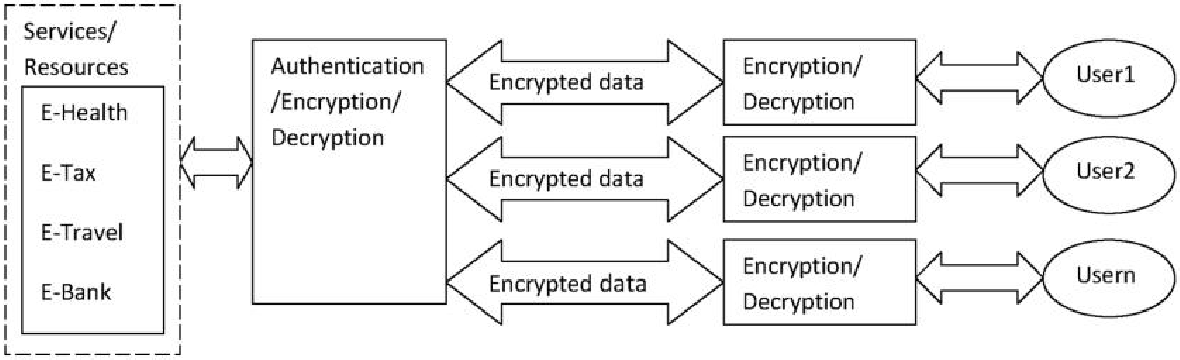


Figure 11: PKI for e-government (Agangiba et al, 2013)

2.6.1. **PKI in Estonia**

Estonia has established a national Public Key Infrastructure whereby the state ensures its availability and correct functionality of government services. Related services like certification, user request infrastructure, public key distribution and generation of the ID card chip is purchased by the private sector. The PKI is achieved by the use of electronic chip cards. The use of this infrastructure is enforced by the Digital Signature Act (DSA) of 2000.

The DSA equates digital signatures to handwritten ones so long as they are unique to the holder and that data signed with it cannot be changed without altering the signature thereby invalidating it. It also emphasizes on time stamping its use.

In 2001, (AS Sertifitseerimiskeskus, 2003) Estonia established an data exchange layer known as X-ROAD riding on this architecture to enable exchange of data between state systems. Citizens are therefore able to access diverse government services accessing different databases while accessing the same channel. An example is transmission of insurance data to the health insurance fund upon valid identification using the digital ID.

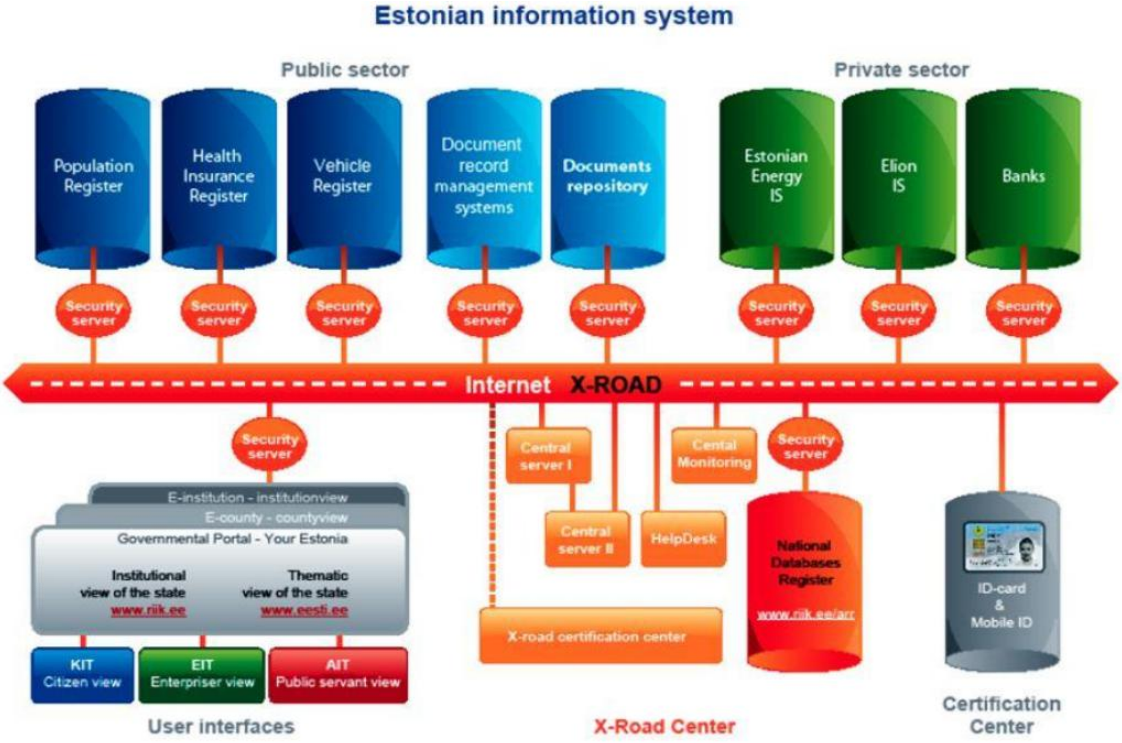


Figure 12: Estonia Information system architecture

E-Health

Estonian health system information system (EHIS) (AS Sertifitseerimiskeskus, 2003.) is a practical application leveraging on this technology. It collects information about patients from different health care provider's portals. All inquiries issued to this system are recorded on account of personal IDs with audit trails well maintained. A digital stamp/ signature is used for all documents to prevent any alterations. The system also employs the use of digital prescriptions that are done entirely online.

Integration of the Population Register and the Estonian Health Insurance Fund via XROAD has seen to various benefits:

i. Cost savings by preventing duplication of data collection registries

ii. Integration of EHIF and EHIS plays a role in social benefits like sick leave. Paperless administration has allowed a more efficient use of resources and time.

iii. Better flow of information on the health system due to use of EHIF and X-road e.g. doctor salaries and hospital reimbursements or claims are managed through the system.

iv. The ID is not just a tool or instrument for patients, but it also serves as an ID for providers (public and private).

v. The use of a unique ID enables the Health Service providers track patients and identify factors affecting quality of care and health outcomes. This also helps in avoiding inefficiencies of fragmented health providers and disruptions due to change of medical providers.

Electronic Land Register

The digital lands register was established to provide a paperless solution and prevent fraudulent transaction of cases. According to Vali et al (2014), all land except that which is state owned is registered electronically. Digital certificates are issued to rightful owners. Land transfers are done through notaries who query the system to verify ownership details. They then prepare digitally signed sale contracts and deeds that are sent to the lands registrar. The registrar ascertains the information and passes it to the judge for registration. The registrar then sends back the decisions to the notaries who update their clients.

Important points to note from the Estonia implementation:

i. It takes time to establish a working system - It took them 15 years to create a successful unified system.

ii. A well articulated legal framework is important as a basis for the initiative

iii. It is important to identify the order of establishment of components that make the environment work i.e. Unique numbering system --> population register --> Digital IDs --> Data exchange channels (X-road)

iv. Importance of interoperability of government databases

v. Focus on processes rather than outcomes.

vi. Importance of service oriented architecture to enable innovation and provide user oriented service.

2.6.2. PKI in India

In the India PKI Forum (https://www.indiapki.org/) the PKI infrastructue in India comprises of the Controller of Certifying Authorities (CCA) which is at the root of the trust chain thereby certifying CAs public keys and issuing their certificates and the Certifying Authorities (CAs). The CCA has established the Root Certifying Authority (RCAI) of India under section 18(b) of the Information Technology Act to digitally sign the public keys of Certifying Authorities (CA) in the country. The Certifying Authorities (CAs) issue digital signature certificates for electronic authentication of users. The forum states the need for PKI is inherent as almost all security controls come down to authentication and access control. Listed are the various applications of PKI in India which are:

Income Tax e-filing

Digital Signature Certificate are used to ensure filing of tax returns is easier and more secure. Mandatory efiling for individuals/professionals and businesses having certain income thresholds is stipulated under revised provisions under section 44AB of IT Act.

Ministry of Corporate Affairs

With the concept of digital certificates, various transactions related to the Ministry of Corporate Affairs, or Registrar of Companies are fully paperless and easy to follow. Organizations can apply for digital signatures for transactions involving these entities

E-Procurement

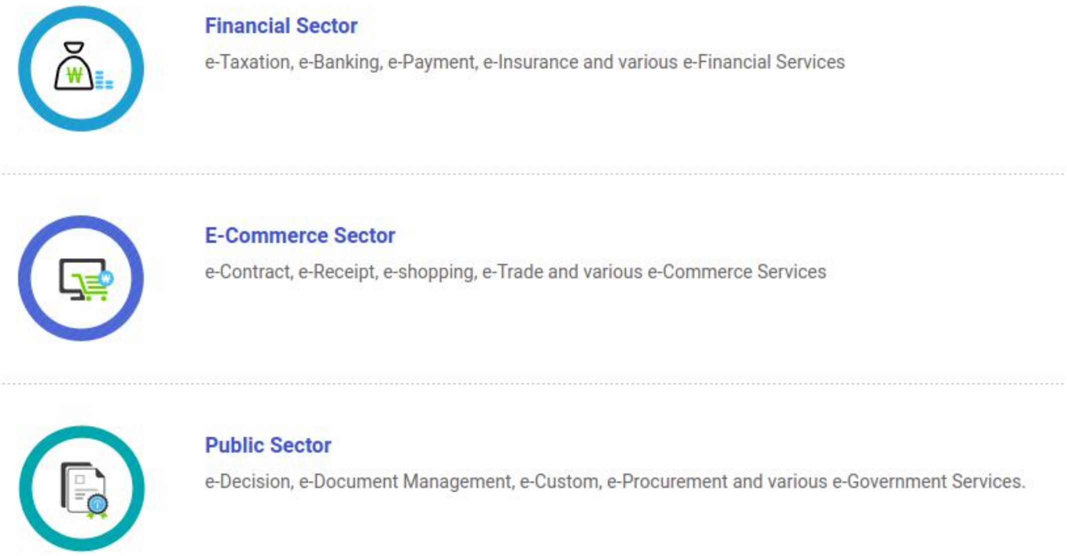
This is an online tender processing system for the state government departments. Digital Signatures are being used by the vendors and government officials for tender submission and processing. The vendors/traders are use it for online tender application, while the government officials use it during tender opening and finalizing.

Voters List Preparation

The State Election Commission issued an order whereby field data and the photo ID are digitized and digitally signed assuring the correctness of data. This data can easily be verified.

2.6.3. PKI in Rwanda

The Root Certification Authority was deployed in 2013 and is managed by the Rwanda Utilities Regulatory Authority (RURA). They have one Government Certification Authority (RGCA) is in place and managed by Rwanda Development Board (RDB).They started issuing digital certificates in e-procurement and over 1000 certificates issued.



Financial Sector

e-Taxation, e-Banking, e-Payment, e-Insurance and various e-Financial Services

E-Commerce Sector

e-Contract, e-Receipt, e-shopping, e-Trade and various e-Commerce Services

Public Sector

e-Decision, e-Document Management, e-Custom, e-Procurement and various e-Government Services.

Figure 13: Applications of PKI in Rwanda

2.7. Current Status of PKI in Kenya

The government of Kenya took the initiative to secure online transactions with the project taking off in 2013. The Communications Authority of Kenya mandated under the Kenya Information Communications Act of 1998 as the Root Certificate Authority to regulate and licence Electronic Certification Service Providers. ICT Authority is identified as the Government Certificate Authority.

The project was rolled out in Kenya Revenue Authority to for user verification but did not take off due to unanticipated logistical issues. Unavailability of the system was cited as the main cause for the flopped project.

2.7.1. The Legal Framework in Kenya

The Kenya Information and Communication Act of 1998 outlines the following in relation to PKI:

i. Licensing of certificate authorities

ii. Responsibilities of a CA

iii. Records management within the PKI

iv. Issuance of certificates

v. Obligations of a subscriber

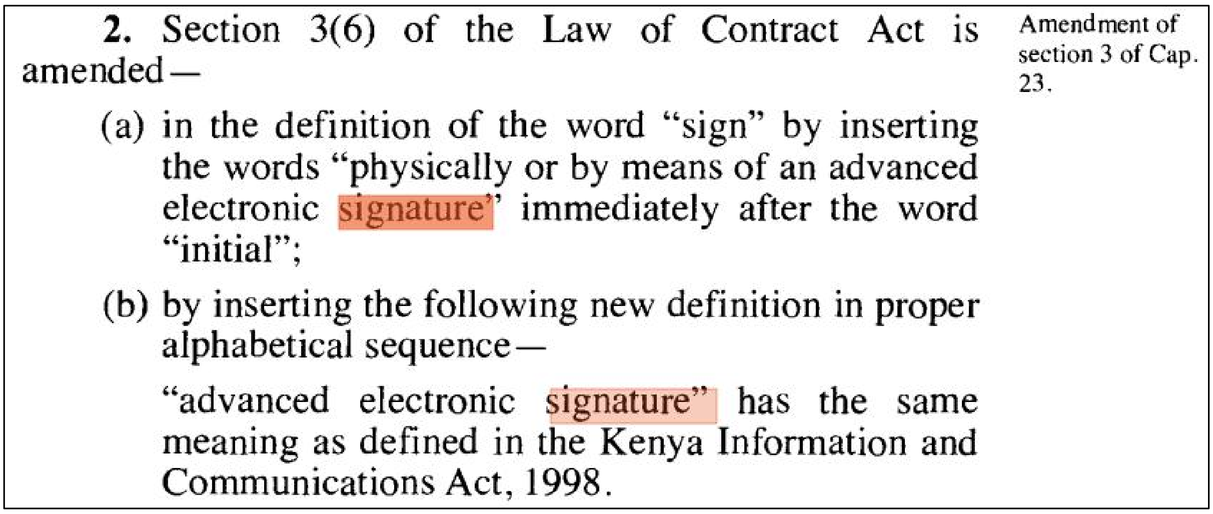
vi. Liability of certification service providers

vii. Renewal, suspension and revocation of certificates

viii. Security guidelines, incident handling and confidentiality among others

The Business Laws Amendment act of 2020 seeks to amend various statutes to facilitate increase in ease of doing business.

i. It identifies a digital signature as form of a sign in various contractual documents



2. Section 3(6) of the Law of Contract Act is amended—

Amendment of section 3 of Cap. 23.

(a) in the definition of the word "sign" by inserting the words "physically or by means of an advanced electronic signature" immediately after the word "initial";

(b) by inserting the following new definition in proper alphabetical sequence—

"advanced electronic signature" has the same meaning as defined in the Kenya Information and Communications Act, 1998.

Figure 14: An excerpt of the definition of the electronic signature in Kenya law (Kenya Gazette Supplement No. 26 (Acts No. 1), 2020)

In the practice directions issued by way of gazette notice 2357 for The Judicature Act (cap. 8) The Civil Procedure Act (Cap. 21), the Chief Justice issued guidelines on electronic case management. Reference is made to the KICA 1998 to define an electronic signature and validate it for use for e-filing.

2.8. **Conceptual Model**

The *conceptual model* aims at creating the following components:

i. Key generation software that will sit within the Judiciary

ii. Registration authority: The existing e-filing system for external users and the case tracking system for judges and magistrates who prepare court documents. This will also include the verification module for documents.

iii. APIs: Document details generated by the case tracking system are transmitted to the EDMS via API

iv. A directory with all digitized court generated documents

v. A key revocation list : This will store suspended and revoked certificates

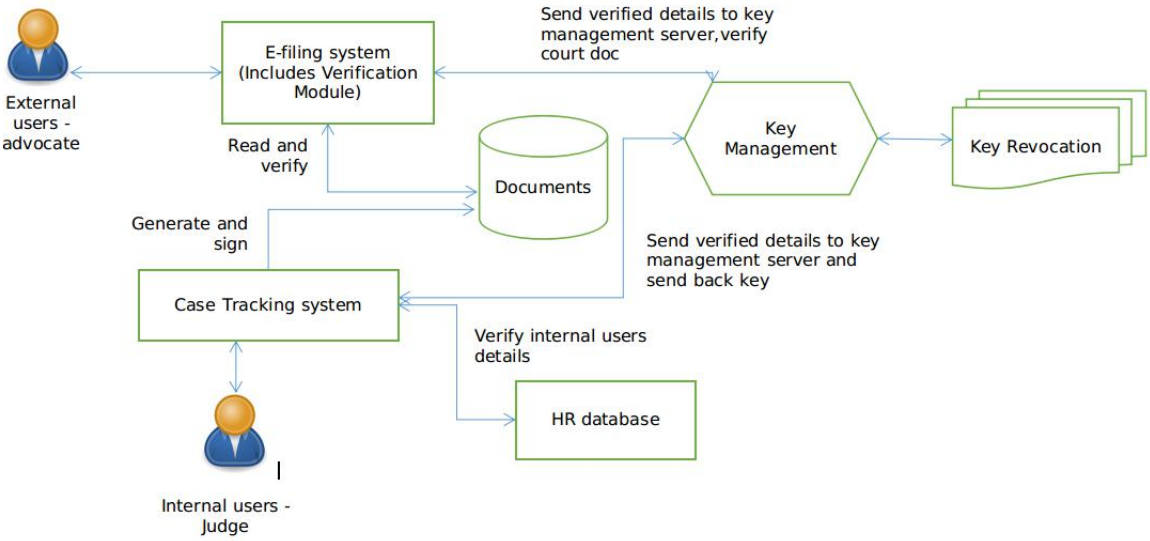

External users - advocate
E-filing system (Includes Verification Module)
Send verified details to key management server,verify court doc
Key Management
Key Revocation
Read and verify
Documents
Generate and sign
Send verified details to key management server and send back key
Case Tracking system
Verify internal users details
HR database
Internal users - Judge

Figure 16: The conceptual model

Chapter 3: Research Methodology

In this section, research methods for this study are described. The ultimate goal of this research study was to design, develop, test, deploy and document a software system that will be used to validate court documents as they are generated by the court and transmitted to the respective audiences.

3.1. Research Design

This study undertook a *qualitative* approach to research in which non-numerical data was collected and analyzed. The key concern was to understand the court process on creation and storage of court documents as well as the gaps in possible means of verification of the same. The research design also embodied a ***design and create*** **strategy** (SWAL Ozan Saltuk & Ismail Kosan , 2014) whose ultimate goal is to create an artifact to solve a detailed problem. The process followed the following guiding principles:

Awareness: Involved the identification and definition of the problem at hand. This was driven by the expression of the need by the court users.

Suggestion: A possible idea on the problem solution was laid out and a digital signatures riding on PKI identified as a possible intervention

Development: A software methodology was identified to develop the proposed solution, Models such as UML diagrams, use cases were generated in the design phase to guide the coding phase. The software environment was set up and the applications developed

Evaluation: Test cases were developed to determine how well the system works and addresses the initial problem. Metrics to measure success were laid down and evaluated

Conclusion: The write up was done and the appropriateness of the solution documented. The principles around the solution are then justified accordingly

The process involved the designing, development, implementing and testing of a court documents validation system having the following components:

Key generation software: Linux OpenPGP software- passwords and keys

Electronic Document Management System: Mayan v 3.8

Postgres database

Web based application with modules to electronically create and sign the documents and a verification module

Research Objective	**Research strategy**
To identify security threats of e-government.	Desktop literature review Questionnaires issued to relevant players
To develop a prototype that uses Public Key Infrastructure in cryptography for verification of documents emanating from the courts.	A modular web based solution was developed based on user oriented requirements
To evaluate court users satisfaction in the existence of a court documents verification mechanism.	A survey to establish users' satisfaction levels will be conducted.

Table 1: Research Strategy

3.2. Data Collection

Data collection was done differently for different user groups in the justice sector. A qualitative approach was used to collect data. The questionnaires are found as appendix 1. The table below shows the various groups of study and the corresponding data collected from each group.

User Group	**Data Collection Techniques**	**Rationale**
5 Judicial Officers	Interviews and questionnaires	Collect views on their confidence levels on whether documents that they generate for public users are consumed in their original form.
10 advocates	Questionnaires	Collect views on their trust on the integrity and authenticity of court documents.
Documents Review		Gather knowledge on similar or related work done in the past.

Table 2: Data Collection

3.3. Location

This study was carried out in the high court and the magistrate's court at Milimani Law Courts in Nairobi. This is due to ease of access as well as the ability to replicate the solution across all courts in the country given to the similarity in structure and operations. The researcher was able to clearly explore the court process on generation of statutory and administrative documents. Ease of access to the Judicial officers greatly influenced the understanding and conceptualization of the developed solution. Advocates within the Nairobi region were also easy to reach and get their views on the gaps in verification of court documents.

3.4. Population

A research population is generally a large collection of individuals or objects that is the main focus of a scientific query. The *accessible population* are those individuals that the researcher is able to reach for the survey. In this study, the researcher aimed at reaching Judges and Magistrates as well as Advocates within the High Court and the subordinate courts in Nairobi, Milimani Law Courts.

3.5. Sample Size

Probability sampling was used by sending the Google form links via Whats-app groups (JOs and Advocates) to ensure non-bias and randomness of the sample population. Pre-Implementation responses were received from 24 advocates and 20 Judicial officers.

3.6. Software Methodology

This section of the methodology shows software engineering best practices methodologies and conventions observed for planning, creating, testing, and deploying the ICT intervention aimed generation and verification of court documents. This section defines the elements of the solution such as the architecture, modules and components, the different interfaces of those components and the data that goes through the solution. This achieves the needs of the organization through a well established and elaborate system.

The method employed for study is the waterfall model which is a stepwise approach to designing, development and testing of the system. This involved getting all the requirements right at the beginning of the process and subsequent development of the proposed solution

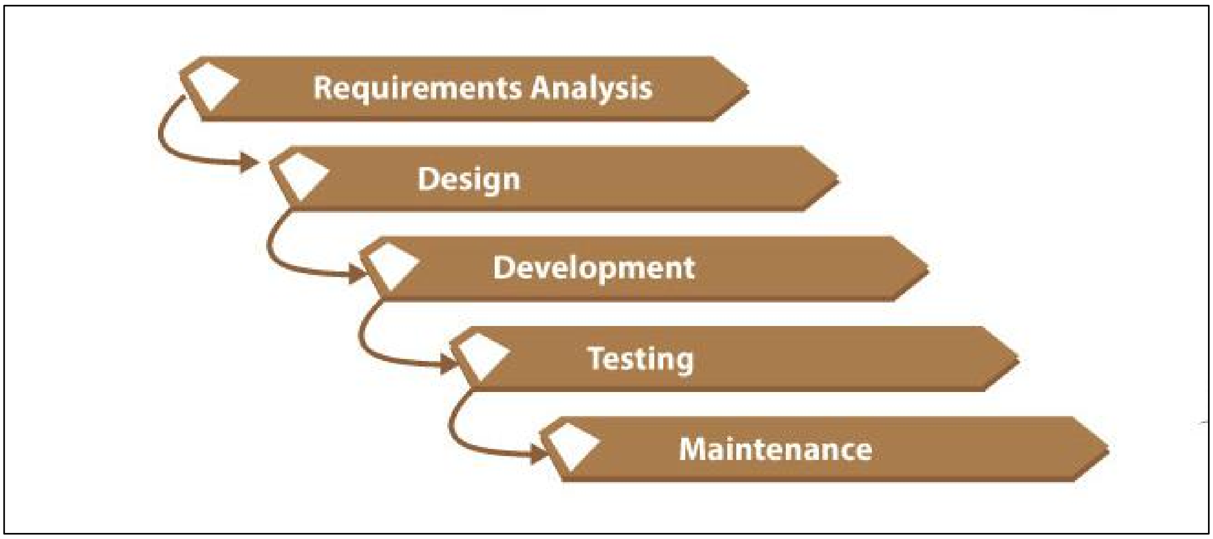


Figure 17: Waterfall model

3.6.1. Requirements Analysis

This is the first phase of development where all the requirements are gathered, documented and analysis done. A requirements feasibility test is done to determine whether the requirements are testable or not. For this study questionnaires are going to be used to collect information from the relevant subjects of study. The questionnaires are used to obtain information from internal users (Judges and Magistrates) and court documents consumers (advocates). This is achieved through the use of online Google forms.

