A Public Key Infrastructure Model for Verification of Court Documents: The Judiciary of Kenya

Hellen N. Kabira
School of Computing and Informatics
The University of Nairobi, Kenya

Robert O. Oboko
School of Computing and Informatics
The University of Nairobi, Kenya

ABSTRACT

The objective of this paper is to review the system developed that incorporates Public Key Infrastructure technology and in particular the use of digital signatures to enable the verification of documents generated in the Judiciary of Kenya. It reviews the existing technical threats on information creation and transmission and addresses the measures implemented to mitigate these.

General Terms

Public Key Infrastructure, Digital Signatures, Security

Keywords

Document Security, Court documents

1. INTRODUCTION

Present day government is heavily invested 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.

2. LITERATURE REVIEW

2.1. 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, 2008 [1]. 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 and Farhad , 2015 [2] 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*

2.2. Conceptual Design

The conceptual model as illustrated in figure 1 below is aimed 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

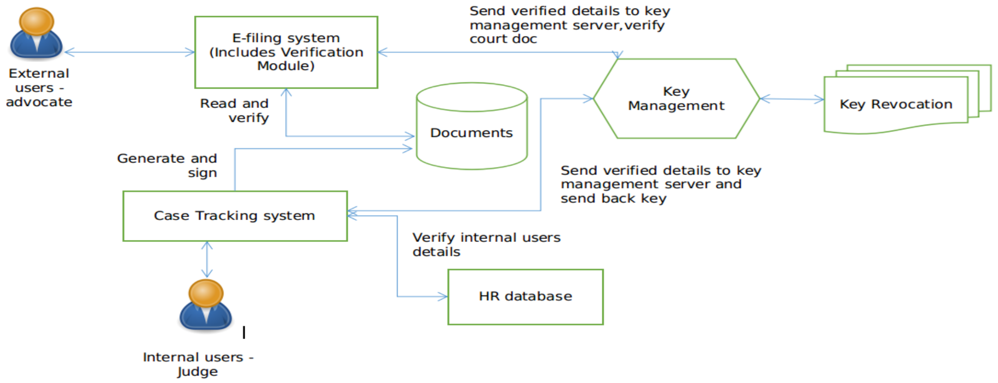

External users - advocate
E-filing system (Includes Verification Module)
Send verified details to key management server,verify court doc
Key Management
Key Revocation
Read and verify
Documents
Generate and sign
Send verified details to key management server and send back key
Case Tracking system
Verify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

Figure 1: Conceptual design

3. METHODOLOGY

3.1. Type of research

This study undertook a qualitative approach to research in which non-numerical data was collected and analyzed.

3.2. Data collection Techniques

Desktop literature review and interviews were used to collect data.

3.3. Data Analysis

Content analysis was used to analyze documented information while narrative analysis was used to analyze content from sources such as respondent's surveys and the test cases.

3.4. System Design and Development

This section illustrates the components of the system and the communication between them to achieve seamless system functionality.The diagram below portrays the high-level system architecture.

