DISOBEYING ORDERS:

THE SCRUTINY OF KENYA'S ELECTORAL TECHNOLOGY

```
Aug  9 18:38:29 appc01srv05 sshd[1368692]: pam_unix(sshd:session): session closed for user
Aug  9 18:38:29 appc01srv05 systemd-logind[1349]: Session 680654 logged out. Waiting
o exit.
Aug  9 18:38:29 appc01srv05 systemd-logind[1349]: Removed session 680654.
Aug  9 18:38:29 appc01srv05 sshd[1368699]: Connection from 192.168.95.64 port
 port 22 rdomain ""
Aug  9 18:38:29 appc01srv05 sshd[1368699]: Accepted key RSA SHA256:+G/bFNLM
2Q7HDfMn/w found at /home/saes/.ssh/authorized_keys:1
Aug  9 18:38:29 appc01srv05 sshd[1368699]: Postponed publickey for saes
8 ssh2 [preauth]
Aug  9 18:38:29 appc01srv05 sshd[1368699]: Accepted key RSA SHA256:
2Q7HDfMn/w found at /home/saes/.ssh/authorized_keys:1
Aug  9 18:38:29 appc01srv05 sshd[1368699]: Accepted publickey
 ssh2: RSA SHA256:+G/bFNLMg30UgfQ2                 9EB+J2Q7HDfMn/w
Aug  9 18:38:29 appc01srv05 s          699]: pam_unix(sshd:session
uid=0)
Aug  9 18:38:29 appc01srv05         d-logind[1349]: New
Aug  9 18:3    appc01     sshd[1368699]: User child
Aug  9         v05 sshd[1368703]: Starting
                appc01srv05 sshd[1368703]: Receiv
             er
        :29 appc01srv05 sshd[1368703]:
      18:38:29 appc01srv05 sshd[1368699]
      9 18:38:29 appc01srv05 systemd-logind
  exit.
Aug  9 18:38:29 appc01srv05 systemd-
Aug  9 18:38:29 appc01srv05 sshd[
 port 22 rdomain ""
Aug  9 18:38:29 appc01srv05
2Q7HDfMn/w found at /home
Aug  9 18:38:29 appc01s
8 ssh2 [preauth]
Aug  9 18:38:
```

africog
Africa Centre for Open Governance

KPTJ
KENYANS FOR PEACE WITH TRUTH & JUSTICE

Who we are

The Africa Centre for Open Governance (AfriCOG) and Kenyans for Peace with Truth and Justice (KPTJ) are pleased to present the latest report in their series covering Kenya's elections.

In these reports, AfriCOG and KPTJ analyse developments throughout the electoral cycle, with a focus on pre-election preparedness, the administration of Election Day, results announcement processes, post-election dispute resolution, and the broader governance issues arising.

AfriCOG is an independent, non-profit organisation that provides research and monitoring on governance and public ethics issues to address the structural causes of Kenya's unfolding governance crisis.

KPTJ is a coalition of governance, democracy, and human rights organisations that was formed following the 2008 post-election violence to work for electoral justice and accountability for the widespread atrocities and political violence that the country had experienced. AfriCOG convenes the secretariat of the KPTJ. During the 2022 general election, both have worked with the steering committee of the Angaza Movement electoral platform, which succeeded the Kura Yangu Sauti Yangu coalition, to actively monitor the electoral process, engage key stakeholders, and facilitate dialogue amongst a broad range of stakeholders to promote credible elections.

We offer these assessments of our electoral processes to educate Kenyans on the conduct of their elections and to inform the public debate on the strengthening of our electoral governance framework. AfriCOG and KPTJ's goal is to transform the management of Kenya's elections to truly represent the choices and interests of the Kenyan voter.

ICT Experts' Report
for Presidential Petition No E003 of 2022 on the Scrutiny of IEBC's Electoral Technology

Table of Contents

WHAT HAPPENED IN THE ELECTORAL TECHNOLOGY SCRUTINY?

Introduction

On August 9th, 2022, Kenyans voted for a new president in an election that used a hybrid system, embracing both technology and manual processes to ensure the integrity of the final physical count. When the presidential result was contested, the Supreme Court of Kenya ordered a scrutiny on August 30th to see if the technology deployed by the Independent Electoral and Boundaries Commission (IEBC) for the conduct of the general elections met the standards of integrity, verifiability, security and transparency to guarantee accurate and verifiable results as demanded by the petitioners.