This activity used the research objectives to define the functional and non-functional requirements. Requirements gathering was done mainly through questionnaire analysis and desktop research.

Functional Requirements

These specify what a system should do to achieve the outlined objectives.

The system shall generate key pairs for verified system users

The system shall allow importation of key pairs against each user

The system shall generate PDF documents based on templates designed by law

The system shall store all PDF files in a file server

The system shall transmit all PDF document alongside respective keys to the electronic Document Management system for signing

The system shall store the digitally signed documents for distribution and verification

The system shall uniquely identify each document by a unique code and a corresponding digital signature.

The system shall allow for verification of documents via the public facing portal

Non-functional requirements

Availability: The system should be available 24 hours a day

Usability: The proposed intervention shall be easy to use and should be straight forward to users

Accessible – The system should be accessible to anyone with an internet enabled device irrespective of the device's operating system or computing capability.

Correctness: The intervention should provide information that is correct to its users.

Scalability– The system should be able to grow in terms of data stored and requests handled without service degradation.

3.6.2. Data Analysis: Pre-Implementation Survey

This section critically analyzes data collected from the questionnaires issued to the judicial officers and the advocates. It is important in acquisition of new knowledge based on this study's research objectives. The main aim is to determine if verification of documents generated in court is a real issue and if the use of digital signatures is a valid mechanism to ensure integrity, authenticity and non-repudiation. The following topics were picked as a basis of the questions issued on the Pre-Implementation questionnaires.

3.6.2.1. Current system usage to track litigation process

Both categories of system users were asked if they use of the present system to follow up with the court work

Advocates: there is an overall dependence on the efiling system by advocates in use of the efiling system for tracking of their cases

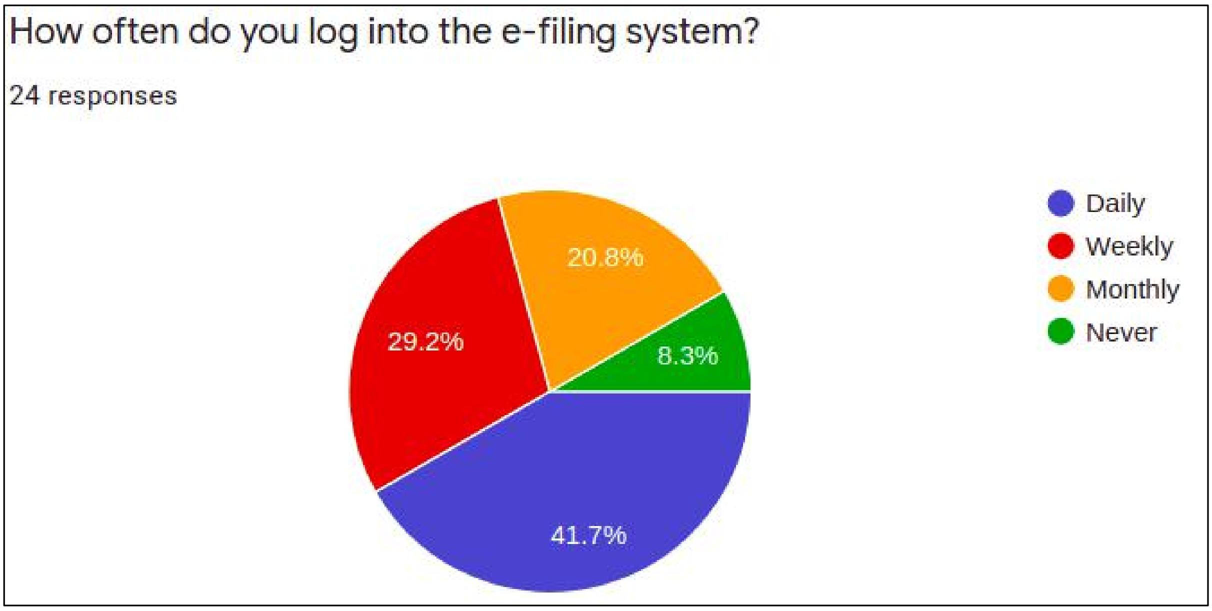


Figure 18: Advocates usage of system

The advocates were also asked what the best way of receiving court documents is. Most of them confirm that they are happy to receive them via the public efiling portal

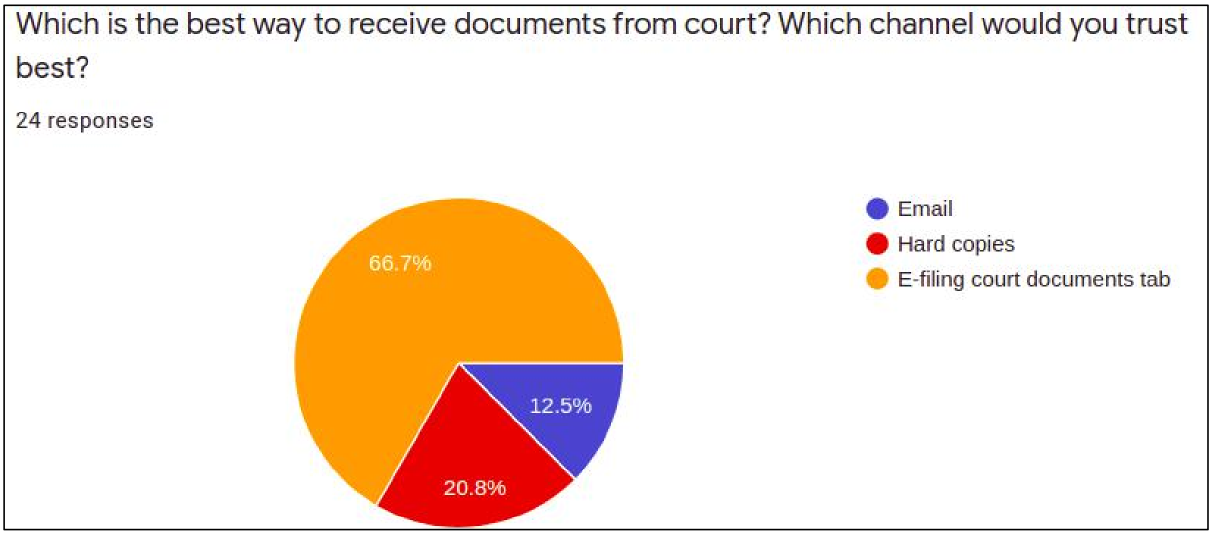
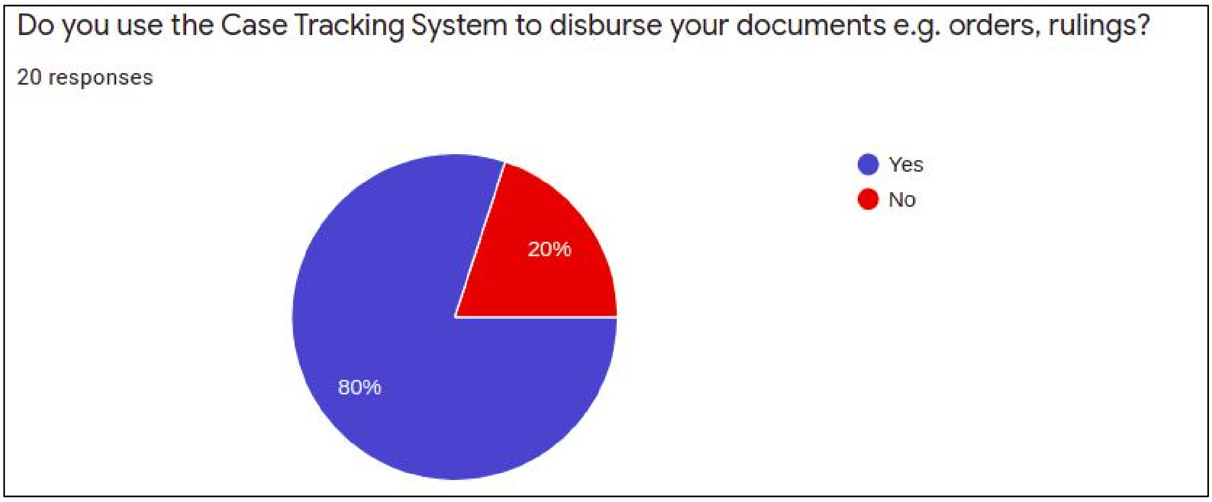


Figure 19: Best channel to receive documents

Judicial officers: Most judicial officers use the case tracking system to disburse their handwritten and typed documents to the litigants. A follow up question indicated that email is also used for disbursal while other litigants visit the courts physically for the hard copies.



Do you use the Case Tracking System to disburse your documents e.g. orders, rulings?

20 responses

Figure 20: JO's usage of system

3.6.2.2. System security confidence

This section was meant to gauge the level of confidence in secure access of their accounts of the systems

Advocates: Quite a number of advocates were not entirely sure that their accounts are safe and individualized.

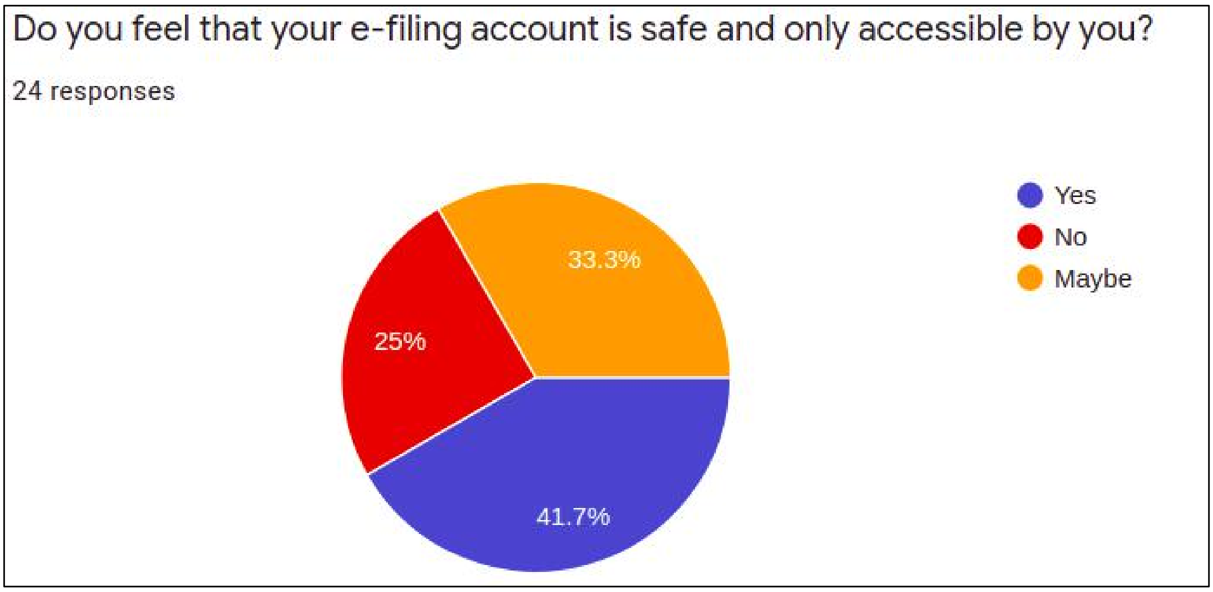


Figure 21: Advocate security confidence

Judicial officers: Most Judicial Officers are confident on security issues to do with their accounts. They cited possible cyber attacks as one of the possible threats to the system security. They also suggested One Time Passwords as in 2 factor authentication as a way to improve security

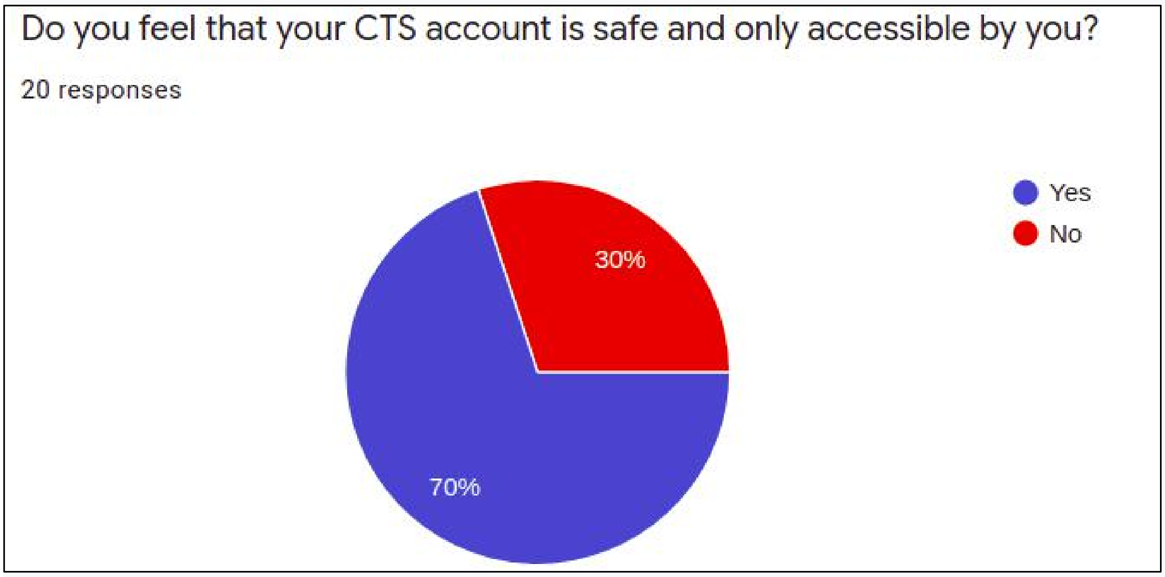
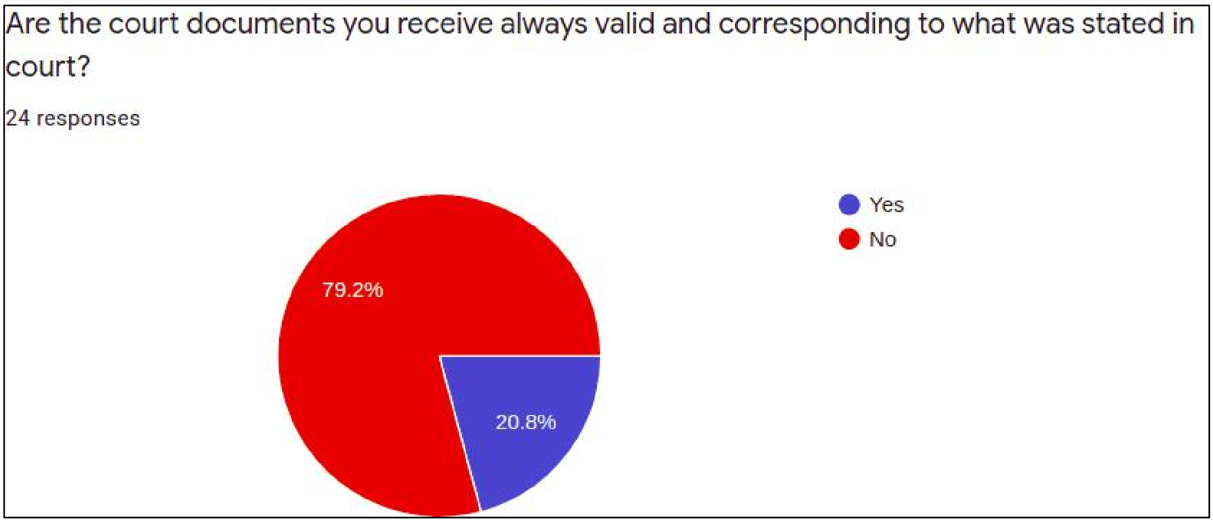


Figure 22: JO CTS account security confidence

3.6.2.3. **Current court documents authenticity and validity**

This category was aimed at determining if court documents are received in as intended once issued at the courts

Advocates: A large number have received documents that did not conform to the original directions and orders of the court. They cited change of document content as one of the major threats. They also indicated that opponents may also be possession of fake documents that did not emanate from court.

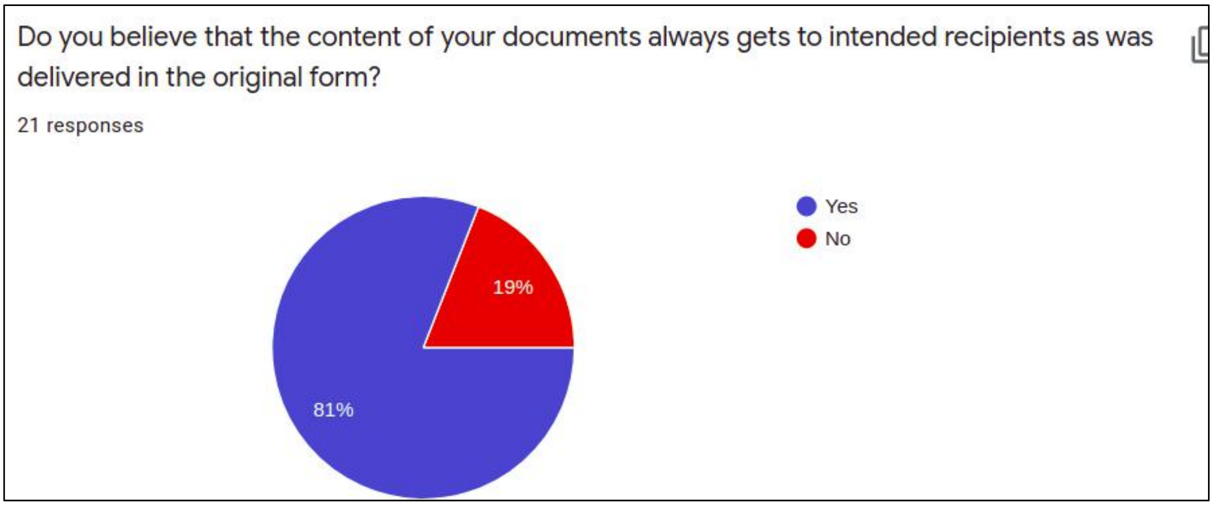


Are the court documents you receive always valid and corresponding to what was stated in court?

24 responses

Figure 23: Court documents transmission validity

Judicial officers: They were asked if they thought that content generated in court always got as intended to the respective parties.



Do you believe that the content of your documents always gets to intended recipients as was delivered in the original form?

21 responses

Figure 24: Court documents content validity

They were also asked if any of their documents had been altered after initial delivery

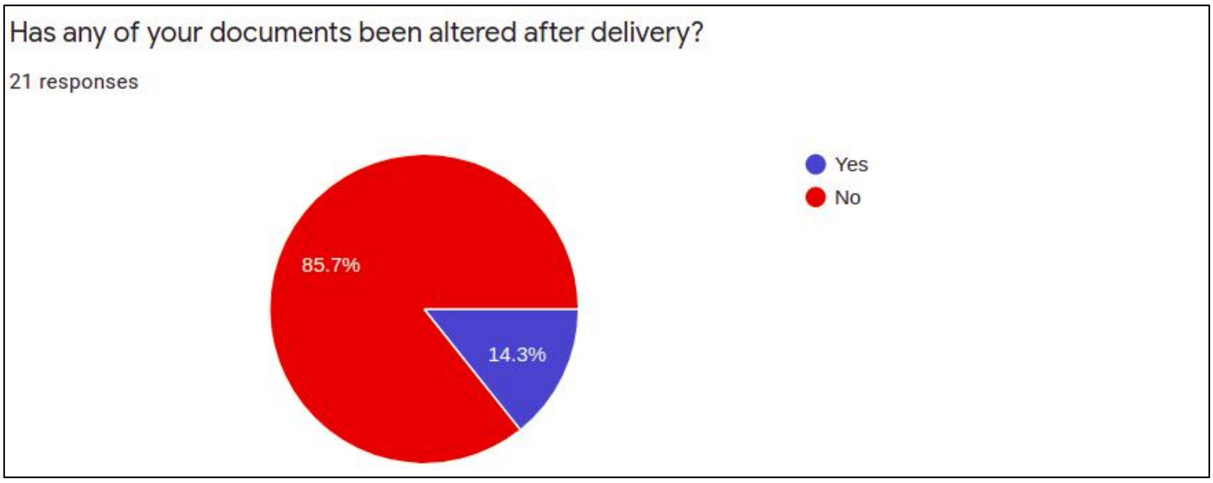


Figure 25: Document alteration

3.6.2.4. New technologies adaptation for verification

Here users are gauged on their willingness for new system features to enable verification of documents

Judicial officers: Most of them indicated that they would be willing to seek new ways of ensuring validity of the court documents disbursal process. Some pointed out that they didn’t want to learn new technologies or added tasks in the system. The research therefore seeks to create a seamless and non-complex way of interaction of the system for digital signing.

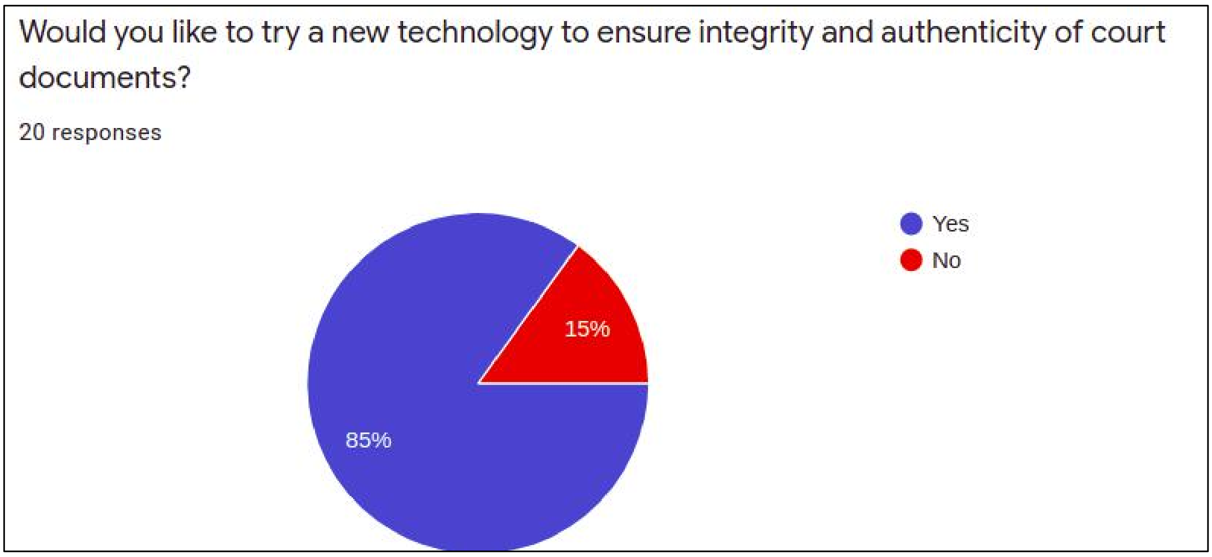


Figure 26: new technology trial

***Advocates*:** They also indicated interest in having a way to verify their documents. They also suggested features such as bar codes, document serialization, SMS code verification and watermarks be added.