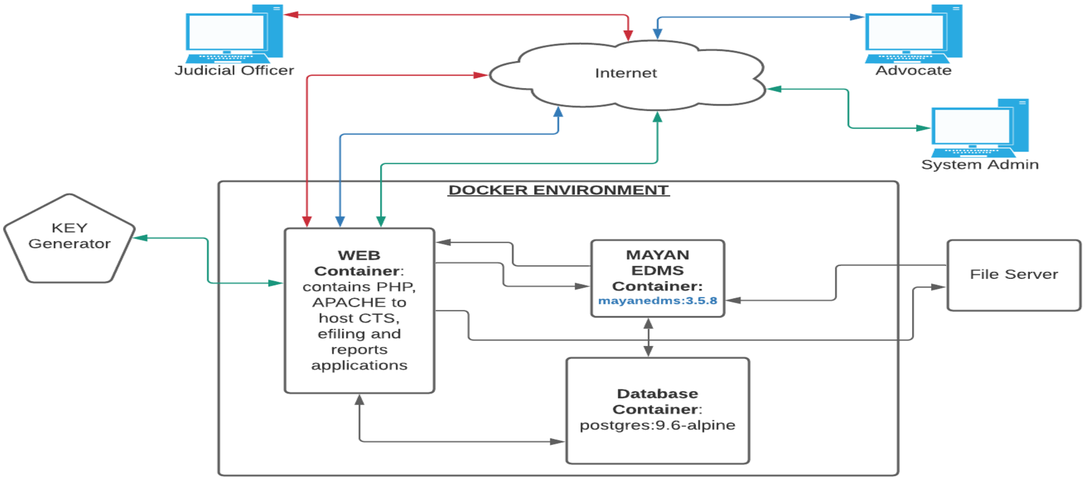

Judicial Officer
Internet
Advocate
System Admin
DOCKER ENVIRONMENT
KEY Generator
WEB Container: contains PHP, APACHE to host CTS, efiling and reports applications
MAYAN EDMS Container: mayanedms:3.5.8
File Server
Database Container: postgres:9.6-alpine

Figure 2: System Architecture

System Components

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

b. 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

c. 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

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

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

f. 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

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

3.5. Flowcharts

Algorithm to create and sign a document

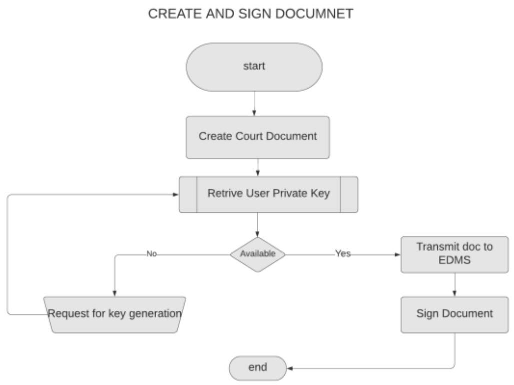


Figure 3: Create and sign document

Algorithm to verify a document

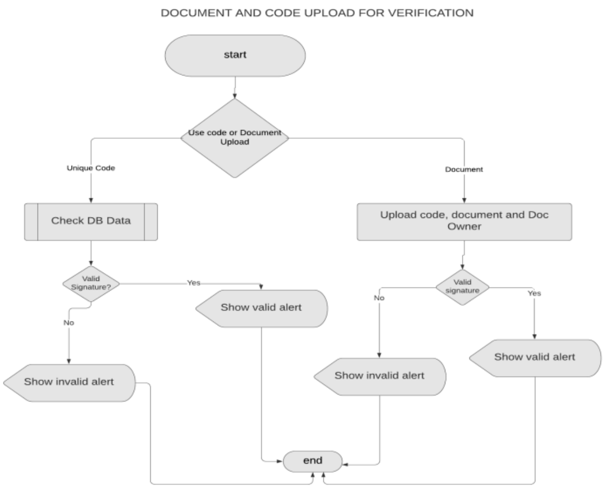
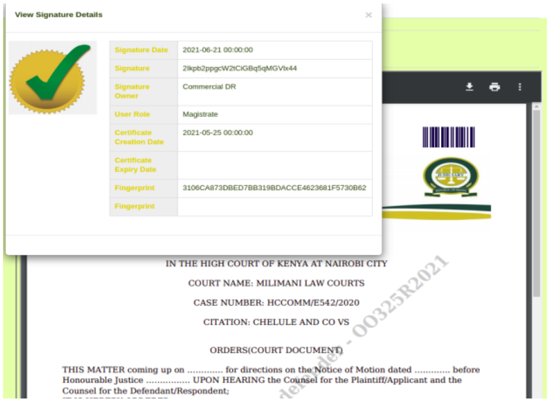


Figure 4: verify a document

3.6. The system

A system generated document and its signature details



View Signature Details

Signature Date	2021-06-21 00:00:00
Signature	2Ikpb2ppgcW2tCiGBq5qMGVlx44
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