Overall, the scrutiny was intended to establish whether the election system may have been compromised, and whether its handling by the Independent Electoral and Boundaries Commission (IEBC) had delivered an election that met the constitutional standard of free and fair. During the scrutiny, a team of ICT experts[1] found security control weaknesses, system vulnerabilities and compromises, and an extensive level of non-compliance by the IEBC with the ordered scrutiny. They noted the IEBC used practical and interpretative excuses to delay or avoid compliance instead of demonstrating that the election system had been built with transparency and cooperation in mind.

The IEBC had every reason to be prepared – the Supreme Court has demanded a scrutiny of election technology in every one of the four elections held since the IEBC first deployed the electronic Kenya Integrated Management System (KIEMS), in 2013. Instead, the approach of the IEBC to the 2022 election showed from the start that there was little to distinguish it from the previous disputed elections in terms of poor management, missed deadlines, problematic voter registration, procurement scandals – particularly around Smartmatic, the multinational company contracted to supply KIEMS – and early technological challenges. It has become clear in Kenya, as in many other countries, that the use of technology does not guarantee the credibility of democratic elections, but opens new frontiers for uncertainty and fraud with a 'black box' approach – a scientific term for when a system can be viewed in terms of its inputs and outputs without any knowledge of its internal workings. Advocates for transparency are increasingly uncomfortable with how election technology sits within state practice, and seek to understand what demands should be made for change. With this in mind, the scrutiny exercises can provide civil society with valuable insights into the technical and political weaknesses and failings of Kenya's election technology system.

The information in this report is organized around the four court orders that determined the Supreme Court 2022 scrutiny, and was prepared by the attending ICT Experts Team representing the 3rd Petitioners in Petition E003 of 2022.

[1] ICT Experts Team, led by Dr Jim Otieno, representing 3rd Petitioner on Electoral Technology Scrutiny

ISSUES FOR DETERMINATION

When demanding the scrutiny, the Court sought to understand the following in order to make a judgement:

Whether the technology deployed by the IEBC for the conduct of the general elections met the standards of integrity, verifiability, security and transparency to guarantee accurate and verifiable results.

If there was interference with the uploading and transmission of Forms 34A, which record results from the polling stations, to the IEBC Portal in the Bomas Tallying Center, Nairobi.

Was there a difference between Forms 34A uploaded on the IEBC Portal, the Forms 34A received at the National Tallying Centre, and the Forms 34A issued to the Agents at the Polling Stations?

Timeline of Scrutiny Exercise

30th August 2022

Court grants orders for IEBC ICT scrutiny to be carried out on 31st August.

9.00 a.m.
31st August 2022

Arrival at IEBC HQ at Anniversary Towers by petitioners' and respondents' appointed ICT experts.

10.00 a.m.
31st August 2022

ICT experts registered and Supreme Court Pass processed.

11.00 a.m. – 2:30 p.m.
31st August 2022

Court Registrar calls the meeting to order.

Deliberations on how to go about the scrutiny begin.

Delegates request to be granted forensic image of the RTS server to carry out scrutiny themselves.

A standoff ensues regarding the interpretation of the granting of access to the IEBC server used for results transmission and the logs.

The meeting adjourned for the 1st and 2nd Respondents to seek clarification of the order for supervised access to the RTS server from the Court.

3:30 p.m. – 6.00 p.m.
31st August 2022

Meeting reconvened with the standoff of provision of forensic image still not resolved.

IEBC proposes to grant supervised access where their staff operates the system.

The team agrees to carry on with the proposal so as not to continue wasting time while waiting for Court's direction

Petitioners' ICT experts raise concern about the date of creation of the server presented by the ICT staff for scrutiny. Experts request screenshots of selected screens of interest throughout the process . Server creation date is established as 31st August 2022, during commencement of scrutiny, which is reflected in Registrar's report.

6:00 p.m. – 9.00 p.m.
31st August, 2022

Experts waiting for Court's direction on the provision of forensic image of the RTS server.