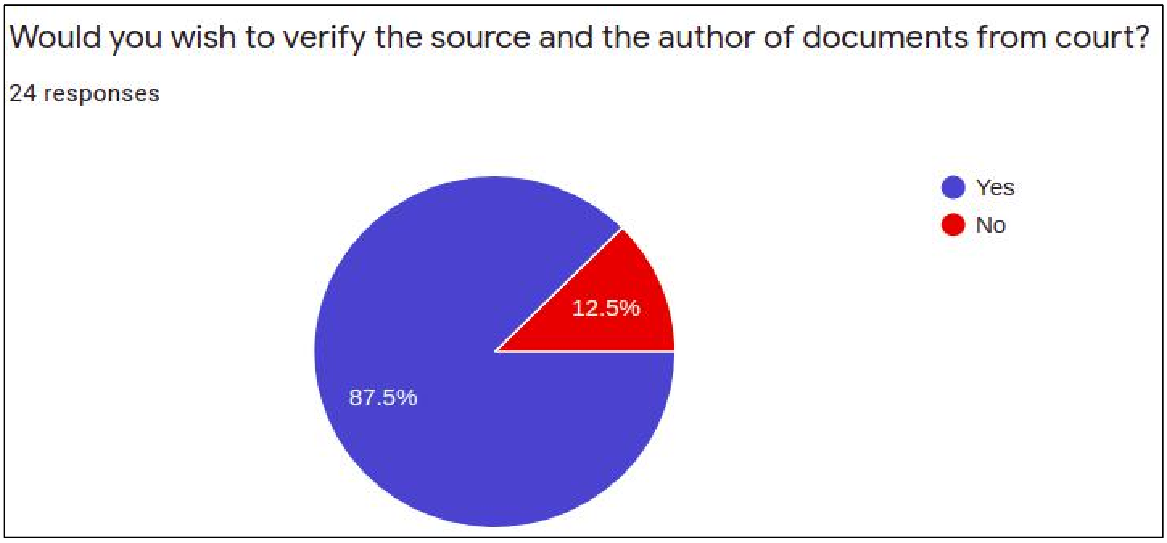


Figure 27: Need to verify source and document author

3.6.2.5. **Conclusion**

20 Judicial officers and 24 advocates responded to the questionnaires. This largely informed and validated the need to verify court generated documents. It is imperative that any document purported to have originated from court is verifiable, is authentic and that its integrity is

beyond reproach. It is also important that once a system user (judicial officer) generates a document through the system, they do not have the leeway to refute its origin.

3.6.3. System Analysis and Design

This study uses system design tools such as the data dictionary, data flow diagrams, class diagrams, database schema, data models, system models, use cases and system flowcharts. These tools will be useful to design user interfaces, to design data and processes that will constitute the architecture. Design diagrams were achieved at the end of this phase.

3.6.3.1. System Architecture

This section illustrates the components of the system and the communication between them to achieve seamless system functionality. At this stage, the overall system design and architecture was done. The diagram below portrays the high-level system architecture.

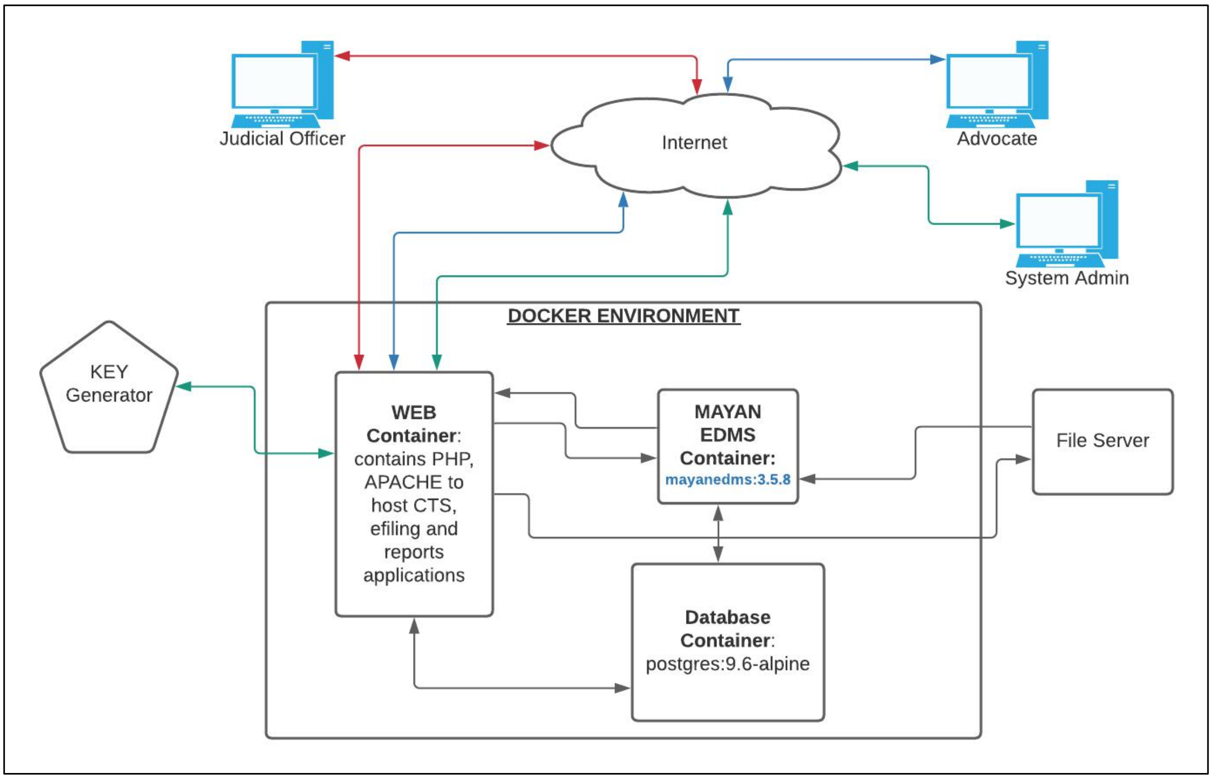

Judicial Officer
Internet
Advocate
System Admin
DOCKER ENVIRONMENT
KEY Generator
WEB Container: contains PHP, APACHE to host CTS, efiling and reports applications
MAYAN EDMS Container: mayanedms:3.5.8
File Server
Database Container: postgres:9.6-alpine

Figure 28: System Architecture

System Components

End Users: The Judicial officers generate court documents and sign them using the private keys while advocates receive the documents and validate them on the public portal. The system admin is responsible for account maintenance and oversight of the key server management

Key Generation software: The Passwords and Keys application software for Linux was adopted for the generation and management of PGP keys that are used to create digital signatures for the court documents. Each key pair is generated using the RSA algorithm and uses 4096 bits. The key is tied to the verified users’ email and user ID

Registration Authority: The case management system has a comprehensive users module in which all Judges and Magistrates are duly registered based on the institution’s human resource records. Here, verifiable email and ID details are acquired in order to generate key pairs

Court Documents generation module: The Case Management system is used to generate PDF documents based on existing templates

File Server: Upon generation of court documents, they are initially pushed to a file server for backup storage.

Electronic Document Management Server: Files generated form the Case Tracking system are pushed to Mayan EDMS alongside the private key of the Judicial Officer handling the court document for signing via API

Database: This runs on postgresql and uses the relational model.

3.6.3.2. Use Case diagram

This is used to depict all the actors of the system and how they interact with the system. The diagram below details how the system responds to a user's interactions to give a successful transaction. It also depicts the scope of the system.On login, an admin is able to upload the key pair that is used to create digital signatures for court documents generated in the system. In the same light, a Judicial officer is able to login and create a court document which is stored in the EDMS and a digital signature embedded. When an advocate logs in to the public portal, they are able to view all documents mapped to their cases. A user with no public account can use the portal to verify the integrity and authenticity of documents transmitted to them.

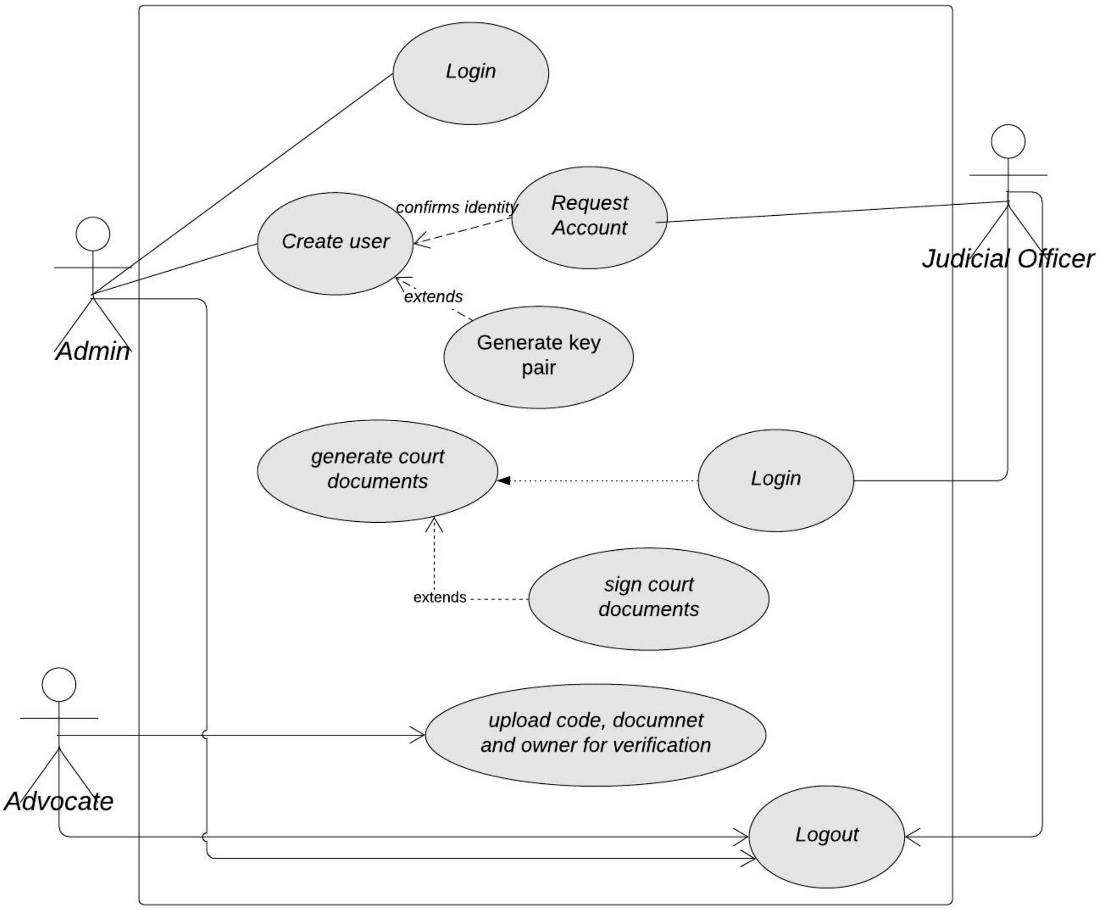


Figure 31: Use Case Diagram

3.6.3.3. System Flow Chart

Generate Key and store flow chart

When a system administrator generates a key pair for each user, they upload it on the case tracking system and subsequently to the EDMS for management as it awaits transmission of documents for signing

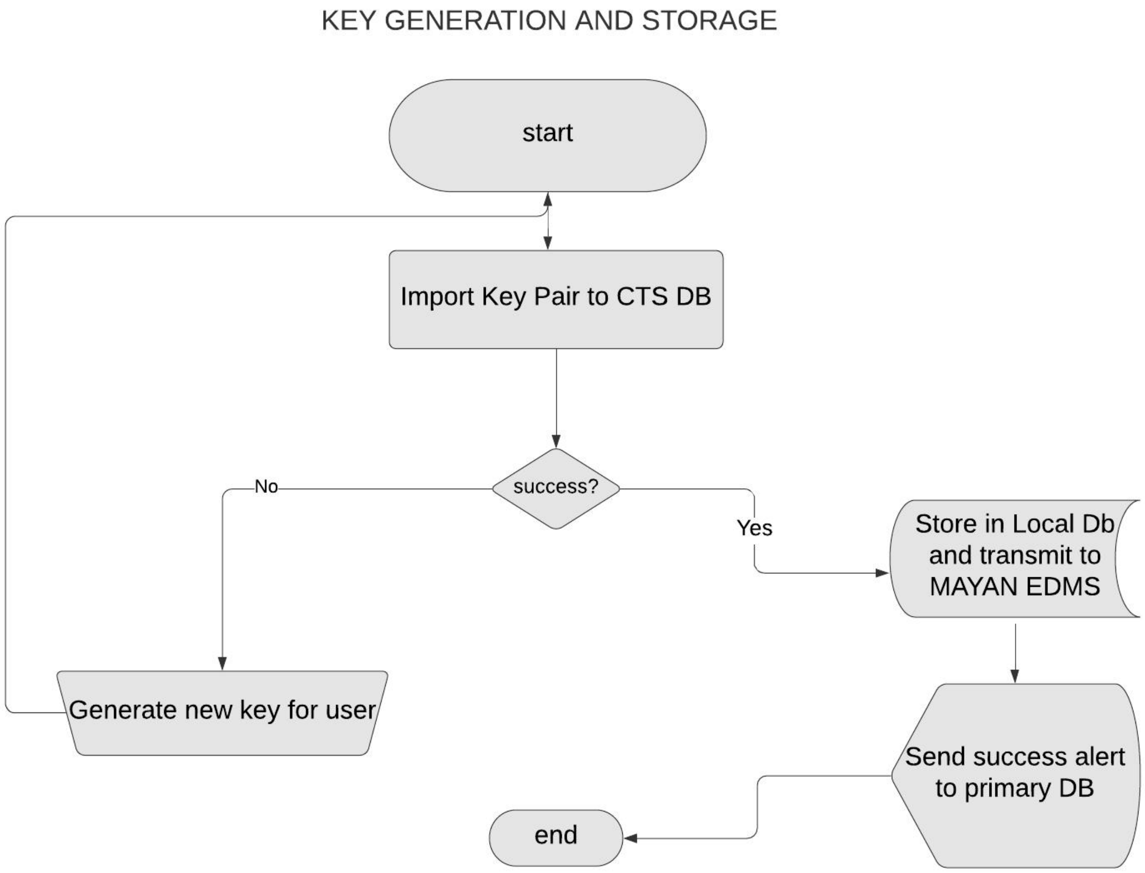

KEY GENERATION AND STORAGE
start
Import Key Pair to CTS DB
success?
No
Yes
Store in Local Db and transmit to MAYAN EDMS
Generate new key for user
Send success alert to primary DB
end

Figure 32: Generate Key and store flow chart

Create and Sign Document Flow Chart

A Judicial officer logs in to the system and creates a document which is transmitted alongside with their private key ID to enable digital signing and storage of the document.

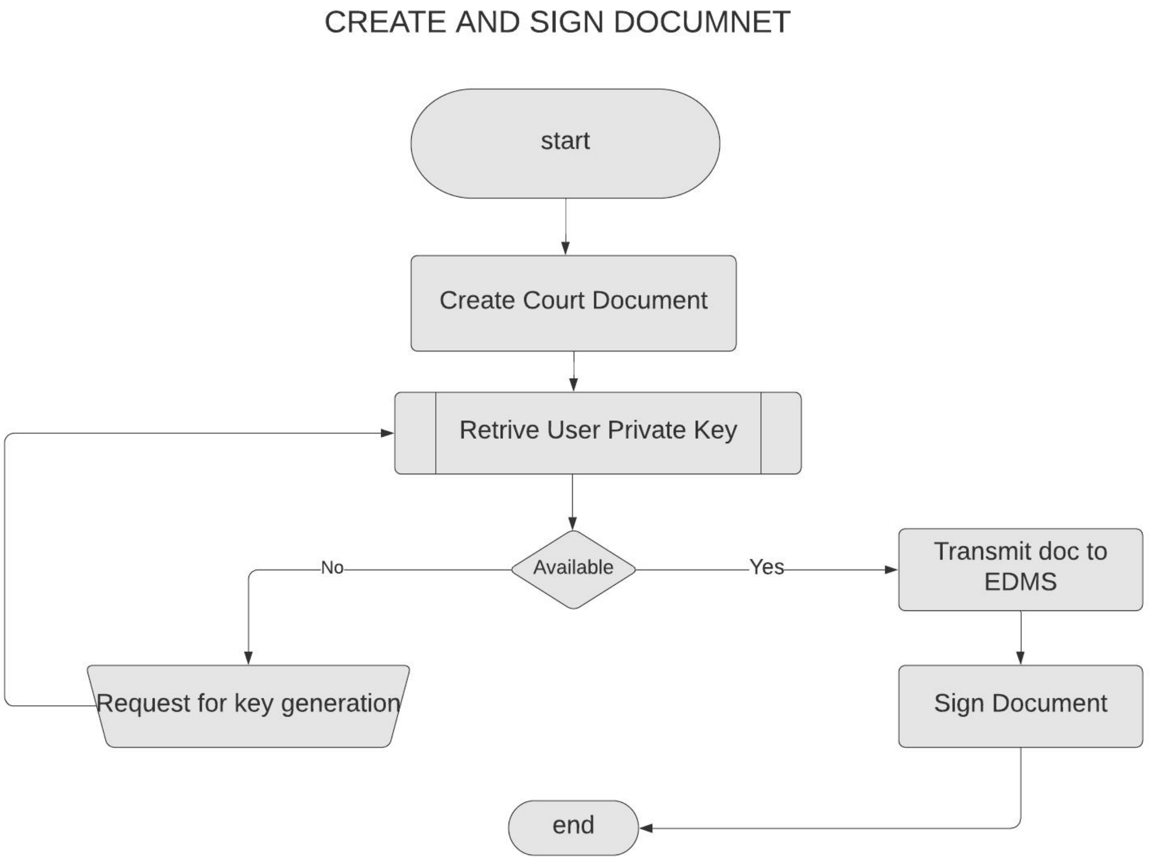


Figure 33: Create and Sign Document Flow Chart

Verification of Documents Flowchart

On the public portal, an advocate/ litigant may verify the authenticity and integrity of the document by way of keying in a code that is uniquely generated for each document. The advocate may also upload a document alongside the public key of the purported originator of the the document for signing. A comparison of the hashes reveals the validity of the uploaded document and gives the relevant feedback

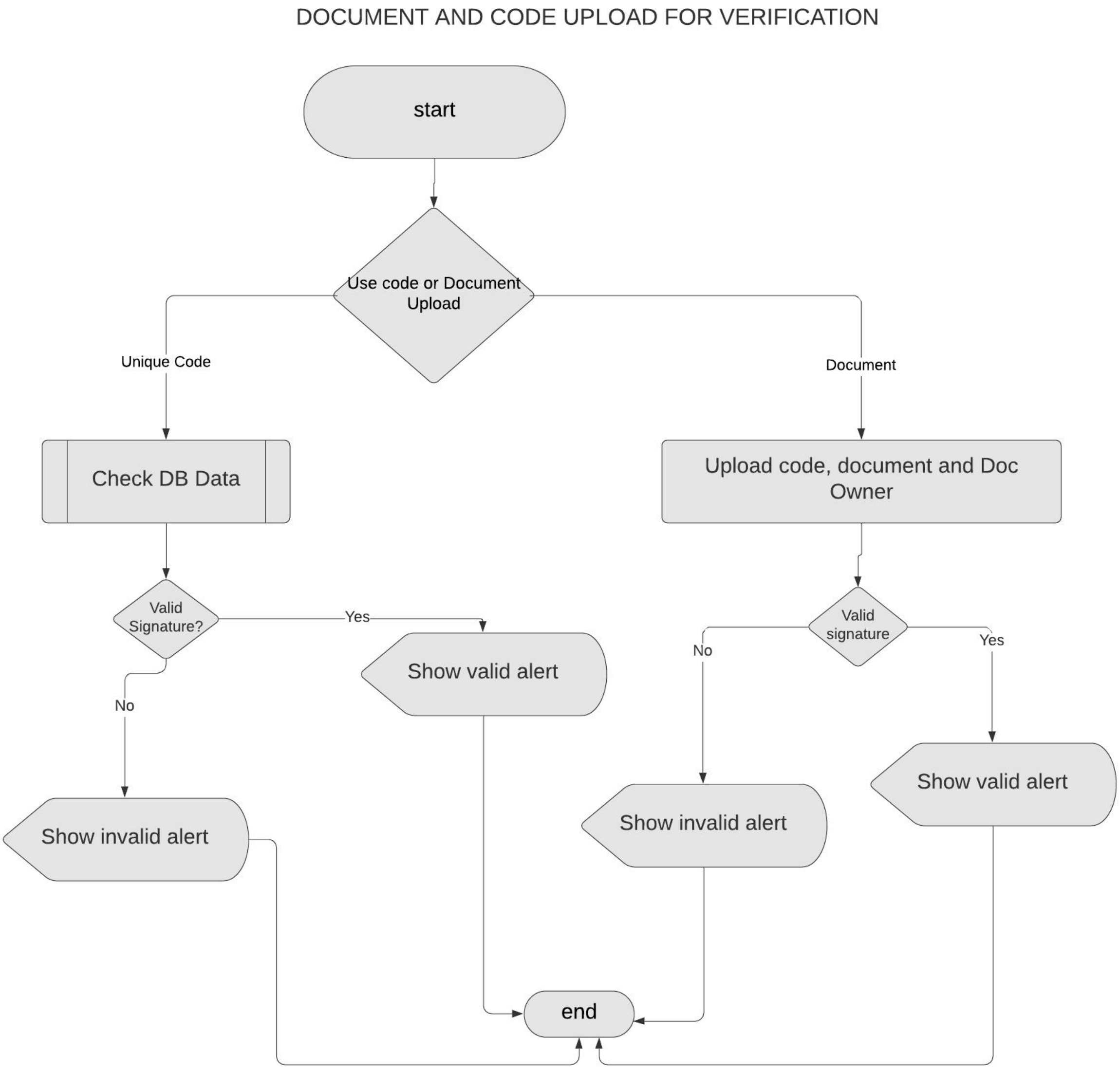


Figure 34: Verification of Documents Flowchart

3.6.3.4. Document verification sequence diagram

The diagram below shows the messages that are transmitted by the advocate to the verification module in the system to confirm the authenticity and integrity of the document