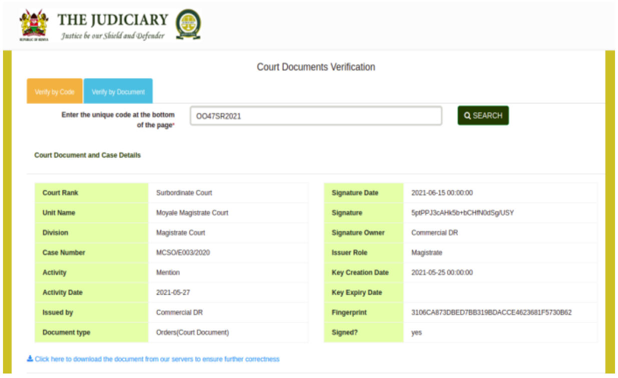
ORDERS(COURT DOCUMENT)

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;

defender - OO325R2021

Figure 5: verify document on public portal

Verifying a document on the public portal



THE JUDICIARY
Justice be our Shield and Defender

Court Documents Verification

Verify by Code | Verify by Document

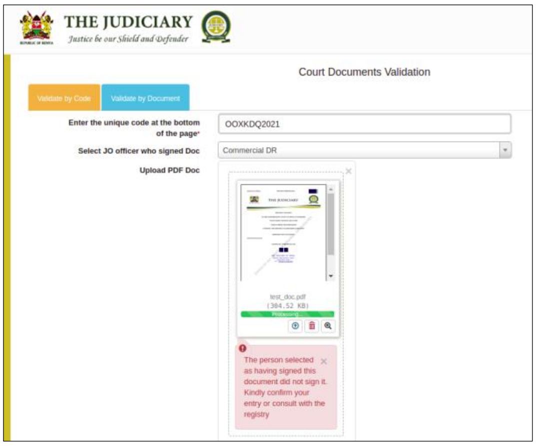
Enter the unique code at the bottom of the page*: OO47SR2021 SEARCH

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 6: Details of valid document



THE JUDICIARY
Justice be our Shield and Defender

Court Documents Validation

Validate by Code | Validate by Document

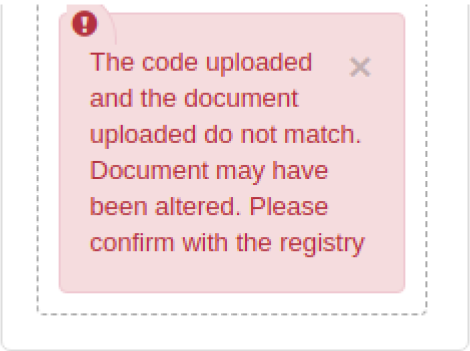
Enter the unique code at the bottom of the page*: OOXKDQ2021

Select JO officer who signed Doc: Commercial DR

Upload PDF Doc: test_doc.pdf (384.52 KB) Processing...

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

Figure 7: A document failing the authenticity test



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

Figure 8: A document failing the integrity test shown above

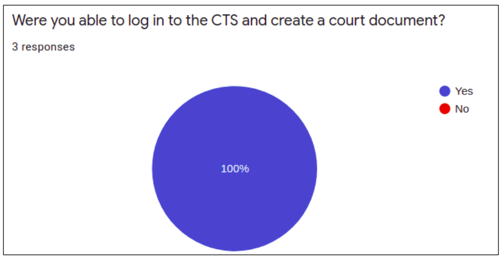
4. RESULTS AND FINDINGS

4.1. Results

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.

4.1.1. System Availability

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

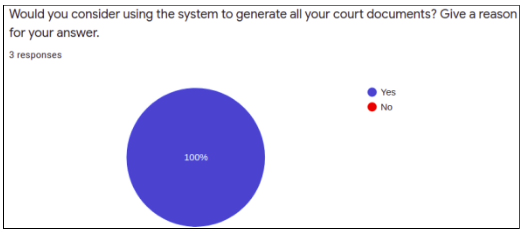


Were you able to log in to the CTS and create a court document?