At 21:00h, IEBC provides only some of the copies of documents ordered by the Court.

Meeting adjourned and Court Registrar informs experts that scrutiny to continue the following day once the Court provides direction.

11 a.m.
1st September, 2022

Court Registrar convenes meeting and informs agents that the scrutiny is complete, given that IEBC have been advised by Smartmatic not to provide the forensic image of the RTS server due to purported Intellectual Property issue.

12 Noon
1st September 2022

Court prematurely files scrutiny report, which does not reflect the ongoing observations of petitioners' experts during the scrutiny and which also does not include the screenshots requested by experts during the scrutiny. Experts receive the report, which largely does not include their observations.

COURT ORDER 1:

Overview

This was broadly about how the system functioned, with a focus on security. The IEBC was required to provide copies of its technology system security policy, comprising but not limited to password policy, password matrix, owners of system administration password(s), system users and levels of access and workflow charts for identification, tallying, transmission, and posting of portals, and any Application Programming Interfaces (API's)[2] that had been integrated and the list of human interface and controls for such intervention.

The scrutiny showed that although IEBC has a policy restricting activities of third parties, logs indicated activities by external actors, including one named MTO who deleted a file two days before the election. IEBC also failed to provide a programmatic key to enable the petitions experts to plug themselves directly into the system to receive and scrutinize results forms. Lack of crucial documents, passwords and API information made it impossible for the ICT team to understand user roles and rights or determine standards of security.

ICT Expert Observations on Order 1

Documents that were made available, were provided about 9 p.m. on 31st August, 2022 - 36 hours after the scrutiny order - as follows:

(1) IEBC did not provide as ordered critical documents such as password matrix, owners of system administration password(s), system users and levels of access and workflow charts for identification, tallying, transmission, and posting of portals and any API's.

(2) The 1st Respondent's Information and Communication Technology (ICT) Policy is obsolete, and there was no evidence of the ISO 27001 Certification of the Electoral Technology.

(3) Denial of access to Mobile Device Manager (MDM) database made it impossible to distinguish between Ghost Polling Stations and rogue KIEMS Kits.

[2] API is an interface that allows different applications to integrate, or "talk to each other"

(4) The IEBC ICT team provided a document titled '2.0 Overview of Technology'[3]: Item 4 of Article 2.2 Biometric Voter Identification and Verification System indicates: Generate verifiable read-only logs for the voting day activities.

Based on this section of the Policy Document, IEBC did not comply with Order 1 and also disregarded their own policy of information access by not generating the aforementioned logs.

(5) Certification of Compliance by Serianu: There were 16 reports generated from the penetration tests done, but IEBC provided only 2 test reports out of the 16. These two reports were the Serianu Report 13b RTS Backend Functionality, and Serianu Report 10 Internal Network & Infrastructure Vulnerability Assessment and Penetration Testing (VAPT). No explanation was provided by IEBC for the failure to provide the other 14 penetration test reports. An inference could therefore be drawn that such reports, if any, were adverse to IEBC as it is likely to have failed the other 14 penetration tests and not implemented the recommended remediation measures.

(6) The section on Third Party Vendor Support in the policy manual provided- indicates on page 25 that an employee of the IEBC is to be assigned responsibility to monitor and report on the services by the vendor. As indicated in the logs, foreigners or third parties had access to the server before and after elections. The Policy Document regarding Policy on Access indicates (page 30) that authorizations should be processed on forms signed by the relevant responsible officials. IEBC did not provide the authorization documents allowing remote users to access the system. As shown below, IEBC provided access to persons who were not employees of the IEBC but third parties who had remote access.

(7) ICT Policy: The document provided was stamped by an advocate on 31st August 2022. The document's header indicated that it was drafted or dated 26 January, 2017. The Policy document developed indicated the Policy Version 1.1 with the following areas covered in the document - ICT Governance; ICT Budget & Budget Control; Information and Records Management; Software and Information Systems; Information Technology Hardware; IT Support. International security best practice requires that ICT policies be reviewed every 5 years to address emerging threats and vulnerabilities and embrace developing new technologies. Thus the IEBC policies were obsolete, exposing the systems to threats and vulnerabilities.