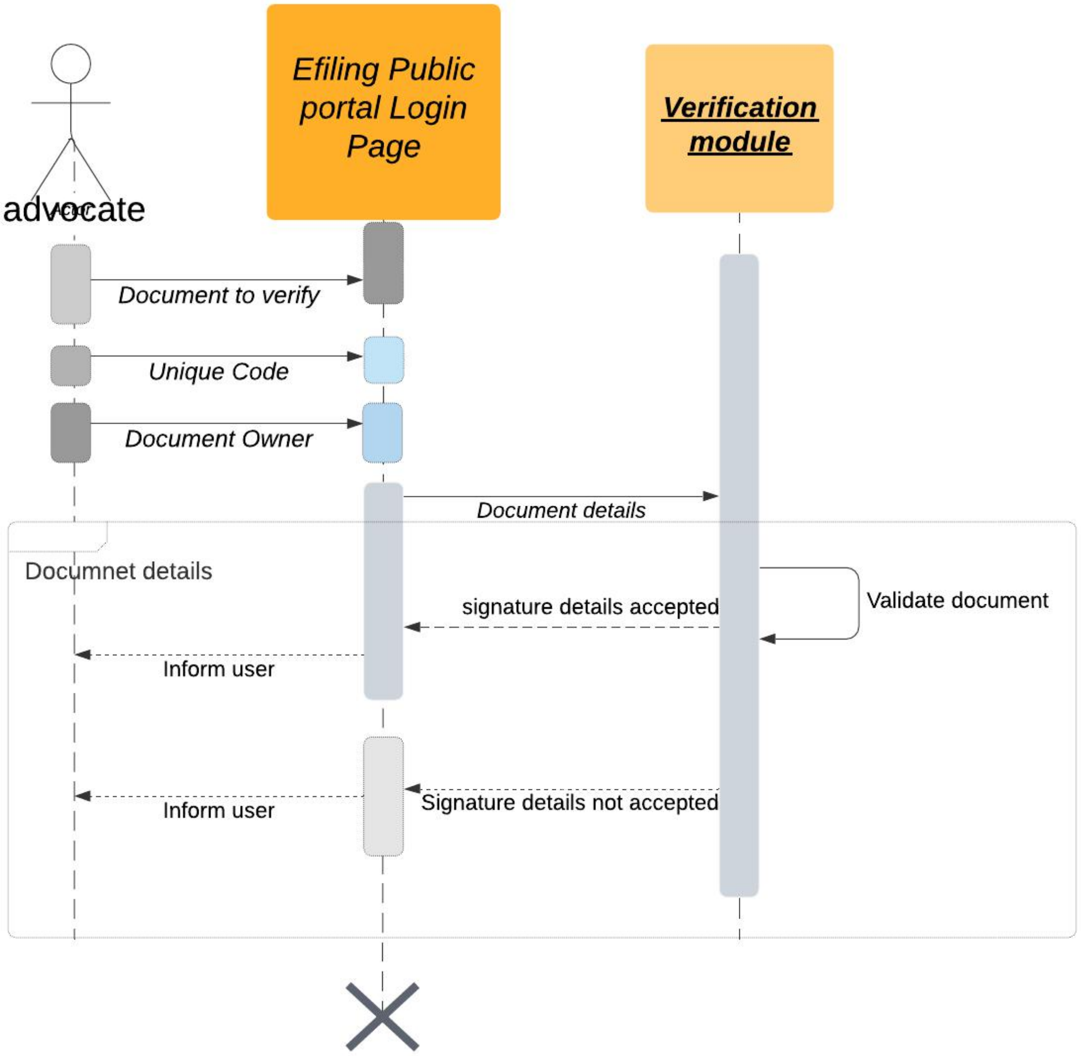
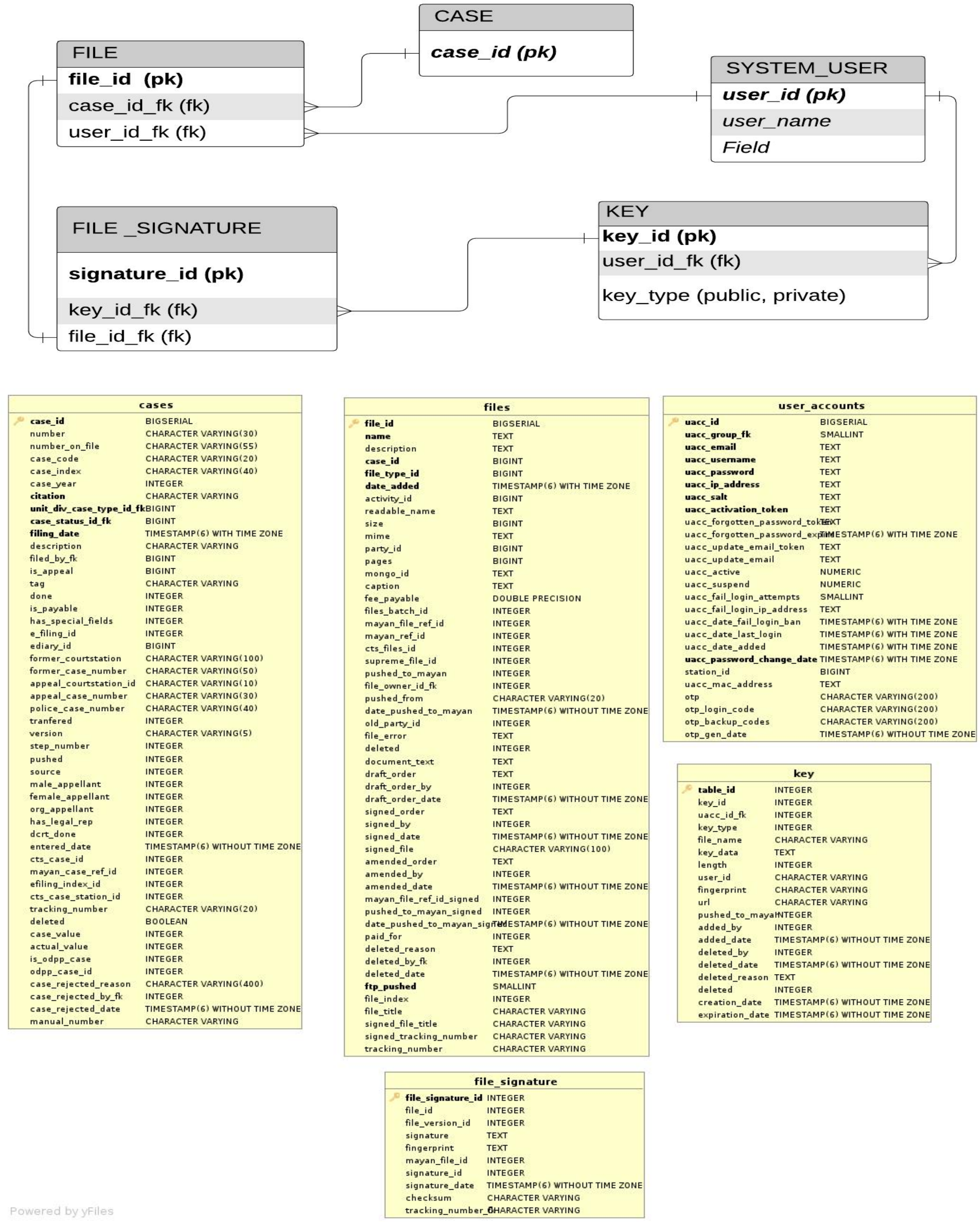


Figure 35: Document verification sequence diagram

3.6.3.5. **Database Schema**

Below is a diagram shat shows a subset of tables the larger case management system used to achieve the digital signatures.



cases	
case_id	BIGSERIAL
number	CHARACTER VARYING(30)
number_on_file	CHARACTER VARYING(55)
case_code	CHARACTER VARYING(20)
case_index	CHARACTER VARYING(40)
case_year	INTEGER
citation	CHARACTER VARYING
unit_div_case_type_id_fk	BIGINT
case_status_id_fk	BIGINT
filing_date	TIMESTAMP(6) WITH TIME ZONE
description	CHARACTER VARYING
filed_by_fk	BIGINT
is_appeal	BIGINT
tag	CHARACTER VARYING
done	INTEGER
is_payable	INTEGER
has_special_fields	INTEGER
e_filing_id	INTEGER
ediary_id	BIGINT
former_courtstation	CHARACTER VARYING(100)
former_case_number	CHARACTER VARYING(50)
appeal_courtstation_id	CHARACTER VARYING(10)
appeal_case_number	CHARACTER VARYING(30)
police_case_number	CHARACTER VARYING(40)
tranfered	INTEGER
version	CHARACTER VARYING(5)
step_number	INTEGER
pushed	INTEGER
source	INTEGER
male_appellant	INTEGER
female_appellant	INTEGER
org_appellant	INTEGER
has_legal_rep	INTEGER
dcrt_done	INTEGER
entered_date	TIMESTAMP(6) WITHOUT TIME ZONE
cts_case_id	INTEGER
mayan_case_ref_id	INTEGER
efiling_index_id	INTEGER
cts_case_station_id	INTEGER
tracking_number	CHARACTER VARYING(20)
deleted	BOOLEAN
case_value	INTEGER
actual_value	INTEGER
is_odpp_case	INTEGER
odpp_case_id	INTEGER
case_rejected_reason	CHARACTER VARYING(400)
case_rejected_by_fk	INTEGER
case_rejected_date	TIMESTAMP(6) WITHOUT TIME ZONE
manual_number	CHARACTER VARYING

files	
file_id	BIGSERIAL
name	TEXT
description	TEXT
case_id	BIGINT
file_type_id	BIGINT
date_added	TIMESTAMP(6) WITH TIME ZONE
activity_id	BIGINT
readable_name	TEXT
size	BIGINT
mime	TEXT
party_id	BIGINT
pages	BIGINT
mongo_id	TEXT
caption	TEXT
fee_payable	DOUBLE PRECISION
files_batch_id	INTEGER
mayan_file_ref_id	INTEGER
mayan_ref_id	INTEGER
cts_files_id	INTEGER
supreme_file_id	INTEGER
pushed_to_mayan	INTEGER
file_owner_id_fk	INTEGER
pushed_from	CHARACTER VARYING(20)
date_pushed_to_mayan	TIMESTAMP(6) WITHOUT TIME ZONE
old_party_id	INTEGER
file_error	TEXT
deleted	INTEGER
document_text	TEXT
draft_order	TEXT
draft_order_by	INTEGER
draft_order_date	TIMESTAMP(6) WITHOUT TIME ZONE
signed_order	TEXT
signed_by	INTEGER
signed_date	TIMESTAMP(6) WITHOUT TIME ZONE
signed_file	CHARACTER VARYING(100)
amended_order	TEXT
amended_by	INTEGER
amended_date	TIMESTAMP(6) WITHOUT TIME ZONE
mayan_file_ref_id_signed	INTEGER
pushed_to_mayan_signed	INTEGER
date_pushed_to_mayan_sign	TIMESTAMP(6) WITHOUT TIME ZONE
paid_for	INTEGER
deleted_reason	TEXT
deleted_by_fk	INTEGER
deleted_date	TIMESTAMP(6) WITHOUT TIME ZONE
ftp_pushed	SMALLINT
file_index	INTEGER
file_title	CHARACTER VARYING
signed_file_title	CHARACTER VARYING
signed_tracking_number	CHARACTER VARYING
tracking_number	CHARACTER VARYING

user_accounts	
uacc_id	BIGSERIAL
uacc_group_fk	SMALLINT
uacc_email	TEXT
uacc_username	TEXT
uacc_password	TEXT
uacc_ip_address	TEXT
uacc_salt	TEXT
uacc_activation_token	TEXT
uacc_forgotten_password_tok	TEXT
uacc_forgotten_password_exp	TIMESTAMP(6) WITH TIME ZONE
uacc_update_email_token	TEXT
uacc_update_email	TEXT
uacc_active	NUMERIC
uacc_suspend	NUMERIC
uacc_fail_login_attempts	SMALLINT
uacc_fail_login_ip_address	TEXT
uacc_date_fail_login_ban	TIMESTAMP(6) WITH TIME ZONE
uacc_date_last_login	TIMESTAMP(6) WITH TIME ZONE
uacc_date_added	TIMESTAMP(6) WITH TIME ZONE
uacc_password_change_date	TIMESTAMP(6) WITH TIME ZONE
station_id	BIGINT
uacc_mac_address	TEXT
otp	CHARACTER VARYING(200)
otp_login_code	CHARACTER VARYING(200)
otp_backup_codes	CHARACTER VARYING(200)
otp_gen_date	TIMESTAMP(6) WITHOUT TIME ZONE

key	
table_id	INTEGER
key_id	INTEGER
uacc_id_fk	INTEGER
key_type	INTEGER
file_name	CHARACTER VARYING
key_data	TEXT
length	INTEGER
user_id	CHARACTER VARYING
fingerprint	CHARACTER VARYING
url	CHARACTER VARYING
pushed_to_maya	INTEGER
added_by	INTEGER
added_date	TIMESTAMP(6) WITHOUT TIME ZONE
deleted_by	INTEGER
deleted_date	TIMESTAMP(6) WITHOUT TIME ZONE
deleted_reason	TEXT
deleted	INTEGER
creation_date	TIMESTAMP(6) WITHOUT TIME ZONE
expiration_date	TIMESTAMP(6) WITHOUT TIME ZONE

file_signature	
file_signature_id	INTEGER
file_id	INTEGER
file_version_id	INTEGER
signature	TEXT
fingerprint	TEXT
mayan_file_id	INTEGER
signature_id	INTEGER
signature_date	TIMESTAMP(6) WITHOUT TIME ZONE
checksum	CHARACTER VARYING
tracking_number_0	CHARACTER VARYING

Figure 36: ERD

3.6.4. System Implementation

Following the system design phase, the various system components were set up/ developed to create the entire software ecosystem. The components are the key generation software, the internal web module for court documents creation and the verification module in the public portal, the Mayan EDMS as well as the Database set up

3.6.4.1. Technology Stack

The table below shows the technology that was applied in the development and deployment of this system

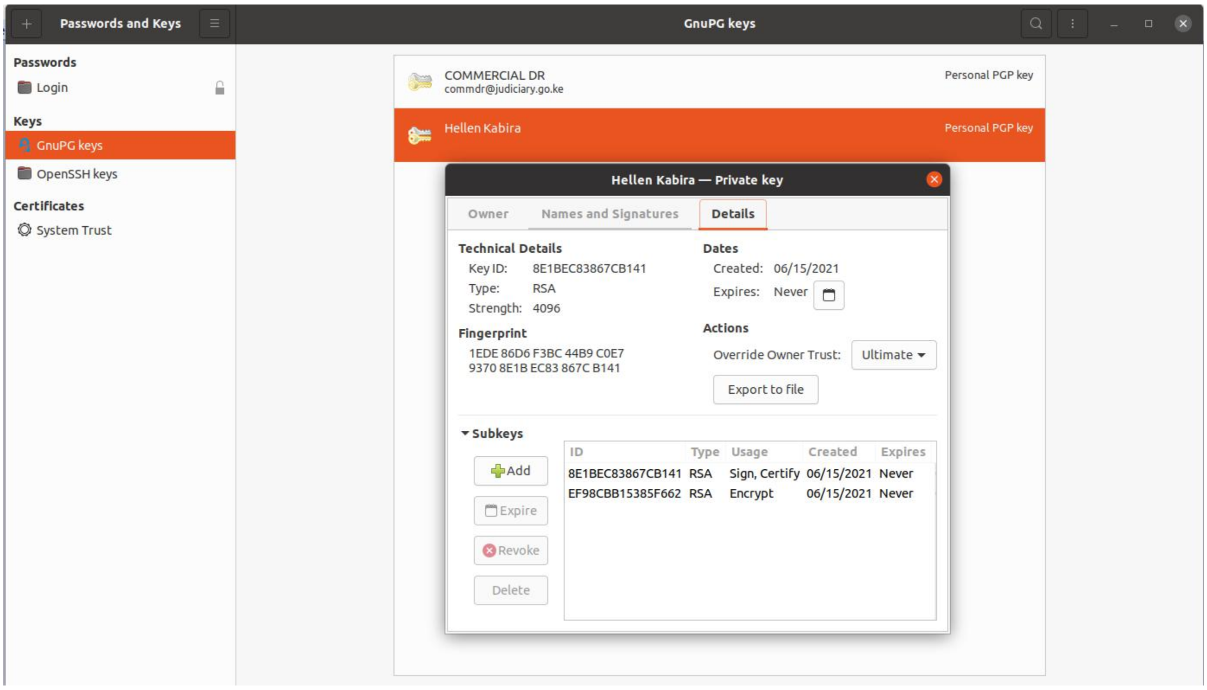
Component	**Technology**
Hardware	Laptop computer 16GB RAM, 1TB Hard Disk, intel® Core™ i7-10510U CPU @ 1.80GHz × 8
Operating System	Linux - Ubuntu 20.04
Containerization	Docker version 20.10.6
Database	Postgres 9.6 pgAdmin 4 for DB visualization
Electronic Document Management System	Mayan EDMS v3.5.8
Web system (Case Management System and efiling portal)	Framework: codeigniter Server side scripting:php v7.2 Client side scripting: AJAX, JavaScript API calls: JSON User interface: HTML5, CSS IDE: Netbeans 12.0
API tests	Postman

Key generation	OpenPGP using Passwords and Keys software
Notable libraries used	SummerNote: Text editor to create documents on the system MPDF: convert generated documents to PDF Guzzle: PHP HTTP client to send HTTP requests (API)

Table 3: Technology stack

3.6.4.2. Key generation software

Passwords and Keys v3.36 application software system was installed on Ubuntu 20.04. This is used to generate key pairs that are used in the encryption and decryption process for the creation and verification of court documents. Keys are stored in a secure folder on the administrator’s computer for upload into the web system.



Technical Details

Key ID: 8E1BEC83867CB141

Type: RSA

Strength: 4096

Fingerprint

1EDE 86D6 F3BC 44B9 C0E7
9370 8E1B EC83 867C B141

Dates

Created: 06/15/2021

Expires: Never

Actions

Override Owner Trust: Ultimate

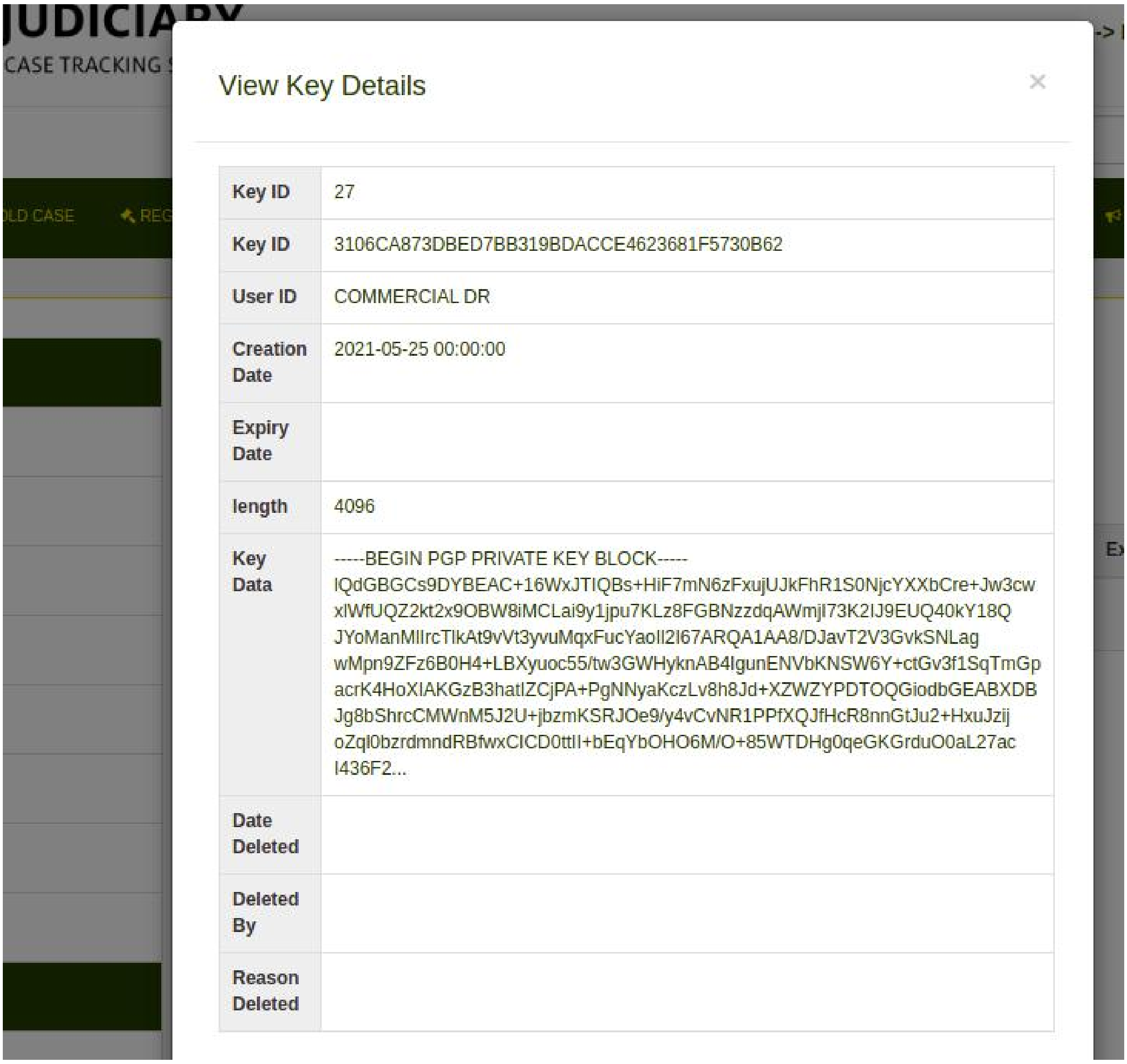
Subkeys

ID	Type	Usage	Created	Expires
8E1BEC83867CB141	RSA	Sign, Certify	06/15/2021	Never
EF98CBB15385F662	RSA	Encrypt	06/15/2021	Never

Figure 37: Key generation software

3.6.4.3. Key Pair Management

On the administration module of the internal case tracking system is an interface to manage keys belonging to the originators of the court documents



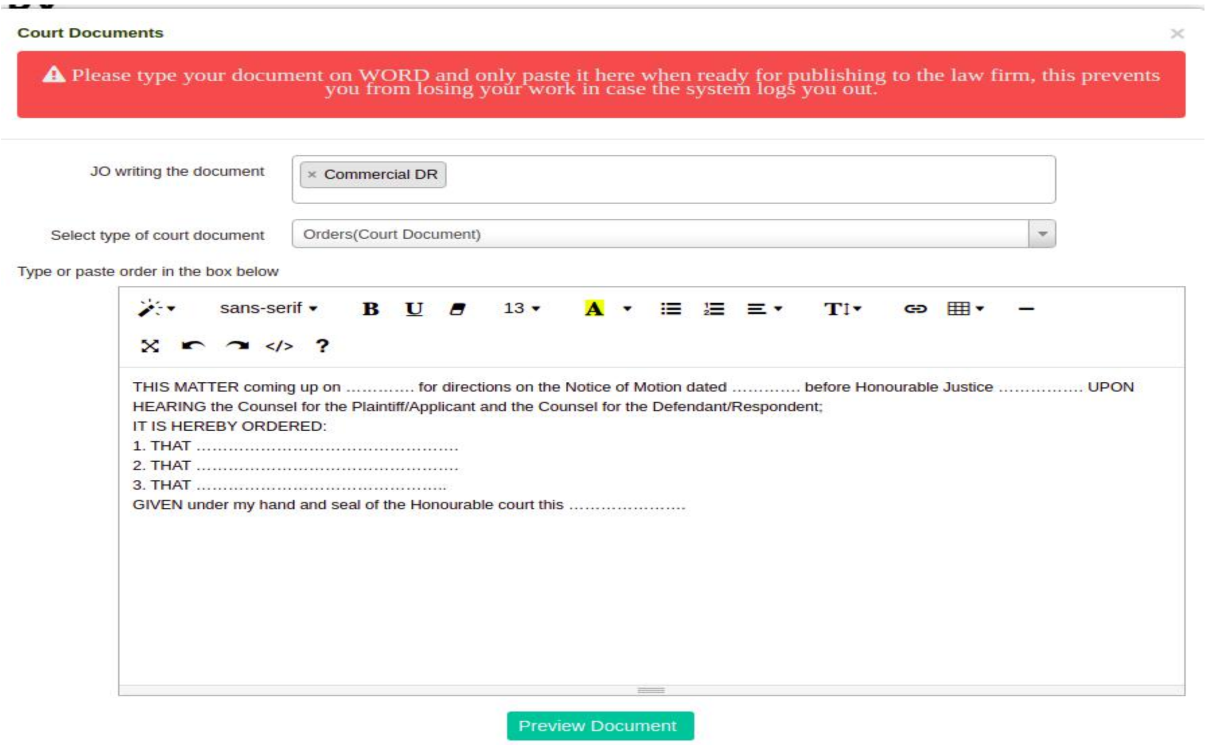
View Key Details

Key ID	27
Key ID	3106CA873DBED7BB319BDACCE4623681F5730B62
User ID	COMMERCIAL DR
Creation Date	2021-05-25 00:00:00
Expiry Date	
length	4096
Key Data	-----BEGIN PGP PRIVATE KEY BLOCK----- lQdGBGCs9DYBEAC+16WxJTIQBs+HiF7mN6zFxujUJkFhR1S0NjcYXXbCre+Jw3cw xlWfUQZ2kt2x9OBW8iMCLai9y1jpu7KLz8FGBNzzdqAWmjI73K2IJ9EUQ40kY18Q JYoManMIIrcTlkAt9vVt3yvuMqxFucYaoIl2I67ARQA1AA8/DJavT2V3GvkSNLag wMpn9ZFz6B0H4+LBXyuoc55/tw3GWHyknAB4IgunENVbKNSW6Y+ctGv3f1SqTmGp acrK4HoXIAKGzB3hatIZCjPA+PgNNyaKczLv8h8Jd+XZWZYPDTOQGiodbGEABXDB Jg8bShrcCMWnM5J2U+jbzmKSRJOe9/y4vCvNR1PPfXQJfHcR8nnGtJu2+HxuJzij oZql0bzrdmndRBfwxCICD0ttlI+bEqYbOHO6M/O+85WTDHg0qeGKGrduO0aL27ac l436F2...
Date Deleted	
Deleted By	
Reason Deleted	