Figure 9: System availability

4.1.2. *System Adoption*

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



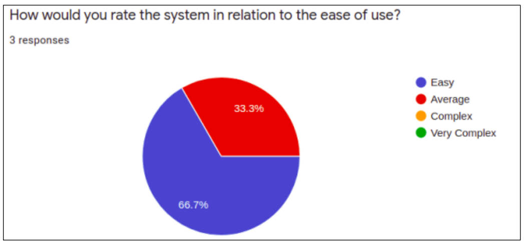
Would you consider using the system to generate all your court documents? Give a reason for your answer.

Figure 10: System adoption

4.1.3. *User Experience*

To determine the users experience in navigation of the system, Judicial Officers were asked

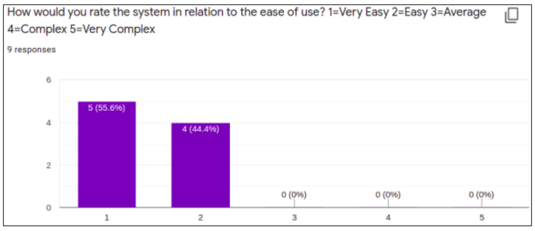
how easy it was to use the system



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

Figure 11: System ease of use by Judicial officers

Advocates termed the verification system easy to use

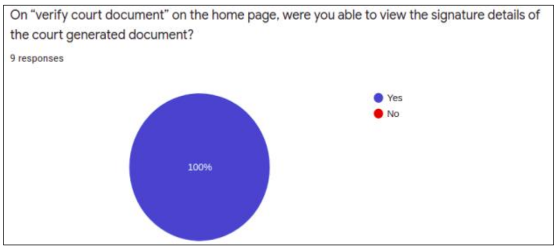


How would you rate the system in relation to the ease of use? 1=Very Easy 2=Easy 3=Average 4=Complex 5=Very Complex

Figure 12: Ease of use by advocates

4.1.4. *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



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

Figure 13: System accuracy

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.

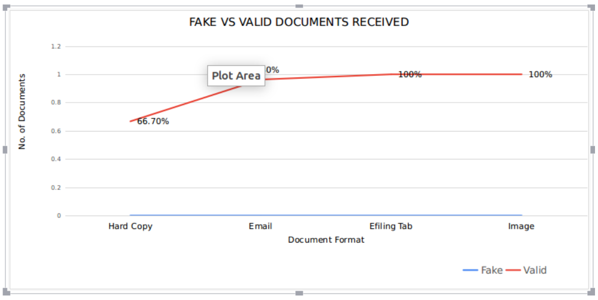
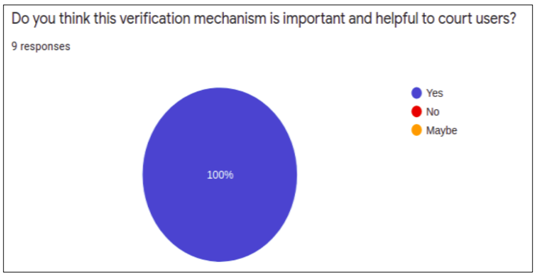


Figure 14: Valid vs fake documents

4.1.5. *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.



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

Figure 15: User satisfaction

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

Table 1: General User comments

● "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"

4.2. 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. The original bid to achieve Integrity, Authentication and Non-repudiation in relation to court documents was achieved

5. CONCLUSION

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 [3], 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. 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.

5.2. 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.

5.3. Future Work

There is room to 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.

6. ACKNOWLEDGEMENT

The authors wish to appreciate the University of Nairobi for creating a enabling environment to conduct this research. Gratitude is extended to all participants of the requirements gathering survey and those who reviewed and tested the developed system.

7. REFERENCES

[1] 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

[2] 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”.

[3] 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