Note on Information and Records Management:

IEBC indicates in its policy document (page 13) that documents or records or ICT resources will be the preserve of the IEBC and not a third party. On the same page IEBC indicates that the Commission shall ensure information is accurate, verifiable, secure, accountable and transparent. However, a foreigner named MTO deleted data or a resource, in this case a file, that ordinarily must not be deleted 2 or so days to the elections as shown below (page 6).

[3] IEBC ICT Policies Vol 1 page 192 with pagination as page 63 of 103

(8) Results Transmission System Workflows: The KIEMS Diagram provided only entails a high-level diagram, Vol. 1 page 64. This high-level document does not indicate critical components used during the elections or the actual Results Transmission System (RTS) platform. Order 1 requires IEBC to provide the applicants with an API (Application Programming Interface) document used during the elections. This document would require the IEBC to provide a programmatic key to enable the interested parties to plug in to the sub-systems to receive the results forms. This implies that IEBC did not fully comply with Order 1.

(9) Internal Network & Infrastructure Vulnerability Assessment and Penetration Testing (VAPT) Certificate: This document is stamped by an advocate on 31st August 2022 and dated July 2022. It is noteworthy that this critical test prescribed in Election Act Section 44 was not conducted in time. The penetration test certificate was obsolete, given that it was more than five years old.

Summary of Observations

The lack of crucial documents such as password matrix, owners of system administration password(s), system users and levels of access as well as API information made it impossible to understand the user roles and rights, as well as the interaction of the critical systems used in the transmission and tallying of 2022 presidential results.

Documents provided could not be validated due to the lack of provision of access to the authentic servers used in the presidential elections.

The obsolete ICT Policy could not be relied on to determine whether the technology deployed by the IEBC for the conduct of the general elections met the standards of integrity, verifiability, security and transparency to guarantee accurate and verifiable results.

On the basis of the information and access provided it was impossible to determine whether the technology deployed by the IEBC for the conduct of the general elections met the standards of integrity, verifiability, security and transparency to guarantee accurate and verifiable results. Further, it was impossible to verify whether there was interference with the uploading and transmission of Forms 34A from the polling stations to the IEBC Portal.

COURT ORDER 2:

Overview

This order concerned the crucial Form 34C - the official document from which the IEBC Chair announces the results and declares the president – and gave agents access to the overall architecture of the system, including KIEMS kits. The order compelled the IEBC to give supervised access to any server(s) at the National Tallying Centre for storing and transmitting voting information, and which are forensically imaged to capture a copy of the Form 34C which contains the total votes cast.

The refusal of the IEBC to comply with this order was stark and contentious, particularly when it produced a letter from Smartmatic, the multinational company contracted to supply KIEMS, claiming that full access to the servers "would infringe our intellectual property rights". This assertion of proprietary rights over data pertaining to Kenyan citizens by a foreign company poses a challenge to the country's sovereignty.