Figure 38: Key Pair Management

3.6.4.4. Court Document Creation

Against each court activity is a provision of a text editor to generate court documents using predefined templates



Court Documents
×
⚠ Please type your document on WORD and only paste it here when ready for publishing to the law firm, this prevents you from losing your work in case the system logs you out.
sans-serif
B
U
13
A
T
</>
?
Preview Document

JO writing the document: × Commercial DR

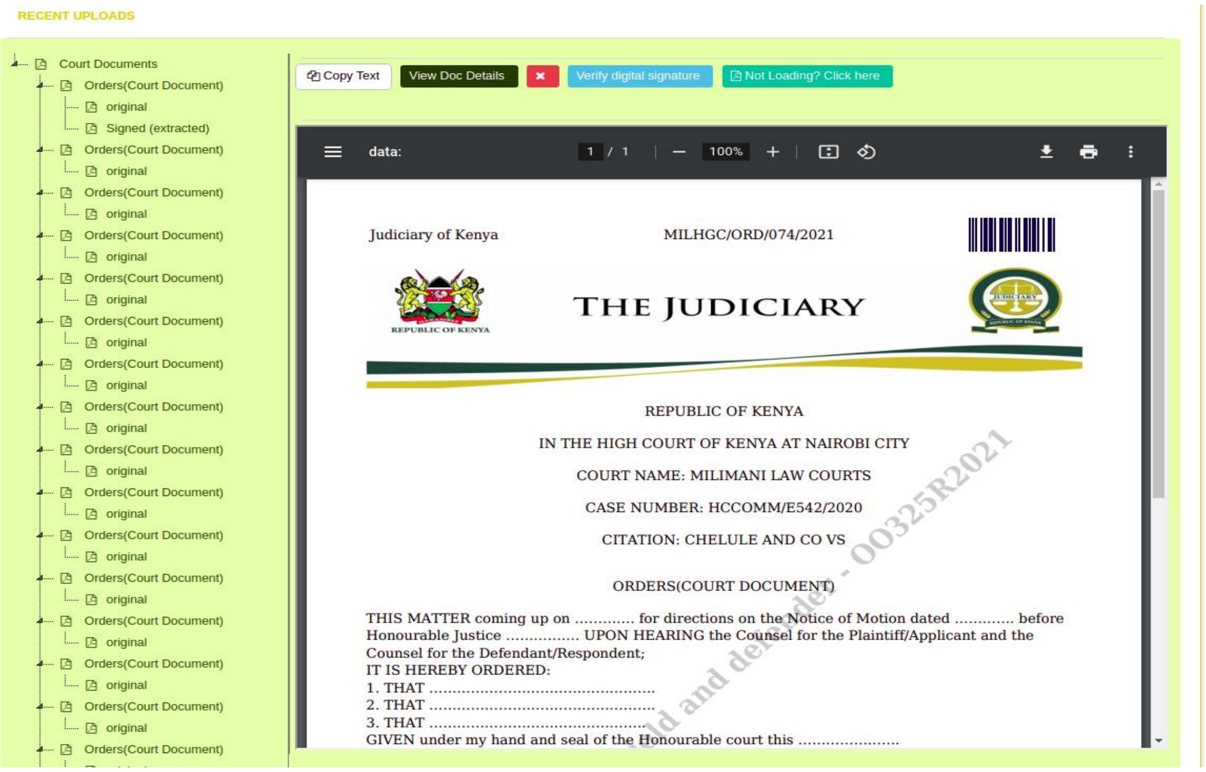
Select type of court document: Orders(Court Document)

Type or paste order in the box below

THIS MATTER coming up on .... for directions on the Notice of Motion dated .... before Honourable Justice .... UPON HEARING the Counsel for the Plaintiff/Applicant and the Counsel for the Defendant/Respondent;
IT IS HEREBY ORDERED:
1. THAT ....
2. THAT ....
3. THAT ....
GIVEN under my hand and seal of the Honourable court this ....

Figure 39: Court Document Creation

On submission of input from the text editor, a PDF document is generated from system and sent to the EDMS with users private key



MILHGC/ORD/074/2021

REPUBLIC OF KENYA

IN THE HIGH COURT OF KENYA AT NAIROBI CITY

COURT NAME: MILIMANI LAW COURTS

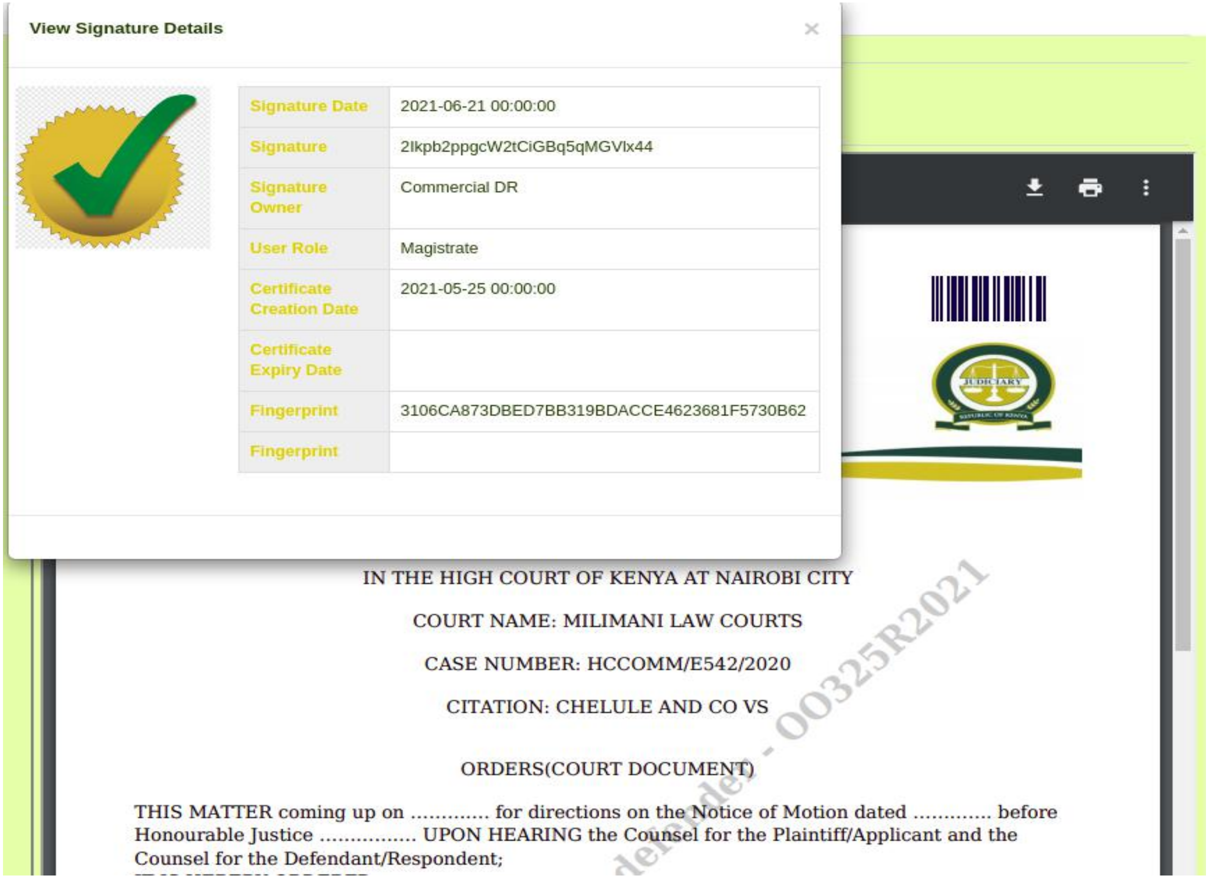
CASE NUMBER: HCCOMM/E542/2020

CITATION: CHELULE AND CO VS

ORDERS(COURT DOCUMENT)

THIS MATTER coming up on .... for directions on the Notice of Motion dated .... before Honourable Justice .... UPON HEARING the Counsel for the Plaintiff/Applicant and the Counsel for the Defendant/Respondent;
IT IS HEREBY ORDERED:
1. THAT ....
2. THAT ....
3. THAT ....
GIVEN under my hand and seal of the Honourable court this ....

Below is a depiction of the digital signature details as transmitted via API from the EDMS upon signing of the PDF document



View Signature Details

Signature Date	2021-06-21 00:00:00
Signature	2lkpb2ppgcW2tCiGBq5qMGVlx44
Signature Owner	Commercial DR
User Role	Magistrate
Certificate Creation Date	2021-05-25 00:00:00
Certificate Expiry Date	
Fingerprint	3106CA873DBED7BB319BDACCE4623681F5730B62
Fingerprint	

IN THE HIGH COURT OF KENYA AT NAIROBI CITY

COURT NAME: MILIMANI LAW COURTS

CASE NUMBER: HCCOMM/E542/2020

CITATION: CHELULE AND CO VS

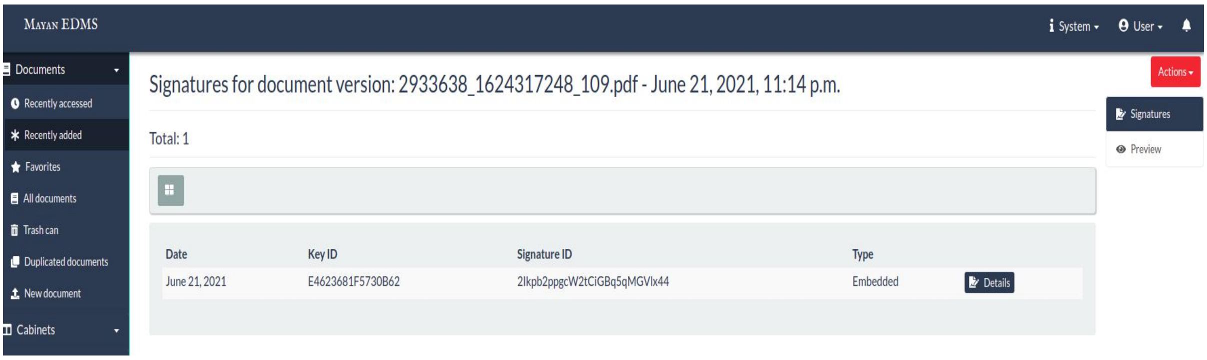
ORDERS(COURT DOCUMENT)

THIS MATTER coming up on .... for directions on the Notice of Motion dated .... before Honourable Justice .... UPON HEARING the Counsel for the Plaintiff/Applicant and the Counsel for the Defendant/Respondent;

Figure 40: Signature details

3.6.4.5. Document signing via MAYAN API

The EDMS has inbuilt functionality to append digital signatures given a PDF document and the private key of the user. The output is transmitted back to the web application via API



Signatures for document version: 2933638_1624317248_109.pdf - June 21, 2021, 11:14 p.m.

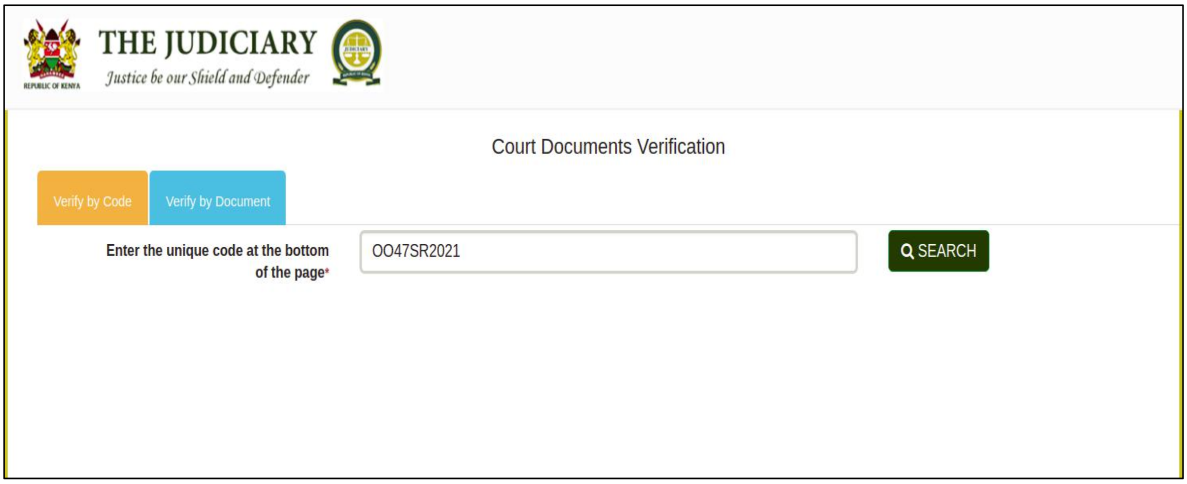
Total: 1

Date	Key ID	Signature ID	Type	
June 21, 2021	E4623681F5730B62	2lkpb2ppgcW2tCiGBq5qMGVlx44	Embedded	Details

Figure 41: Signature in Mayan

3.6.4.6. Public Facing verification module

The interface shows the public facing portal where court users may verify their document. They do not have to login to carry out this function

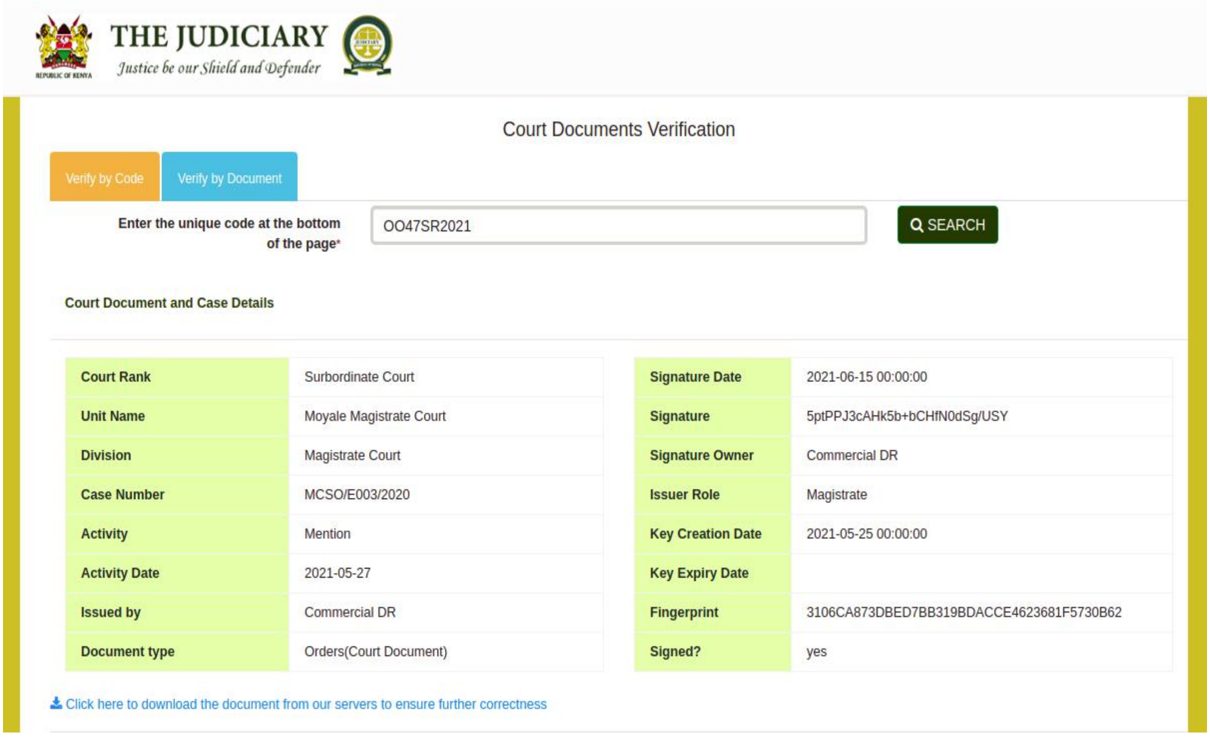


Court Documents Verification

Enter the unique code at the bottom of the page*: OO47SR2021

Figure 42: Verify document by code on e-filing

Details of a Valid Document appear as follows:



Court Documents Verification

Enter the unique code at the bottom of the page*: OO47SR2021

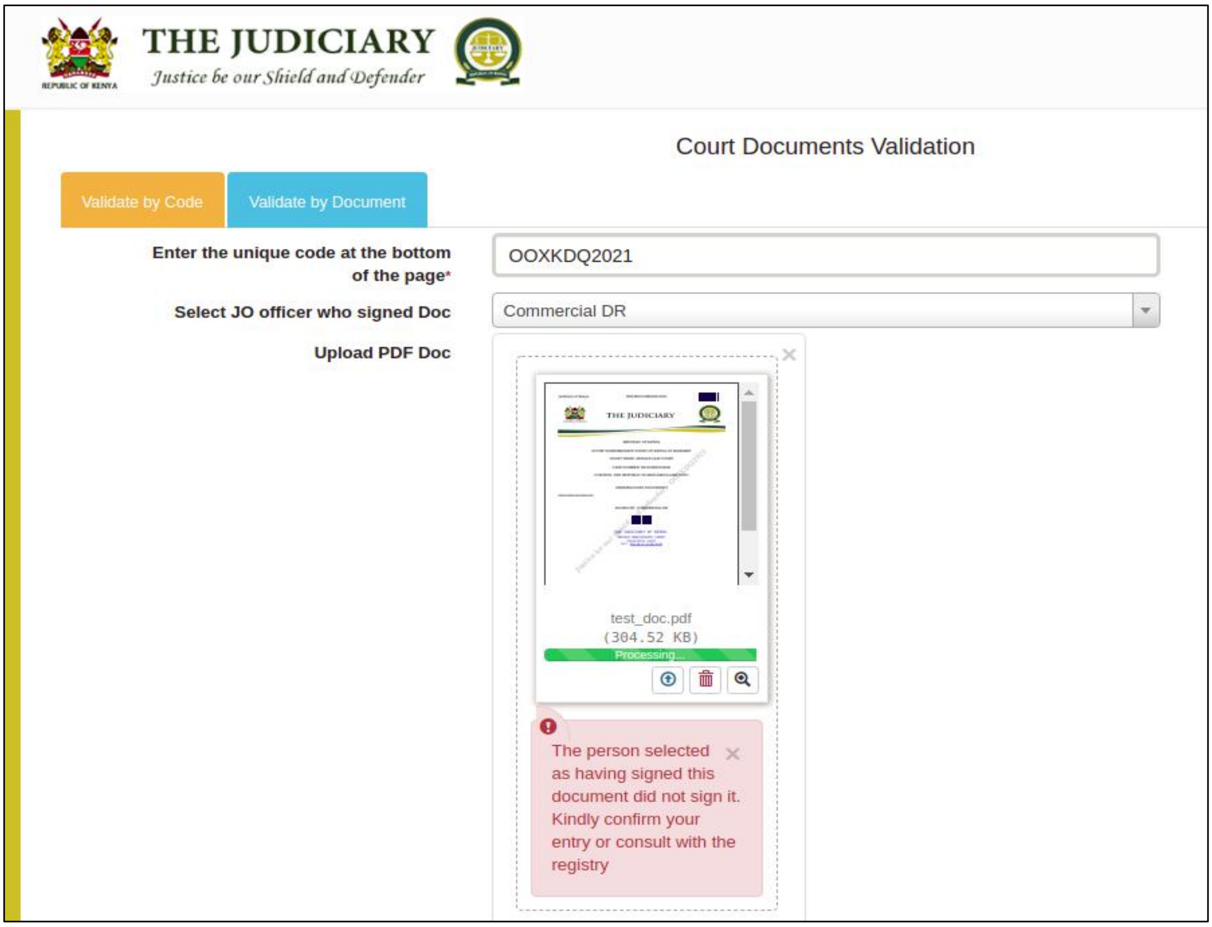
Court Document and Case Details

Court Rank	Surbordinate Court	Signature Date	2021-06-15 00:00:00
Unit Name	Moyale Magistrate Court	Signature	5ptPPJ3cAHk5b+bCHfN0dSg/USY
Division	Magistrate Court	Signature Owner	Commercial DR
Case Number	MCSO/E003/2020	Issuer Role	Magistrate
Activity	Mention	Key Creation Date	2021-05-25 00:00:00
Activity Date	2021-05-27	Key Expiry Date	
Issued by	Commercial DR	Fingerprint	3106CA873DBED7BB319BDACCE4623681F5730B62
Document type	Orders(Court Document)	Signed?	yes

Click here to download the document from our servers to ensure further correctness

Figure 43: Valid document details

Documents whose details are not correct are reported as below



Court Documents Validation

Enter the unique code at the bottom of the page*: OOXKDQ2021

Select JO officer who signed Doc: Commercial DR

Upload PDF Doc

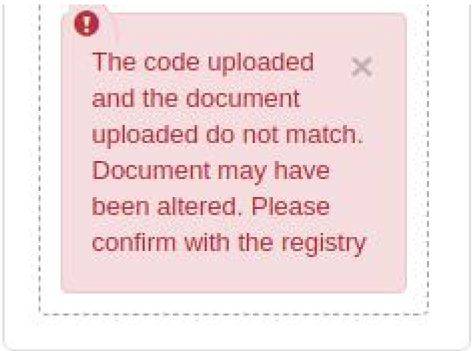
test_doc.pdf
(304.52 KB)
Processing...

The person selected as having signed this document did not sign it. Kindly confirm your entry or consult with the registry

Figure 44: Error: Wrong JO selected as document signer

Other error codes:

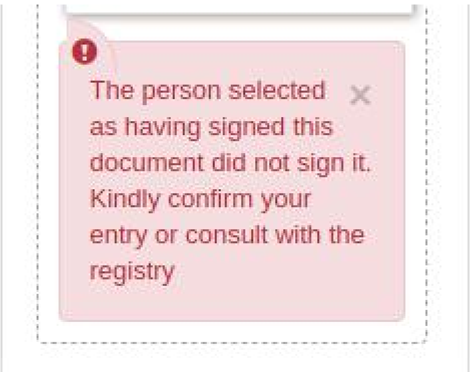
The unique code is directly matched with the hash of the document. If the uploaded document’s hash does not match with the document in the server, the error below is displayed. Proof of document validity and correctness is thereby achieved



The code uploaded and the document uploaded do not match. Document may have been altered. Please confirm with the registry

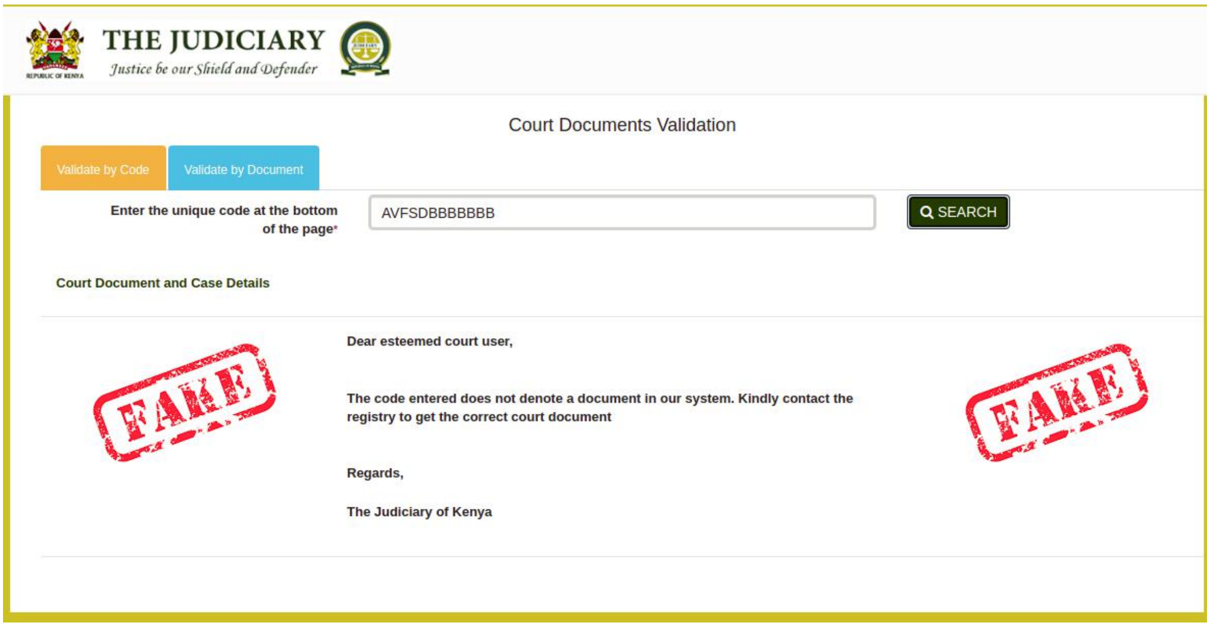
Figure 45: Error- document was altered

During verification, if the wrong key is used in signing the document to be verified (by choosing the wrong judicial officer) then the following error is displayed. Here an assurance of authenticity is achieved



The person selected as having signed this document did not sign it. Kindly confirm your entry or consult with the registry

A document whose code does not exist in the system at all shows the following:



Court Documents Validation

Enter the unique code at the bottom of the page* AVFSDBBBBBBBB

Court Document and Case Details

Dear esteemed court user,

The code entered does not denote a document in our system. Kindly contact the registry to get the correct court document

Regards,

The Judiciary of Kenya

Figure 46: Non-existent document

3.6.5. Verification, testing and deployment

This involves deployment and testing of the developed software. It involves pitting the deployed software against the users' requirements. Continuous tests are carried out through out the development of the system. All code goes through comprehensive screening to ensure no bugs and errors are found before production or release. Modules are tested independently to confirm full functionality. The modules are also tested in relation to all other modules to ensure seamless integration and flow of data between them. Test cases were developed and together with the prototype deployed in one division of the High court at Milimani, Nairobi.

The testing stage involved thorough checking of the software components to verify that they satisfy the defined requirements and also to detect errors and defects requiring correction.

Testing Approaches Used

Source Code Inspection – The source code and documentation were examined systematically to identify defects.

Functionality Testing – This was done by pitting the developed software against the requirements to check if it did what it was supposed to achieve.

3.6.5.1. Unit Testing

Each system component and standalone modules were subjected to tests to ensure correctness. Test cases were used to achieve this.

	Activity	Objective	Expected Outcome	Actual Outcome	Comments
	Name of the Tester:		Court Station:		
1.	Key generation	Admin able to generate and export key pair using the application	Using the given link, the user accesses the system and successfully login to the respective court station		
2.	Court Document Configuration	Admin able to add a court document template on CTS	Court doc successfully configured in CTS		
3.	Court Document Generation	JO able to log in and generate a court document against a case activity	Court Document generated and transmitted to the EDMS, visible on verified court docs page		
4.	Court Document verification using code	On the efiling portal, enter the code on the court	Message return displays document is either valid or invalid		

		document			
5.	Court Document verification using document	On the e-filing portal, enter the code and document originator, upload the document and submit	Message return displays document is either valid or invalid		

Table 4: Test cases

3.6.5.2. Integration Testing

Once each module and component had gone through successful tests, tests for the whole system as a combination of all components was done. On successful generation of a valid key pair on the key generation software, it was uploaded to the case Tracking system via the admin portal for the respective Judicial officer. The admin was also able to configure a court document template. The Judicial Officer was thereafter able to long in to the system and create and sign a court document. The document could then be viewed in Mayan EDMS with the embedded signature. The same details can be seen on the Case Tracking system verified docs interface. Upon receiving the court document, an advocate was thereafter able to verify the authenticity and integrity of the court document on the public portal.

3.6.6. Maintenance

This stage involves the incorporation of users’ feedback in the system. User change request forms are the main methods of collecting feedback entailing envisioned corrections and upgrades.

Chapter 4: Results and Discussion

This chapter is a summary of the research and the development aspects of this project. We seek to determine if the objectives set were met and the challenges encountered. This seeks to show how the research objectives were met by the end of this project life cycle with the data sources being the desktop literature review and the post implementation survey.

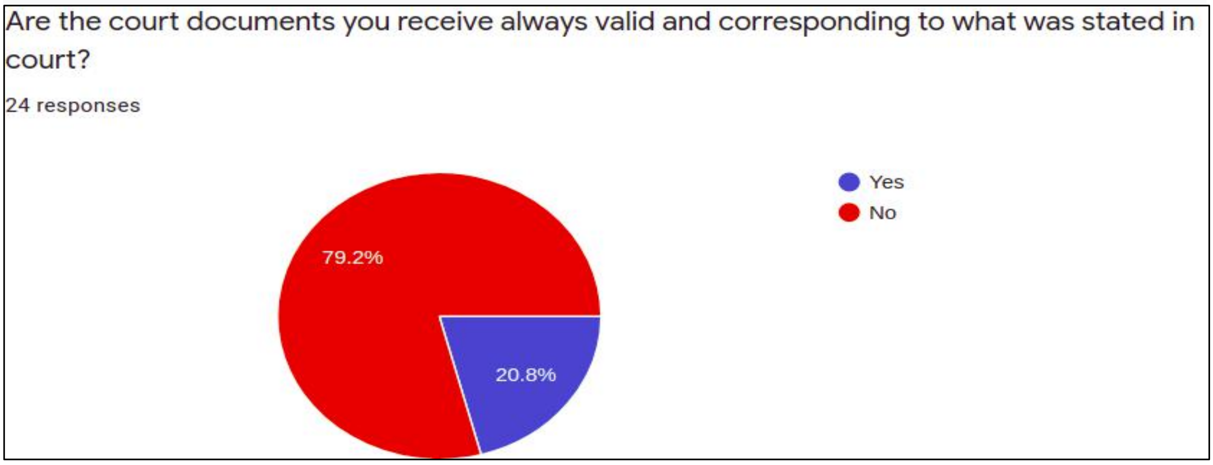
4.1. Results: Data Analysis

Two methods of qualitative data analysis(Manu Bhatia, 2018) were largely employed. ***Content analysis*** is used to analyze documented information in the form of texts, media or physical items.This was used to analyze data for research question one. ***Narrative analysis*** is used to analyze content from sources such as respondent’s interviews, field observations , or surveys. It focuses on using the stories and experiences shared by people to answer the research questions.

4.1.1. Objective 1: To identify security threats of e-government.

From the onset of this project, the researcher sought to identify means in which e-government can leverage on PKI to provide a security and verification mechanism for its services. ***Desktop review*** and user interaction showed that the validity, authenticity and integrity of documents generated by government entities (the Judiciary) are some of the issues that needed to be addressed for e government to be successful, Tri Kuntoro, 2017. Citizenry must be assured of the protection and security of information distributed by government systems, Upadhyaya, 2012 through Tri Kuntoro, 2017.Unauthorized information access and integrity loss are identified as technical threats of e-government by Zaipuna, 2014. In the ***Pre-Implementation survey***, Judges and

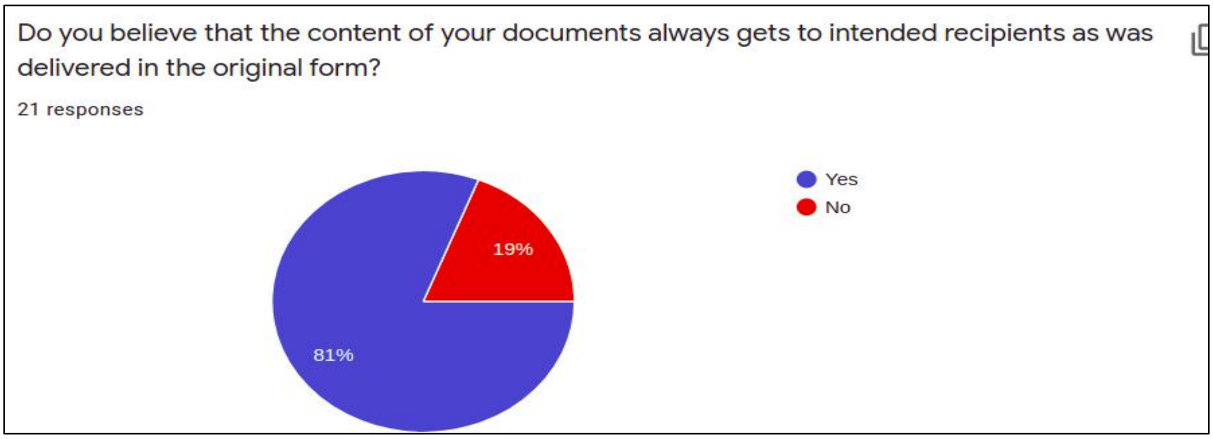
Magistrates were asked whether they had encountered questionable court documents to which 79.2% of advocates and 81% of Judicial Officers responded in the affirmative. 85.7% of Judicial Officers also indicated that they were privy to alteration of their documents. They also alluded to the suggestion that there was need to provide a mechanism to verify court generated documents.



Are the court documents you receive always valid and corresponding to what was stated in court?

24 responses

Figure 47: Advocates responding to validity of court documents



Do you believe that the content of your documents always gets to intended recipients as was delivered in the original form?

21 responses

Figure 48: Judicial officers response to whether document content gets to recipient as intended

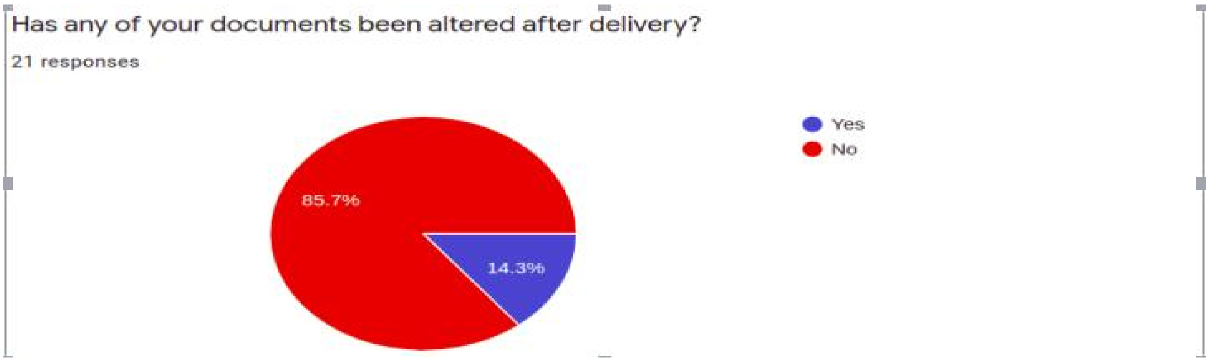


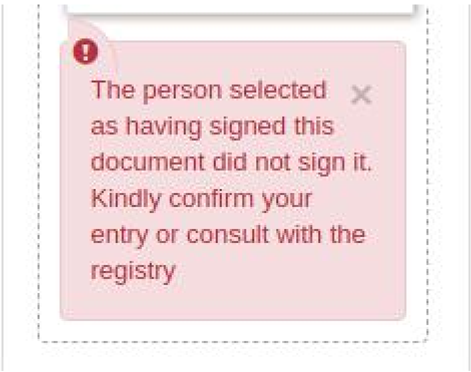
Figure 49: Document alteration

4.1.2. Objective 2: To develop a prototype that uses Public Key Infrastructure in cryptography for verification of documents emanating from the courts.

A software ecosystem that includes a key generation software, a web application that has a document generation and signing module and a verification module, an electronic document management system was developed and set up to achieve this objective. Judicial officers are now able to generate court documents, sign them and view their signature details online while advocates and parties receive the documents on email as well as the web portal on which they can still verify its authenticity and validity.

4.1.2.1. Authentication

That only a genuine user should be able to carry out a transaction is one of the goals of this research. All accounts created in the system are username and password protected and the additional key pair attachment to each user sees to genuine generation of the court documents. Measures such as ensuring that only a Judicial officer who is publicly cause listed as being the one handling a court activity for which a document is to be generated also ensures integrity. The appearance of a stamp with the JO’s name and the court stamp further shows authenticity.

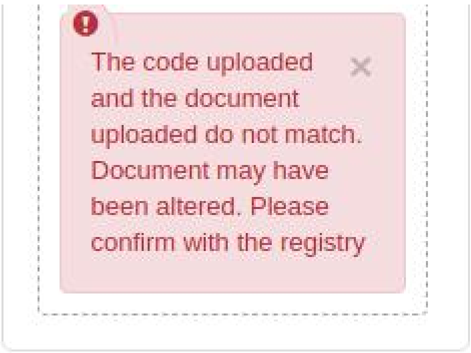


The person selected as having signed this document did not sign it. Kindly confirm your entry or consult with the registry

Figure 50: showing that the purported document generator is not valid

4.1.2.2. **Integrity**

Document integrity requires that no alterations are made on the document during storage or transmission. When a court document is generated, it is converted to PDF and transmitted via a secure API to the EDMS for storage and signing. The private key of the user is used to sign the hashed value of the document and create a signature. Upon reception of the document, court users are able to verify the signature by re-uploading the received document alongside the 'signer's' public key for decryption upon which the hashes are compared. Any variation in the hashes would be evidence of alteration hence invalidating the document.

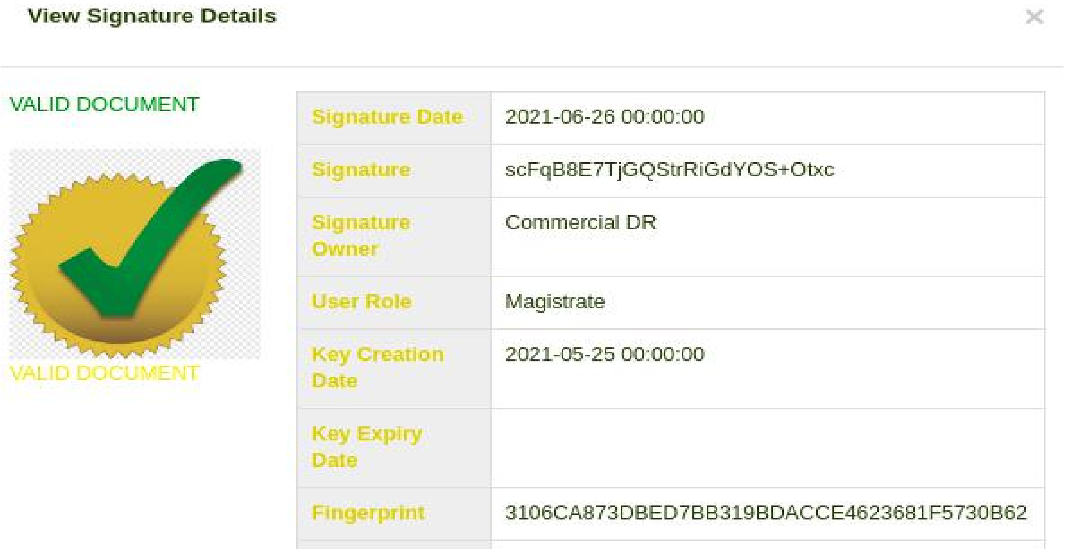


The code uploaded and the document uploaded do not match. Document may have been altered. Please confirm with the registry

Figure 51: showing a document whose content has been altered

4.1.2.3. **Non-Repudiation**

On generation and disbursement of a court document by a rightful Judicial Officer, they cannot deny having created and signed the said document. This is ensured by having secure accounts and generation of a key pair that is linked only to them. This is shown in the digital signature details window that is shown on valid documents



View Signature Details

VALID DOCUMENT

VALID DOCUMENT

Signature Date	2021-06-26 00:00:00
Signature	scFqB8E7TjGQStrRiGdYOS+Otxc
Signature Owner	Commercial DR
User Role	Magistrate
Key Creation Date	2021-05-25 00:00:00
Key Expiry Date	
Fingerprint	3106CA873DBED7BB319BDACCE4623681F5730B62

Figure 52: A valid document

4.1.3. Objective 3: To evaluate court users satisfaction in the existence of a court documents verification mechanism.

This section critically analyzes data collected from the questionnaires issued to the judicial officers and the advocates post deployment of the system. The main aim is to determine if the system meets the laid out requirements to facilitate verification of documents generated in court and whether it solves the problem at hand. The following topics were picked as a basis of the questions issued on the Post-Implementation questionnaires.

4.1.3.1. System Availability

The study sought to check if the various users were able to access their respective pages on the web applications and carry out their tasks.

Judicial Officers: All the Judicial officers in the test phase were able to log in to the system and generate their court documents

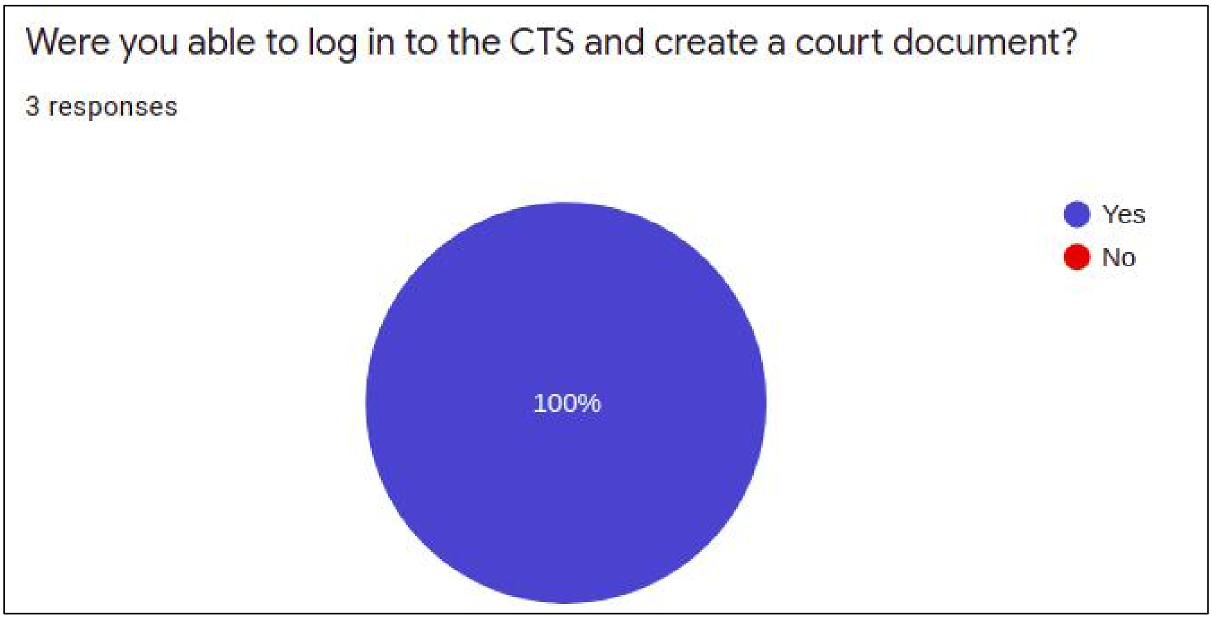


Figure 53: JOs login

Advocates: 8 out of 9 advocates said that they logged in to the e-filing portal to check if their documents were indeed valid

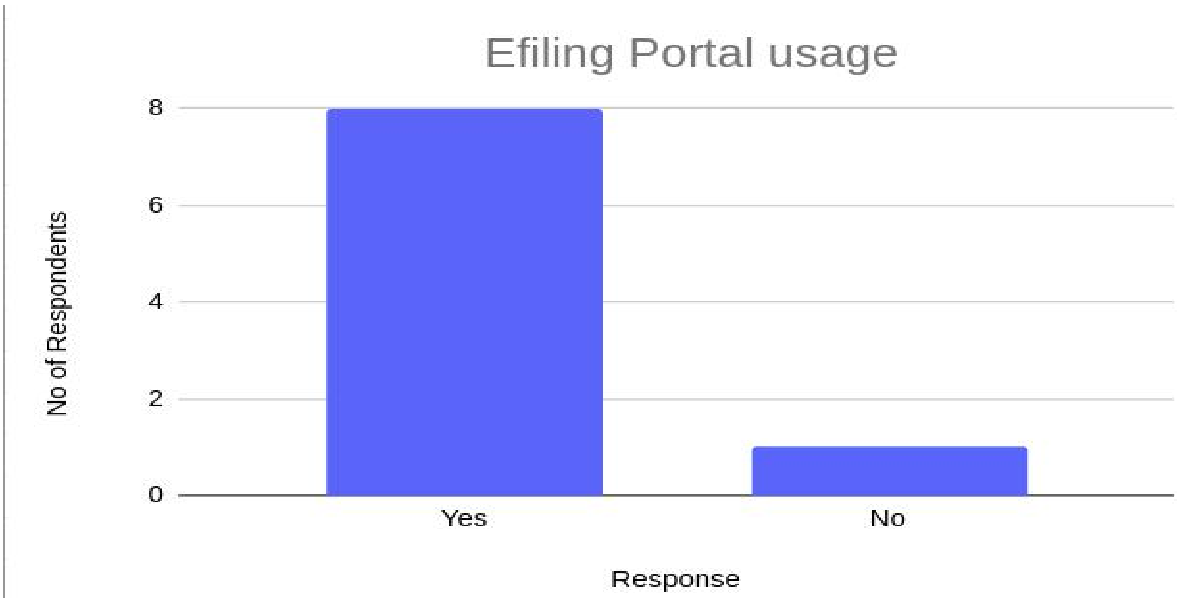
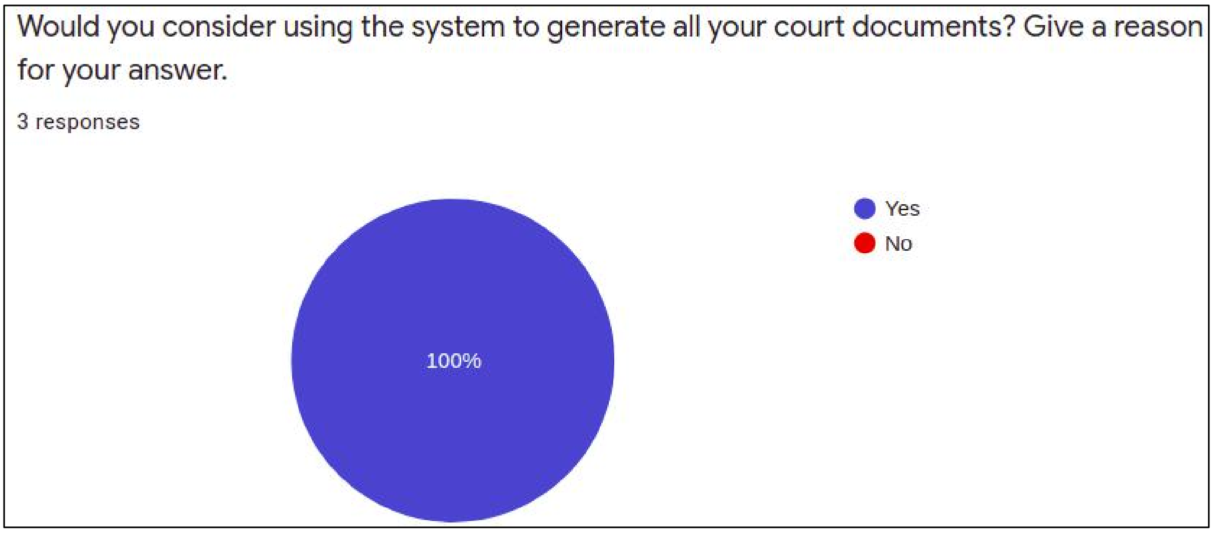