ICT Expert Observations on Order 2

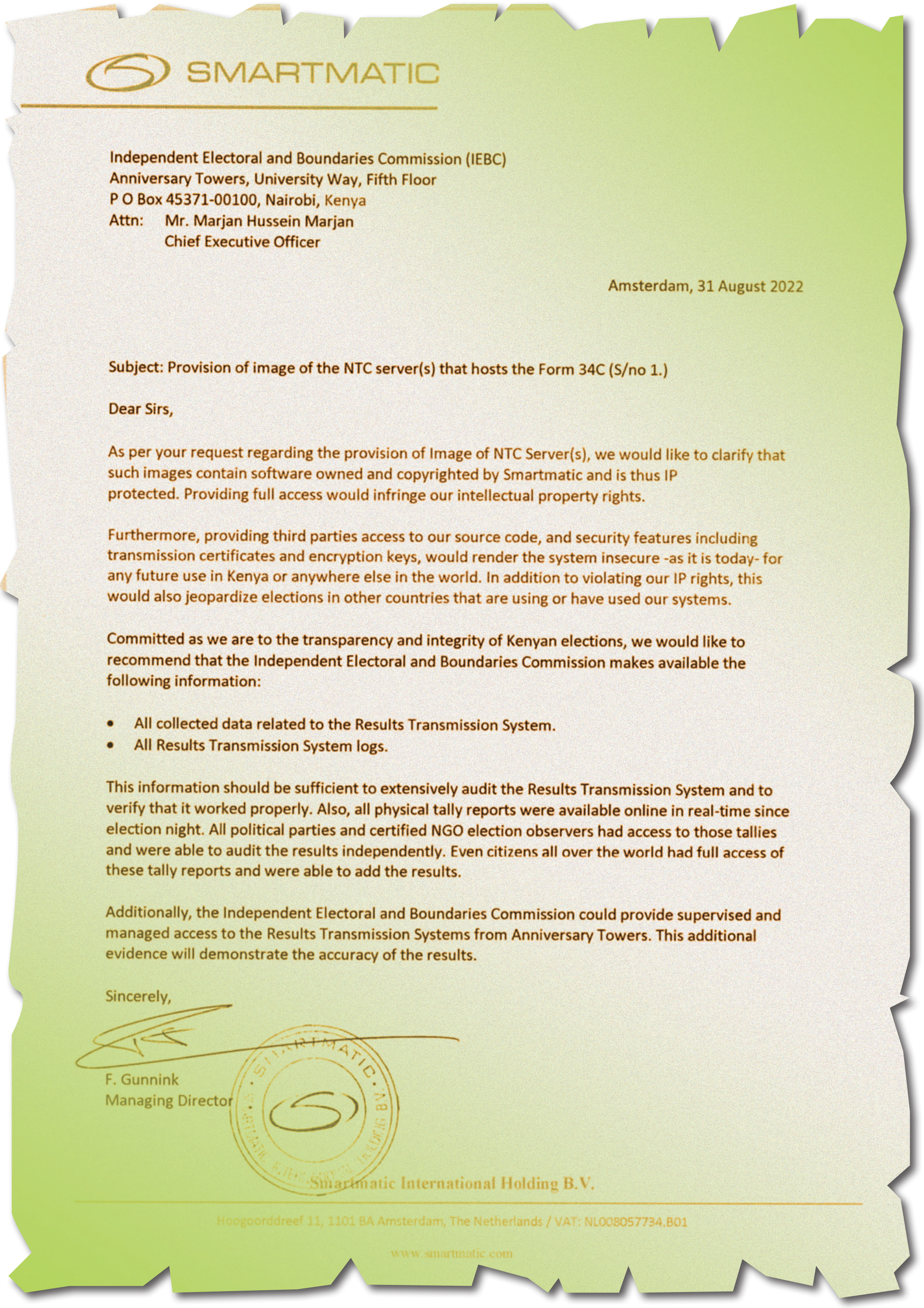
(1) IEBC confirmed that the RTS (Results Transmission System) runs on 8 servers of which one is a virtual server and seven are docker containers (server within a server). There was no explanation of how internal RTS services running as docker containers operated. IEBC denied agents access to the docker servers. The agents' technical teams were therefore unable to probe further. There was no document showing final implemented design and user sign off, when the system went live, handover etc.

(2) The Virtual Image availed for scrutiny was created on 31st August 2022 and cannot be the same server that ran the elections – this was noted in the Registrar's Report that was submitted to the Court. The forensic image of the server was not provided.

(3) The purported server casually demonstrated to the experts is not and cannot be the server used by IEBC in the 2022 Presidential Elections. The specifications of the EMP04 virtual server[4] which was used by IEBC for the demonstration – after observers purportedly having been granted supervised access - were far too low for such a critical component/module of the KIEMS. The specifications provided by IEBC for this server are less than for most desktops and laptops[5].

[4] EMP04 is the name of the server used for demonstration to the observers by IEBC staff

[5] The exact specifications of the EMP04 server given were: Memory 6.4 GB; Clock speed 9.84 GHz; Hard Disk 300 GB



SMARTMATIC

Independent Electoral and Boundaries Commission (IEBC)
Anniversary Towers, University Way, Fifth Floor
P O Box 45371-00100, Nairobi, Kenya
Attn: Mr. Marjan Hussein Marjan
Chief Executive Officer

Amsterdam, 31 August 2022

Subject: Provision of image of the NTC server(s) that hosts the Form 34C (S/no 1.)

Dear Sirs,

As per your request regarding the provision of Image of NTC Server(s), we would like to clarify that such images contain software owned and copyrighted by Smartmatic and is thus IP protected. Providing full access would infringe our intellectual property rights.