Figure 54: Advocates system usage

4.1.3.2. System Use

The researcher sought to find out if the sensitized users actually used the new features of the system

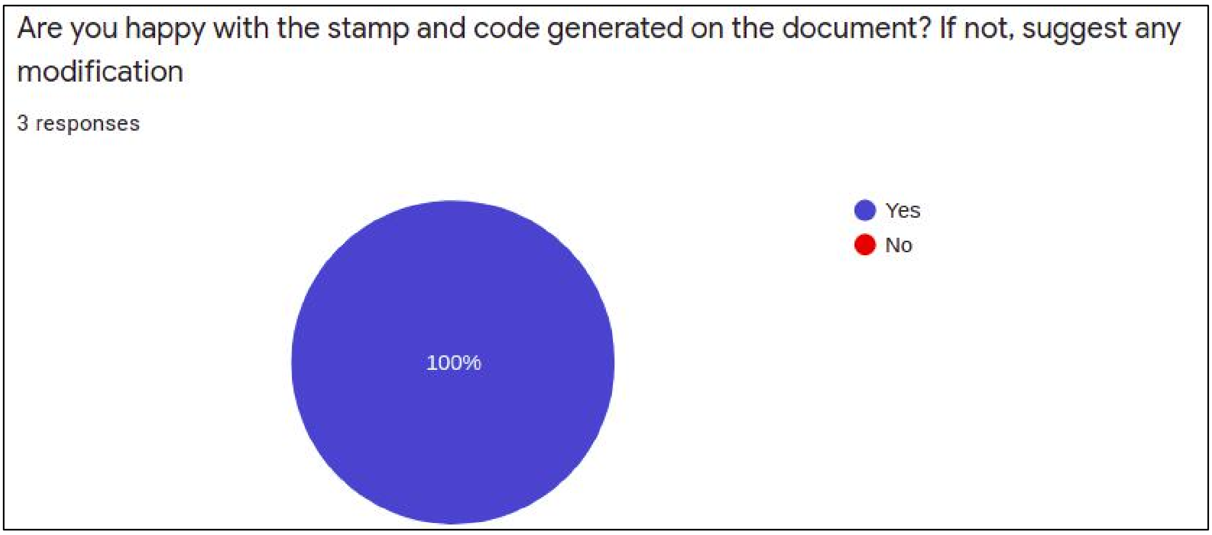
Judicial officers: The 3 Judicial Officers involved in the testing phase were all able to generate their documents from the system and were pleased with the new security features on the document.



Would you consider using the system to generate all your court documents? Give a reason for your answer.

3 responses

Figure 55: Response to whether JOs would use system for doc generation



Are you happy with the stamp and code generated on the document? If not, suggest any modification

3 responses

Figure 56: Are security features on documents satisfactory?

4.1.3.3. **User experience**

To determine the users experience in navigation of the system, they were asked how easy it was to use the system

Judicial Officers: 2 out of 3 of the Judicial Officers found the solution easy to navigate while one indicated that refresher training on system navigation was required

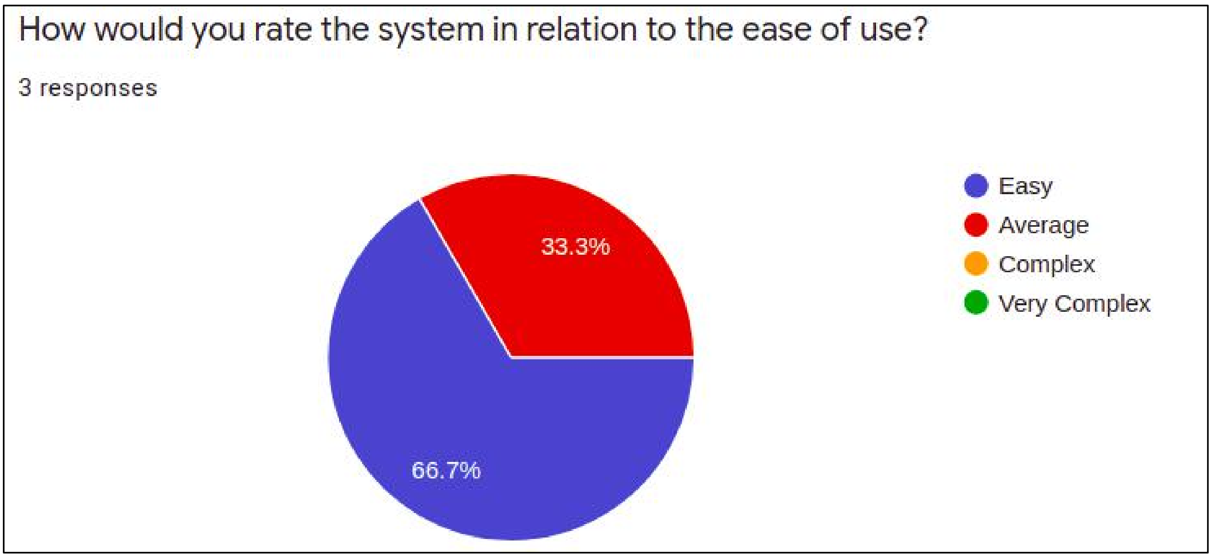


Figure 57: JO System ease of use

Advocates: All advocates indicated that the verification system is easy to use as per the figure below

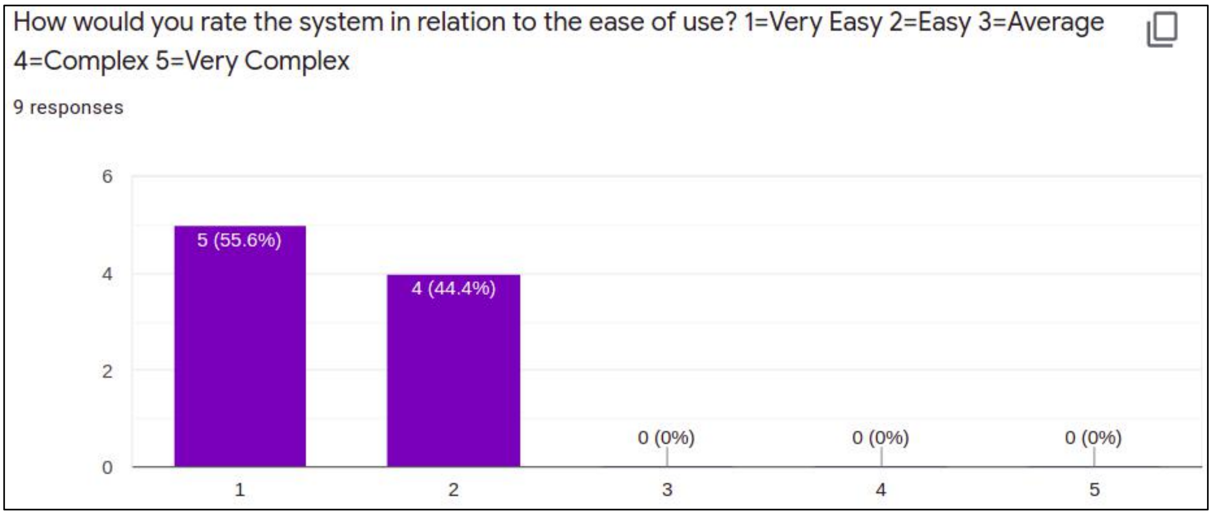
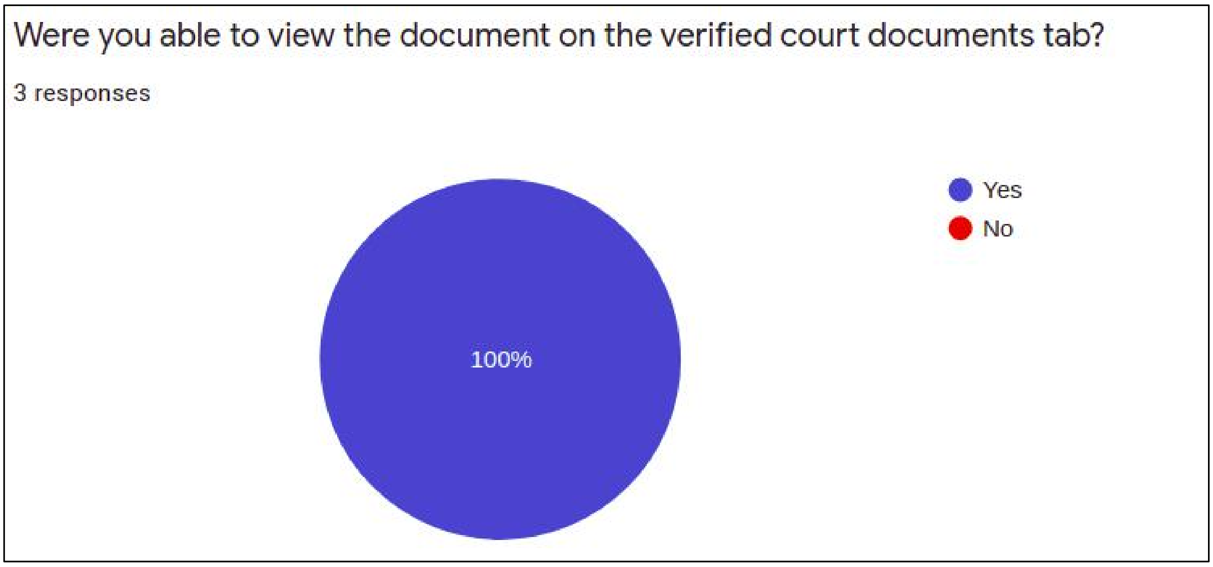


Figure 58: Advocate ease of system use

4.1.3.4. **Accuracy**

The researcher sought to find out if the court documents generation module and the court documents verification module were able to function as expected and produce the correct results

Judicial officers: Upon generating the court documents, the Judicial Officers were able to view them on the new "verified court docs tab in CTS

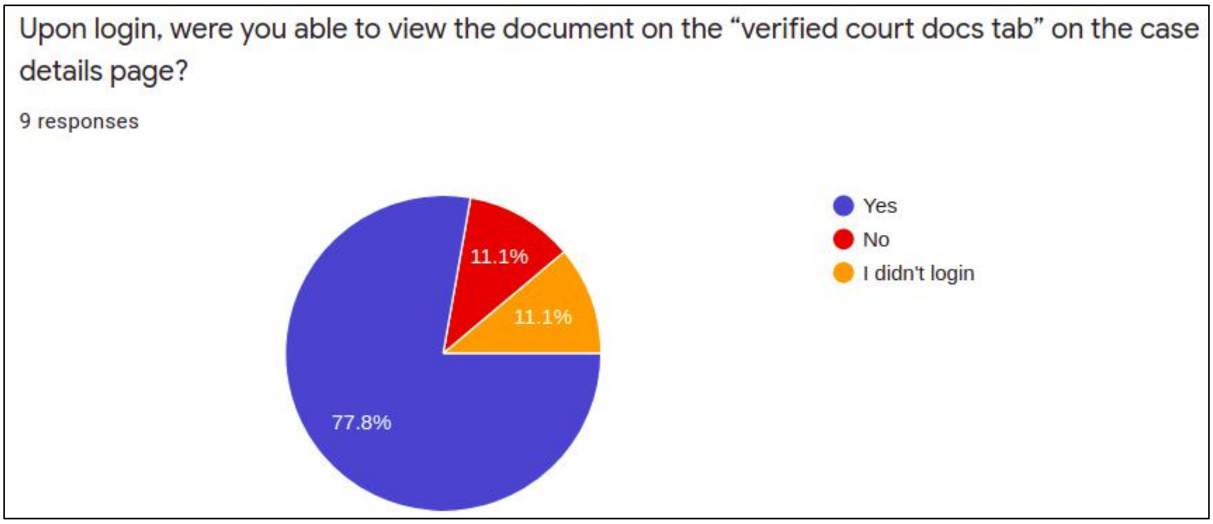


Were you able to view the document on the verified court documents tab?

3 responses

Figure 59: JO system accuracy feedback

Advocates: 100% of the respondents who logged in to the system indicated that they were able to view their documents on the court documents tab

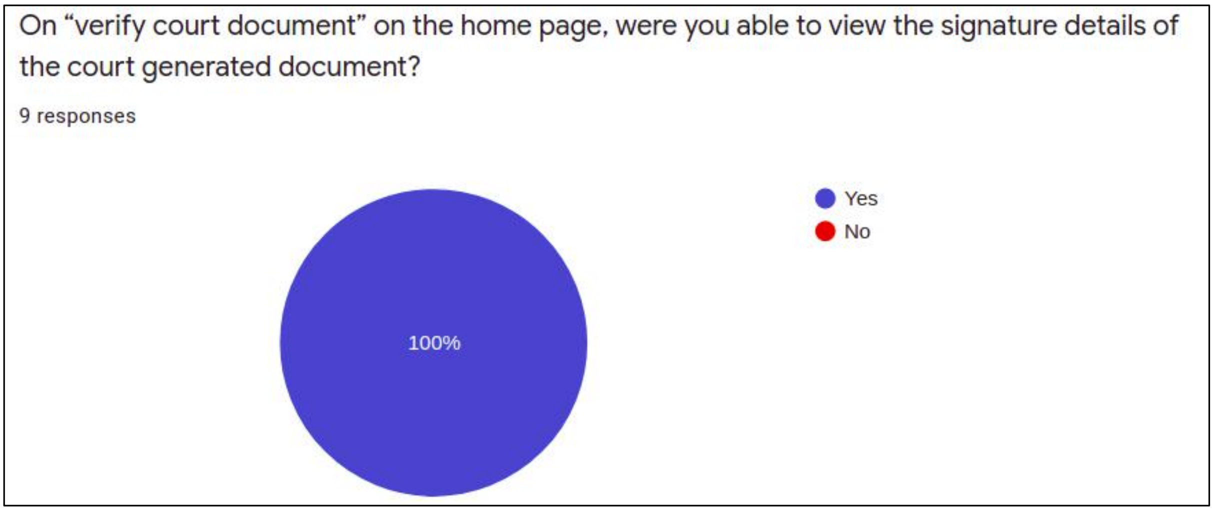


Upon login, were you able to view the document on the "verified court docs tab" on the case details page?

9 responses

Figure 60: Advocate system accuracy

Those who view the documents were also able to view the signature details on the documents page.


On “verify court document” on the home page, were you able to view the signature details of the court generated document?

9 responses

Figure 61: signature details visibility

Of the documents received in different formats, a near 100% validity rate was achieved. One hard copy document and one on email were not system generated hence could not be verified by digital signature.

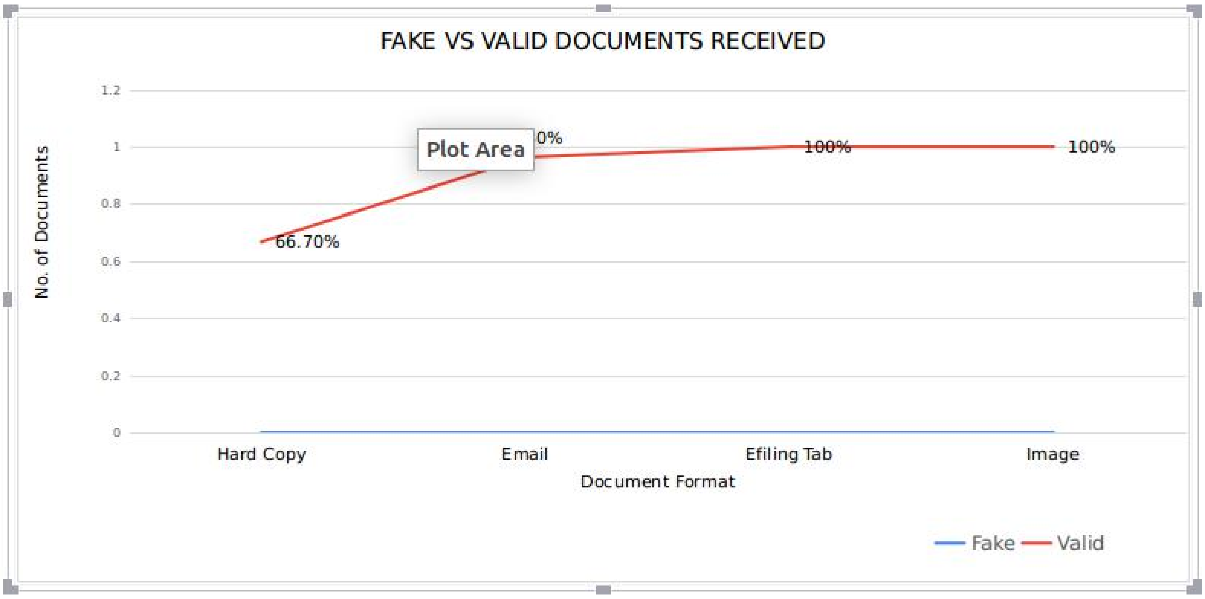


Figure 62: Valid vs fake documents

4.1.3.5. User satisfaction

The researcher sought to find out it the users were satisfied with the new modules and whether it was beneficial to the justice system. All respondents responded in the affirmative indicating user on boarding and readiness to utilize the features.

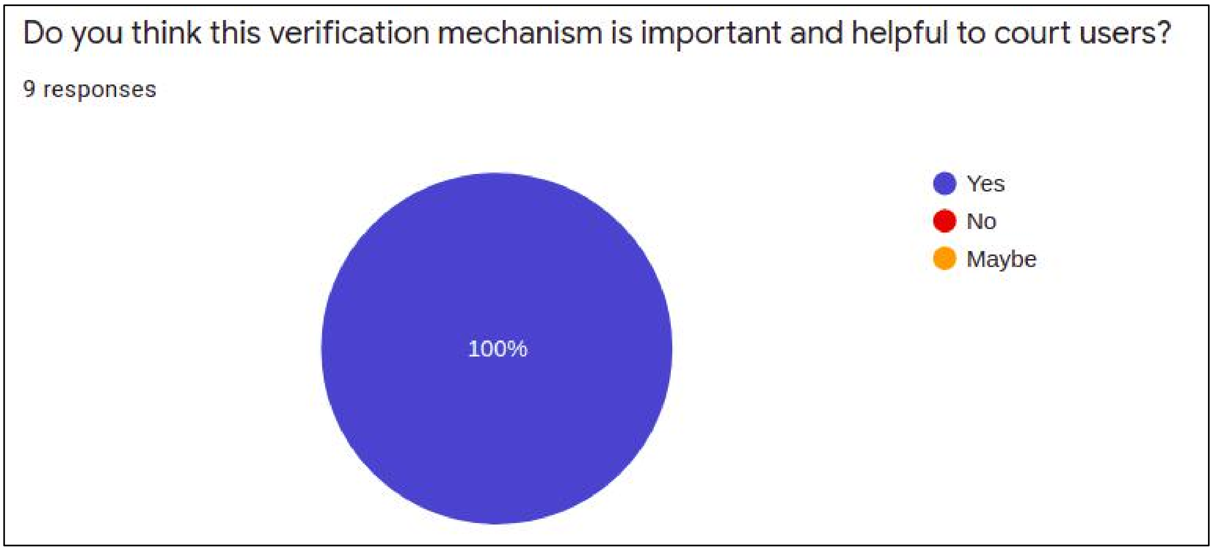
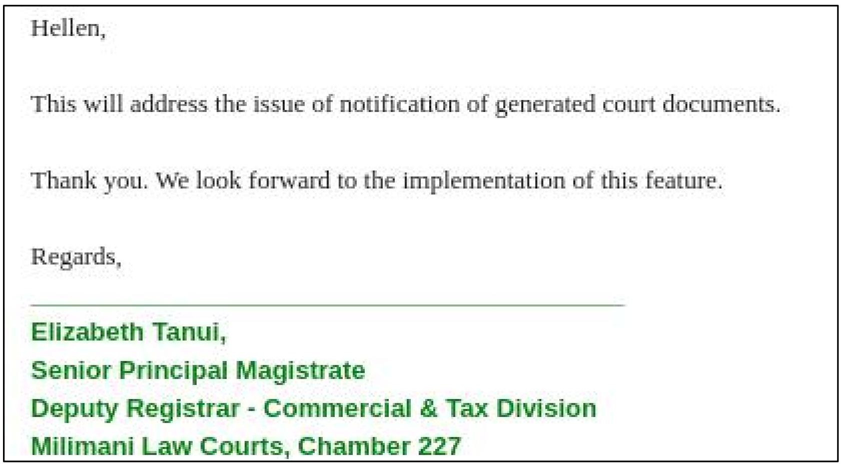


Figure 63: Importance of verification

A comment from the one of the Judicial officers on the notification that now comes with generation of the documents also shows positive reception upon roll out.



Hellen,

This will address the issue of notification of generated court documents.

Thank you. We look forward to the implementation of this feature.

Regards,

Elizabeth Tanui,
Senior Principal Magistrate
Deputy Registrar - Commercial & Tax Division
Milimani Law Courts, Chamber 227

Figure 64: user email feedback

From general comments and free text answer boxes, the following feedback was gathered:

“All documents should be generated via the system”

“The link to download the document directly was very helpful”

“Send SMS when doc is sent”

“Further training and user engagement”

“CTS is indeed quite convenient”

“Water mark of the court station”

Table 5: General user comments

4.2. Summary results and interpretation

Based on the three objectives and the analysis above, it can be submitted that the research was was indeed successful.

		Findings
Objective 1: To identify security threats of e-government. **Research Question 1:** What are the possible security threats to data transmitted electronically in and out of the Judiciary?		
Desktop Review	Desktop Review	Tri Kuntoro, 2017: validity, authenticity and integrity of documents generated by government entities Upadhyaya, 2012 Citizenry need to be assured of the protection and security of information distributed by government systems, through. Zaipuna, 2014: Unauthorized information access and integrity loss
Pre-Implementation survey: broad concepts	Current system usage to track litigation process	Judicial officers and Advocates use the case tracking system and the e-filing system to track their case activities.
	System security confidence	41.7% of advocates and 70% of judges are confident in the security of their accounts.
	Court document	79.2% of advocates have trust

	authenticity and validity	issues with the content delivered in court vs. Content on received document while only 85.7% of JOs have experienced alteration of court documents.
	New technologies adaptation for verification	85% of JOs and 82.5% of advocates were willing to try out new technology for creation, distribution and verification of court documents
Interpretation	Objective 2 was met	
Objective 2: To develop a prototype that uses Public Key Infrastructure in cryptography for verification of documents emanating from the courts. **Research Question 2:** How can we leverage of Public Key Infrastructure to ensure Integrity, authenticity and non-repudiation in e-government systems?		
Tools used	Refer to technology stack on page 65	
System Components	Key generation and revocation application: passwords and keys	Authenticity, integrity and Non-repudiation was achieved by the tests and feedback collected from the users
	Case Tracking System: Document generation and signing module	

	Mayan EDMS: signing, storage and versioning software	
	E-filing document verification module	
Interpretation	Objective 2 was met	
Objective 3: To evaluate court users satisfaction in the existence of a court documents verification mechanism. **Research Question 3:** What are the confidence levels by the system users on incorporation of Public Key Infrastructure?		
Post Implementation survey: broad concepts	System Availability	All users were able to access their respective system
	System Adoption	100% of the users logged in to the system and used CTS to generate documents while 88.9 of advocates used the e-filing portal to view and verify their documents
	User experience	61.2% of users noted that the system was very easy to use while 39% termed it easy citing need for refresher training
	Accuracy	All Judicial officers were able to view their system generated documents of the documents tab and their signature details. Advocates were also able verify the documents received and

		receive accurate feedback from the system. The system was used to verify documents received as hard copy, on email, as image and on the portal and all system generated documents were marked as valid
	User satisfaction	100% of system testers where confident on the importance of use of this verification module for their documents. Other users lauded the initiative in their general comments.
Interpretation	Objective 3 was met	

Table 6: Summary results and interpretation

4.3. Discussion

To understand the threats on documents creation and disbursal from the Judiciary of Kenya, it was evident from the Pre-Implementation survey that there was need to come up with a clear way of verifying documents that are consumed by court users. This is clearly outlined in the methodology chapter including the outlining of functional requirements. The proposed system sought to generate all court documents through the system, include digital signatures and also provide a verification mechanism for external and internal users. Upon completion, system tests and a post implementation survey were carried out. System tests indicated that all outlined requirements were achieved via the system. The survey sought to enquire on : system availability, system adoption, user experience, accuracy and user satisfaction which were all successful as in table 6 above. The original bid to achieve Integrity, Authentication and Non-repudiation in relation to court documents was achieved

4.4. Challenges

Limited or non-existent knowledge on the working of cryptography among a number of the targeted users caused a bit of skepticism and resistance to the introduction of the new feature.

There was a delay in response of the questionnaires issued to the targeted user groups. By the time data analysis was done, only 44 responses had been received. There was a potential to collect more given the large number of court users in Nairobi.

Time limitations did not allow the researcher to build in the key generation functionality into the web based Case Tracking System. There was also no API based application to seamlessly generate the keys and integrate directly into the system.

Chapter 5: Conclusion and Recommendation

5.1. Summary

The project set out to establish the security threats that plague e-government systems and particularly on the documents generated and disbursed from the e-service applications. We also set out to develop an all round software ecosystem to generate documents and sign them while leveraging on the Public Key Infrastructure model. The research was also envisioned to provide a verification mechanism to allow the document consumers to verify the authenticity and integrity of received documents. The researcher also sought to evaluate the success of the system based on a number of metrics as discussed in chapter 4 above.

The use of digital signatures which is one of the major applications of the PKI model is a breakthrough in a step towards reliable and trusted electronic government services. The success of e-government having been pegged on trust, protection and security of the information through application of high security mechanisms between the systems (Upadhyaya, 2012 through Tri Kuntoro, 2017), this verification system is a step towards it. With the main goal having been to achieve document ***integrity***, ***authentication*** and ***non-repudiation***, the prototype fully demonstrates and satisfies this.

5.2. Recommendations

Based on the study, the following recommendations are made in order to improve the process of court documents verification in Kenya:

There is need to map all templates of all statutory and administrative documents that are generated at the court. All the document templates must be coded uniquely to enable easy identification and serialization

There is need to sensitize the public and all court users in the special features of the improved documents and the verification mechanism in order to fully leverage on the developed technology and mitigate any cases of forgery and misrepresentation of the court document generation and disbursal process.

5.3. Further Research Areas

There is room to further improve on the key generation process. Studies should be done to check if there are ways to directly incorporate this process as a module within the system or an independent application via API. There is also need to as study the possible use of other technologies such as block-chain (distributed ledgers) and its possible application in this application where documents got through input cycles from different parties.

5.4. Conclusion

The use of PKI and in particular the use of digital signatures in the generation and verification of documents is a huge success. The researcher has been able to prove the applicability and effectiveness of the developed software through thorough system testing and analysis of the feedback data collected. It is therefore the humble submission of this research that the software set up can be adopted for creation, disbursal and verification of court documents in the Judiciary of Kenya.

References

1. Rasim Alguliyev, Farhad Yusifov,Department of Information Society Problems Institute of Information Technology of ANAS Baku, Azerbaijan, 2015. *“Challenges in E-government: Conceptual Approaches and Views”*
2. C. Martin, A. Bulkan, and P. Klempt, 2011 "*Security excellence from a total quality management approach*," Total Quality Management & Business Excellence, 2011, pp. 345-371
3. Hwang, Min-Shiang, Chun-Ta Li, Jau-Ji Shen, and Yen-Ping Chu, 2004. "*Challenges in E-Government and Security of Information.*" Information & Security: An International Journal 15, no. 1 (2004): 9-20.http://dx.doi.org/10.11610/isij.1501
4. M. Alshehri, S. Drew, 2010. “Implementation of e-Government: Advantages and Challenges”
5. Tri Kuntoro Priyambodo, 2017. *“A Comprehensive Review of e-Government Security*” Asian Journal of Information Technology · January 2017 DOI: 10.3923/ajit.2017.282.286
6. Mohamed D. Waziri and Zaipuna O. Yonah, 2014. *“A Secure Maturity Model for Protecting e-Government Services: A Case of Tanzania*” ACSIJ Advances in Computer Science: an International Journal, Vol. 3, Issue 5, No.11 , September 2014 ISSN : 2322-5157 www.ACSIJ.org
7. Heike Gramckow, Omniah Ebeid et al, 2016. *“GOOD PRACTICES FOR COURTS: Helpful Elements for Good Court Performance and the World Bank’s Quality of Judicial Process Indicators*”
8. Ministry of Health, 2020. “ *First case of corona virus disease confirmed in Kenya*” https://www.health.go.ke/first-case-of-coronavirus-disease-confirmed-in-kenya/ [last accessed 28th March 2021]
9. The Judiciary, 2020. *“Press Statement: Administrative and Contingency Management Plan to Mitigate Covid-19 In Kenya’s Justice Sector”* https://www.judiciary.go.ke/press-statement-administrative-and-

contingency-management-plan-to-mitigate-covid-19-in-kenyas-justice-sector/ [last accessed 28th March 2021]

10. Kiruti Itimu, 2020. *“Kenya Judiciary Launches e-Filing System, Integrates ODPP’s Management and Tracking System*" https://techweez.com/2020/07/01/kenya-judiciary-launches-e-filing-system-integrates-odpps-management-and-tracking-system/ [last accessed 28th March 2021]

11. Hany A. Abdelghaffar Ismail, 2008. *“Citizens*' *Readiness for E-government in Developing Countries*” https://core.ac.uk/download/pdf/17301603.pdf

12. Rao, U. H., & Nayak, U., 2014. The InfoSec Handbook. Apress Media, LLC.

13. Casey Crane, 2020. *“Symmetric Encryption 101: Definition, How It Works & When It’s Used*” https://www.thesslstore.com/blog/symmetric-encryption-101-definition-how-it-works-when-its-used/

14. https://www.sciencedirect.com/topics/computer-science/symmetric-cryptography#:~:text=Symmetric%20cryptography%2C%20known%20also%20as,and%20to%20decrypt%20the%20data.

15. https://publicadministration.un.org/egovkb/en-us/about/unegovdd-framework

16. https://www.ict.go.ke/wp-content/uploads/2019/05/KENYA-E-GOVERNMENT-STRATEGY-2004.pdf

17. Agangiba W. Akotam, Millicent S. Kontoh, and Albert K. Ansah, 2013. *“Int. J. Electronic Governance, Vol. 6, No. 2, 2013 E-governance public key infrastructure (PKI) model”* https://www.researchgate.net/publication/264821916_E-governance_public_key_infrastructure_PKI_model

18. Ali M. Al-Khouri. “*PKI in government identity management systems Emirates Identity Authority, Abu Dhabi, United Arab Emirates*”. https://www.researchgate.net/publication/51909206_PKI_in_Government_Identity_Management_Systems

19. KENYA INFORMATION AND COMMUNICATIONS ACT, CHAPTER 411A, 1998 http://kenyalaw.org/kl/fileadmin/pdfdownloads/Acts/KenyaInformationandCommunicationsAct(No2of1998).pdf

20. http://kenyalaw.org/kl/fileadmin/pdfdownloads/Acts/ComputerMisuseandCybercrimesActNo5of2018.pdf

21. Kenya Gazette Supplement No. 26 (Acts No. 1), 2020. http://kenyalaw.org/kl/fileadmin/pdfdownloads/AmendmentActs/2020/BusinessLawsAmendmentAct2020.PDF

22. Santiago de Chile, 2014. "*Electronic land register which forcefully eliminates real estate fraud and corruption IPRA-CINDER XIX World Registry Law Congress"* https://www.rik.ee/sites/www.rik.ee/files/elfinder/article_files/Electronic%20land%20register%20which%20forcefully%20eliminates%20real%20estate%20fraud%20a%20%20%20.pdf

23. National Public Key Infrastructure, https://ca.go.ke/industry/e-commerce-development/national-public-key-infrastructure/

24. "*Estonia a successfully integrated population-registration and identity management system delivering public services effectively*" http://documents1.worldbank.org/curated/en/873061495178335850/pdf/115147-WP-EstoniaIDPopregistryIDcasestudyNovweb-PUBLIC.pdf

25. AS Sertifitseerimiskeskus, 2003. "*The Estonian ID Card and Digital Signature Concept Principles and Solutions"* https://www.id.ee/public/The_Estonian_ID_Card_and_Digital_Signature_Concept.pdf

26. Tallinn December, 2013. "*eID Estonian experience*", https://nvvb.nl/media/cms_page_media/758/13%20Mari%20Pedak%20eID%20Estonian%20experience.pdf

27. Ingmar Vali, Kadri Laud, Loori Paadik, 2014. "*Electronic land register which forcefully eliminates real estate fraud and corruption*" https://www.rik.ee/sites/www.rik.ee/files/elfinder/article_files/Electronic

%20land%20register%20which%20forcefully%20eliminates%20real%20estate%20fraud%20a%20%20%20.pdf

28. S. Benabdallah, S. Guemara El Fatmi, N. Boudriga, 2002.*“Security issues in e-government models: what governments should do?”* Conference Paper · February 2002 DOI: 10.1109/ICSMC.2002.1173445 · Source: IEEE Xplore

29. Geoffrey Chemwa, 2012. “*OPTIMISING RATIONAL DECISION MAKING WHEN REASONING ABOUT ENHANCING PKI SECURITY FOR eGOVERNMENT: A Quantitative Decision Support Approach*”. http://erepository.uonbi.ac.ke/bitstream/handle/11295/97477/Chemwa_Optimizing%20Rational%20Decision%20Making%20When%20Reasoning%20About%20Enhancing%20Pki%20Security%20for%20Governmen-%20a%20Quantitative%20Decision%20Support%20Approach.pdf?sequence=1&isAllowed=y

30. https://www.indiapki.org/

31. https://www.medien.ifi.lmu.de/lehre/ss14/swal/presentations/topic2-saltuk_kosan-DesignAndCreation.pdf

32. SWAL Ozan Saltuk & Ismail Kosan , 2014. “*Design and Creation*“ https://www.medien.ifi.lmu.de/lehre/ss14/swal/presentations/topic2-saltuk_kosan-DesignAndCreation.pdf

33. Jaime Pereira, João Varajão & Nilton Takagi, 2021. “*Evaluation of Information Systems Project Success – Insights from Practitioners, Information Systems Management”,* DOI:10.1080/10580530.2021.1887982. https://www.tandfonline.com/doi/full/10.1080/10580530.2021.1887982

34. *“Did it Work? 5 Tools for Evaluating the Success of Your Project”* https://www.sumac.com/blog/nonprofit-management-and-hr/did-it-work-5-tools-for-evaluating-the-success-of-your-project/

35. https://libguides.usc.edu/writingguide/abstract

36. Manu Bhatia, 2018. *“Your Guide to Qualitative and Quantitative Data Analysis methods*” https://humansofdata.atlan.com/2018/09/qualitative-quantitative-data-analysis-methods/

Appendices

Appendix A: Judicial Officers Pre-Implementation questionnaire

A SURVEY TO CHECK THE LEVEL OF CONFIDENCE BY JUDGES AND MAGISTRATES ON THE SECURITY AND VALIDITY OF DOCUMENTS GENERATED IN COURT AS TRANSMITTED TO THEIR RECIPIENTS

1. Do you use the Case Tracking System to disburse your documents eg. orders, rulings?

   ○ Yes

   ○ No

If not, how are they disbursed and why do you prefer not to use CTS?

____

______

2. Do you feel that your e-filing account is safe and only accessible by you?

   ○ Yes

   ○ No

If not, what would you suggest as an additional security feature?

____

______

3. Do you believe that the content of your documents always gets to intended recipients as was delivered in the original form?

   ○ Yes

   ○ No

4. Has any of your documents been altered after delivery?

   ○ Yes

   ○ No

If yes, what incident did you encounter and what was the impact on the case?

____

5. Would you like to have a mechanism through which the court users are able to verify the source and content of court documents once transmitted?
   - ○ Yes
   - ○ No
6. Would you like to try a new technology to ensure integrity and authenticity of court documents?
   - ○ Yes
   - ○ No

Appendix B: Advocates Pre-Implementation questionnaire

A SURVEY TO CHECK THE LEVEL OF CONFIDENCE BY ADVOCATES ON THE SECURITY AND VALIDITY OF DOCUMENTS GENERATED IN COURT.

7. How often do you log into the e-filing system?

   o Daily
   o Weekly
   o Monthly

8. Do you feel that your e-filing account is safe and only accessible by you?

   o Yes
   o No

9. How do you receive you court documents?

   o Email
   o Hard copies
   o E-filing court documents tab

10. Which is the best way to receive documents from court? Which channel would you trust best?

    o Email
    o Hard copies
    o E-filing court documents tab

11. Do you trust the source of court documents based on the signatures appended on the documents?

    o Yes
    o No
    Explain? ____

12. Are the court documents you receive always valid and corresponding to what was stated in court?

    o Yes
    o No

If yes, how did you tell? ____

13. Would you wish to verify the source and the author of documents from court?
    - o Yes
    - o No
14. Have you experienced digital signatures?
    - o Yes
    - o No
15. What features would you want added to court documents to ensure their authenticity?____

Appendix C: Judicial Officers Post-Implementation questionnaire

A SURVEY TO GATHER FEEDBACK ON THE NEWLY DEVELOPED FEATURES BY JUDGES AND MAGISTRATES

1. Were you able to log in to the CTS and create a court document?

○ Yes

○ No

2. Were you able to view the document on the verified court documents tab?

○ Yes

○ No

3. Would you consider using the system to generate all your court documents? Give a reason for your answer.

○ Yes

○ No

Why?____

4. Are you happy with the stamp and code generated on the document? If not, suggest any modification

○ Yes

○ No

5. How would you rate the system in relation to the ease of use?

○ Easy

○ Average

○ Complex

○ Very Complex

6. Suggest improvement areas

a) ____

b) ____

c) ____

Appendix D: Advocates Post-Implementation questionnaire

A SURVEY TO GATHER FEEDBACK ON THE NEWLY DEVELOPED VERIFICATION FEATURES BY ADVOCATES

1. Have you received any documents from court since Tuesday 22nd June 2021 to date?

   ○ Yes

   ○ No

2. How many documents did you receive___________________________

3. In which format did you receive the documents ?

   ○ Hard copy _________

   ○ Email ___________

   ○ On the verified court documents page ________

   ○ Image

4. How many documents of each of these formats did you receive ?

   ○ Hard copy _________

   ○ Email ___________

   ○ On the verified court documents page ________

   ○ Image

5. Did you use the e-filing portal to verify the documents?

   ○ Yes

   ○ No

6. How many documents of each were marked as valid on the system?

   ○ Hard copy _________

   ○ Email ___________

   ○ On the verified court documents page ________

   ○ Image ____________

7. How many documents of each were marked as fake on the system?

   ○ Hard copy _________

   ○ Email ___________

○ On the verified court documents page ________

○ Image ____________

8. On “*verify court document*” on the home page, were you able to view the signature details of the court generated document?

   ○ Yes

   ○ No

9. If yes, was the message displayed to show correctness adequate?

   ○ Yes

   ○ No

10. Upon login, were you able to view the document on the “*verified court docs tab*” on the case details page?

    ○ Yes

    ○ No

11. Are you happy with the stamp and code generated on the document to aid in verification?

    ○ Yes

    ○ No

12. How would you rate the system in terms of correctness or accuracy in verification of the documents?

    ○ Accurate

    ○ Somehow accurate

    ○ Not Accurate

13. How would you rate the system in relation to the ease of use?

    ○ Easy

    ○ Very easy

    ○ Average

    ○ Complex

    ○ Very Complex

14. Do you think this verification mechanism is important and helpful to court users?

    ○ Yes

○ No

○ Maybe

15. Please give suggestions on how to better improve the system

a) ______________________________

b) ______________________________

c) ______________________________

d) ______________________________

Appendix E: Sample Code

Send PDF docments to MAYAN EDMS And embed digital signature

```
function send_to_mayan_and_sign($file_id, $file_name, $readable_name,
$src, $user) {
        $ro = $this->CI->db->from('files f')->join('file_types ft',
                'ft.file_type_id=f.file_type_id')->where(array('file_id' =>
$file_id))->get()->row();
        if ($ro->mayan_file_ref_id > 0) {
            $this->delete_document($ro->mayan_file_ref_id);
        }
        $mayan_file_type = $this->check_if_exist_file_type($ro->file_type_id,
trim($ro->description));
        $doc = $this->upload_doc_to_mayan_direct($mayan_file_type,
json_encode($ro), $file_name, $readable_name, $src);
        if (is_object($doc) and $doc->id > 0) {
            //get the key_id for the user signing the document
            //$user = 15457;
            $doc_details = $this->mayan_document_download($doc->id);
//              var_dump($doc_details); die;
            if ($doc_details->latest_version != NULL) {
                $version_url = $doc_details->latest_version->url;
                $checksum = $doc_details->latest_version->checksum;
                $version = explode('/', $version_url)[7];
            } else {
                $doc_details = $this-
>mayan_document_download_version($doc->id);
                $checksum = $doc_details->results[0]->checksum;
                $version_url = $doc_details->results[0]->url;
                $version = explode('/', $version_url)[7];
            }
```

```
//          echo getenv('SIGNATURE');
            if (getenv('SIGNATURE') !== TRUE) {
                $sql = "SELECT * from key where uacc_id_fk = $user and
key_type = 1 and deleted = 0";
                $keys = $this->CI->db->query($sql)->row();
                $d = $this->CI->db->query($sql)->num_rows();

                if ($d > 0) {
                    $keys->key_id;
                    $key_id = str_split($keys->fingerprint, 8)[4];
                    $signature = $this->sign_document($doc->id, $version,
$key_id);

                    $doc_details = $this-
>mayan_document_download_version($doc->id);
//                  $doc_signature = $this->get_document_signature($doc->id,
$version);
                    $mayan_db = $this->CI->load->database('mayan_db', TRUE);
                    $sql = "SELECT max(id) as last_version FROM
documents_documentversion dv where dv.document_id = $doc->id";
                    $last_version = $mayan_db->query($sql)->row()-
>last_version;

                    $sql = "SELECT * from
document_signatures_signaturebasemodel where document_version_id =
$last_version";
                    $signature = $mayan_db->query($sql)->row();
                    $d = $mayan_db->query($sql)->num_rows();
//                      $signature_id = explode('/', $doc_signature->results[0]-
>url)[10];

                    if ($d > 0) {
```

```
            $file_signature = array('file_id' => $file_id,
              'mayan_file_id' => $doc->id,
              'file_version_id' => $last_version,
              'signature_id' => $signature->id,
              'signature' => $signature->signature_id,
              'signature_date' => $signature->date,
              'fingerprint' => $signature->public_key_fingerprint,
              'tracking_number_fk' => $signature-
>public_key_fingerprint,
              'checksum' => $checksum);
            $this->CI->db->insert('file_signature', $file_signature);
p//           $cabinet_doc = $this->add_doc_to_mayan_cabinet($doc-
>id, getenv('RECENT_UPLOAD_CABINET_ID'));

            return $doc->id;
          } else {
            return -1; //signature not created
          }
        } else {
          return -2; //no key available
        }
      } else {
        //  echo 'true';
        return $doc->id;
      }
    } else {
      return -3;     }   }
```

<u>Verify an uploaded document</u>

```
function send_to_mayan_and_validate($file_name, $src, $user) {
    $mayan_file_type = 11;
    $doc = $this->upload_doc_to_mayan_validate($mayan_file_type,
$file_name, $src);
```

```
        if (is_object($doc) and $doc->id > 0) {
            //get the key_id for the user signing the document
            //$user = 15457;
            $doc_details = $this->mayan_document_download($doc->id);
//                  var_dump($doc_details); die;
            if ($doc_details->latest_version != NULL) {
                $version_url = $doc_details->latest_version->url;
                $checksum = $doc_details->latest_version->checksum;
                $version = explode('/', $version_url)[7];
            } else {
                $doc_details = $this-
>mayan_document_download_version($doc->id);
                $checksum = $doc_details->results[0]->checksum;
                $version_url = $doc_details->results[0]->url;
                $version = explode('/', $version_url)[7];
            }
            if (getenv('SIGNATURE') !== TRUE) {
                $sql = "SELECT * from key where uacc_id_fk = $user and
key_type = 1 and deleted = 0";
                $keys = $this->CI->db->query($sql)->row();
                $d = $this->CI->db->query($sql)->num_rows();
                if ($d > 0) {                    $keys->key_id;
                    $key_id = str_split($keys->fingerprint, 8)[4];
                    $signature = $this->sign_document($doc->id, $version,
$key_id);
                    $doc_details = $this-
>mayan_document_download_version($doc->id);
//                      $doc_signature = $this->get_document_signature($doc->id,
$version);
                    $mayan_db = $this->CI->load->database('mayan_db', TRUE);
                    $sql = "SELECT max(id) as last_version FROM
documents_documentversion dv where dv.document_id = $doc->id";
```

```
                    $last_version = $mayan_db->query($sql)->row()-
>last_version;
                    $sql = "SELECT * from
document_signatures_signaturebasemodel where document_version_id =
$last_version";
                    $signature = $mayan_db->query($sql)->row();
                    $d = $mayan_db->query($sql)->num_rows();
                    $ret_array = array("checksum" => $checksum, "id" =>
$doc->id);
                    if ($d > 0) {
                        return $ret_array;
                    } else {
//                    echo "1";
//                    die;
                        return -1; //signature not created
                    }
                } else {
                    return -2; //no key available
                }
            } else {
                // echo 'true';
                return $doc->id;
            }
        } else {
//            echo "3";//            die;
            return -3;
        }    }
```