Furthermore, providing third parties access to our source code, and security features including transmission certificates and encryption keys, would render the system insecure -as it is today- for any future use in Kenya or anywhere else in the world. In addition to violating our IP rights, this would also jeopardize elections in other countries that are using or have used our systems.

Committed as we are to the transparency and integrity of Kenyan elections, we would like to recommend that the Independent Electoral and Boundaries Commission makes available the following information:

- All collected data related to the Results Transmission System.
- All Results Transmission System logs.

This information should be sufficient to extensively audit the Results Transmission System and to verify that it worked properly. Also, all physical tally reports were available online in real-time since election night. All political parties and certified NGO election observers had access to those tallies and were able to audit the results independently. Even citizens all over the world had full access of these tally reports and were able to add the results.

Additionally, the Independent Electoral and Boundaries Commission could provide supervised and managed access to the Results Transmission Systems from Anniversary Towers. This additional evidence will demonstrate the accuracy of the results.

Sincerely,

F. Gunnink
Managing Director

SMARTMATIC
Smartmatic International Holding B.V.

Hoogoorddreef 11, 1101 BA Amsterdam, The Netherlands / VAT: NL008057734.B01

www.smartmatic.com

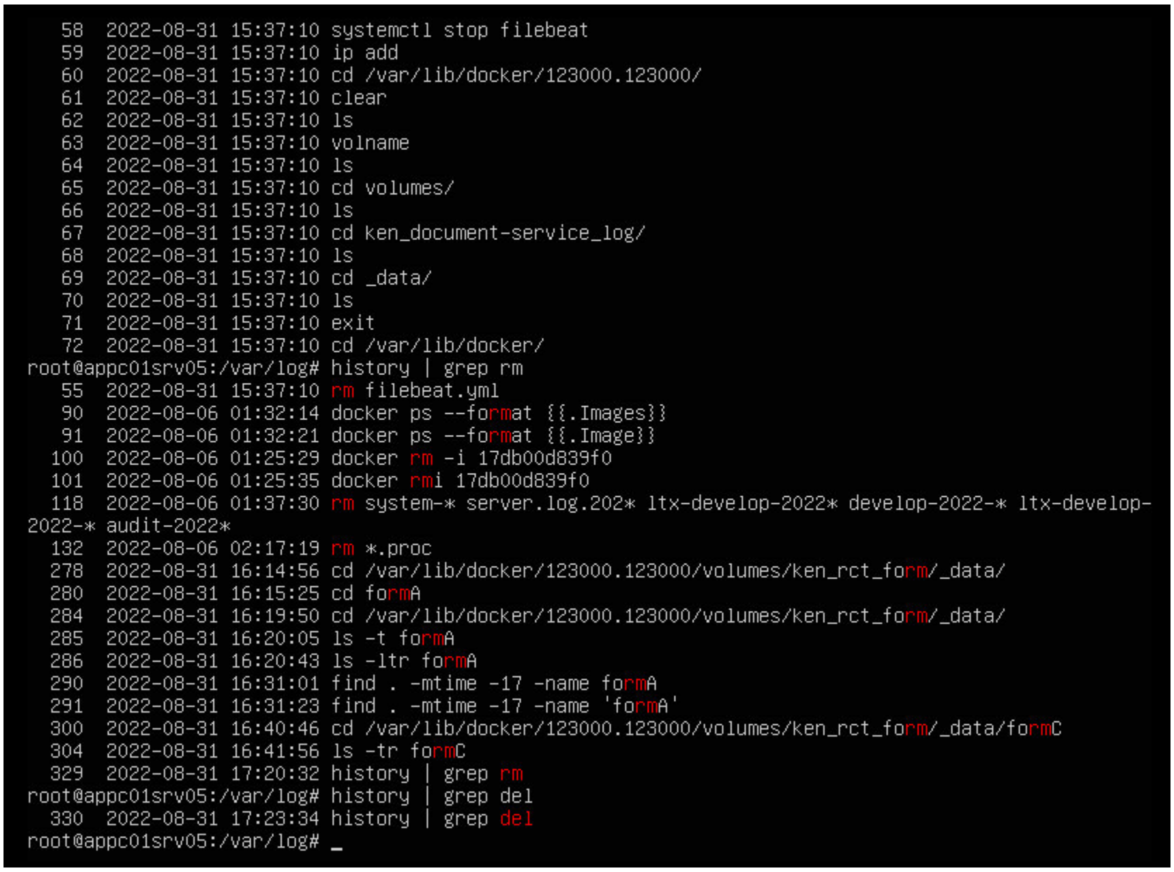
Letter from Smartmatic

(4) The IEBC team provided for the scrutiny were either incompetent on basic Linux operating system operations, or were deliberately sabotaging the exercise. They appeared to lack basic skills in navigating and operating Linux and raised doubts on their being sufficiently competent to be in-charge of their systems. The exercise therefore did not proceed as expected, which was brought to the attention of the Registrar.

(5) The IEBC did not allow scrutiny of the KIEMs kit to establish the availability of embedded scanner application that would verify the image format. This would have enabled the experts to verify whether the scanned document is in the format of jpeg or pdf. It was claimed by petitioners that KIEMS kits transmit Forms 34A in jpeg format and not in pdf format. This is very credible because by default the Android OS (which powers the kit) captures documents in jpeg format and not pdf format. The IEBC declined to hand over the system documentation.

(6) IEBC declined scrutiny of KIEMs kits upload and verification logs.

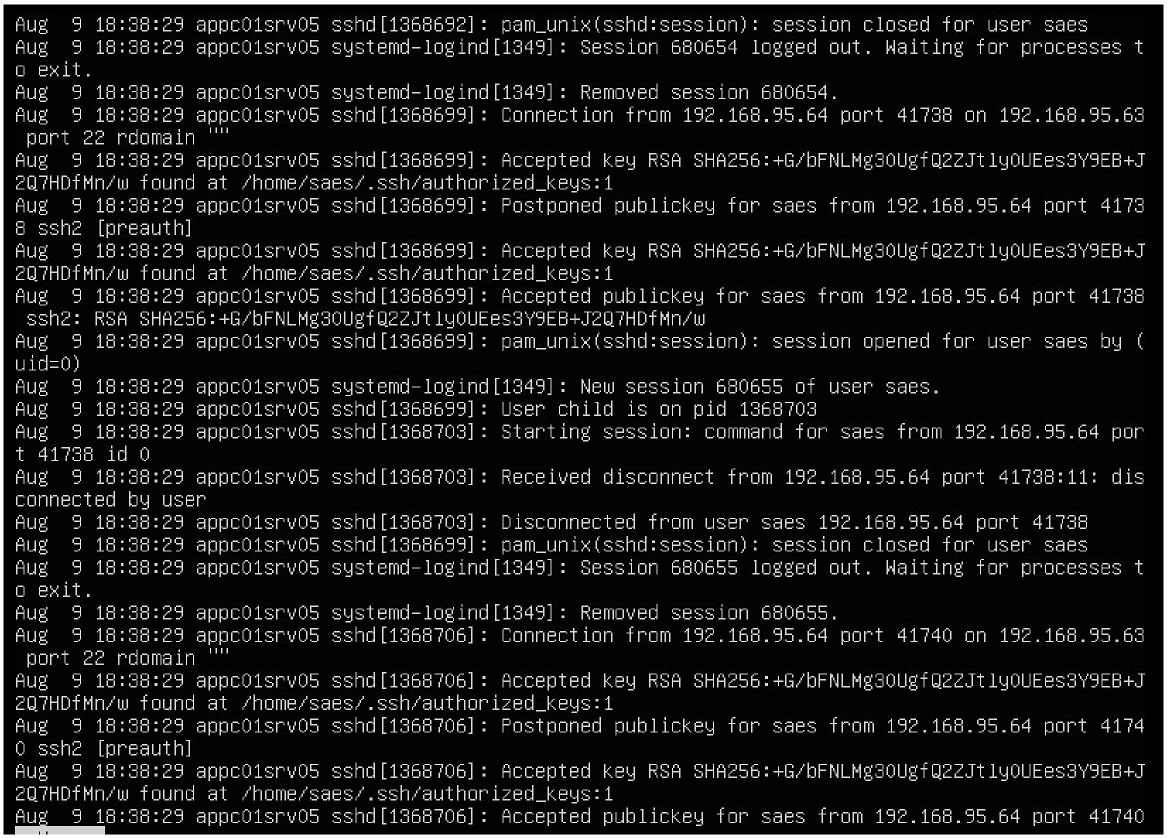
(7) There was evidence of log deletions from the IEBC server two days before the election, on August 6th, yet the Registrar's Report (page 21 issue No. 5) indicates there were no deletions. The "*rm*" command was executed on the RTS server; an "rm" command is used to remove by deletion objects such as files, directories, symbolic links and so on from a file system. The effect of *"rm system**-.log" deletes the entire audit trail – This also indicates the material time external third parties were operating the system, including Ogudino, Vito, J Carmago and Josio. No forensic image of the server was availed, which could have established details of what was deleted.



```
   58  2022-08-31 15:37:10 systemctl stop filebeat
   59  2022-08-31 15:37:10 ip add
   60  2022-08-31 15:37:10 cd /var/lib/docker/123000.123000/
   61  2022-08-31 15:37:10 clear
   62  2022-08-31 15:37:10 ls
   63  2022-08-31 15:37:10 volname
   64  2022-08-31 15:37:10 ls
   65  2022-08-31 15:37:10 cd volumes/
   66  2022-08-31 15:37:10 ls
   67  2022-08-31 15:37:10 cd ken_document-service_log/
   68  2022-08-31 15:37:10 ls
   69  2022-08-31 15:37:10 cd _data/
   70  2022-08-31 15:37:10 ls
   71  2022-08-31 15:37:10 exit
   72  2022-08-31 15:37:10 cd /var/lib/docker/
root@appc01srv05:/var/log# history | grep rm
   55  2022-08-31 15:37:10 rm filebeat.yml
   90  2022-08-06 01:32:14 docker ps --format {{.Images}}
   91  2022-08-06 01:32:21 docker ps --format {{.Image}}
  100  2022-08-06 01:25:29 docker rm -i 17db00d839f0
  101  2022-08-06 01:25:35 docker rmi 17db00d839f0
  118  2022-08-06 01:37:30 rm system-* server.log.202* ltx-develop-2022* develop-2022-* ltx-develop-
2022-* audit-2022*
  132  2022-08-06 02:17:19 rm *.proc
  278  2022-08-31 16:14:56 cd /var/lib/docker/123000.123000/volumes/ken_rct_form/_data/
  280  2022-08-31 16:15:25 cd formA
  284  2022-08-31 16:19:50 cd /var/lib/docker/123000.123000/volumes/ken_rct_form/_data/
  285  2022-08-31 16:20:05 ls -t formA
  286  2022-08-31 16:20:43 ls -ltr formA
  290  2022-08-31 16:31:01 find . -mtime -17 -name formA
  291  2022-08-31 16:31:23 find . -mtime -17 -name 'formA'
  300  2022-08-31 16:40:46 cd /var/lib/docker/123000.123000/volumes/ken_rct_form/_data/formC
  304  2022-08-31 16:41:56 ls -tr formC
  329  2022-08-31 17:20:32 history | grep rm
root@appc01srv05:/var/log# history | grep del
  330  2022-08-31 17:23:34 history | grep del
root@appc01srv05:/var/log# _
```

Evidence of log deletions

(8) IEBC could not explain who the user "saes" was, who attempted to log in to the server from different IP addresses.



```
Aug  9 18:38:29 appc01srv05 sshd[1368692]: pam_unix(sshd:session): session closed for user saes
Aug  9 18:38:29 appc01srv05 systemd-logind[1349]: Session 680654 logged out. Waiting for processes t
o exit.
Aug  9 18:38:29 appc01srv05 systemd-logind[1349]: Removed session 680654.
Aug  9 18:38:29 appc01srv05 sshd[1368699]: Connection from 192.168.95.64 port 41738 on 192.168.95.63
 port 22 rdomain ""
Aug  9 18:38:29 appc01srv05 sshd[1368699]: Accepted key RSA SHA256:+G/bFNLMg30UgfQ2ZJtlyOUEes3Y9EB+J
2Q7HDfMn/w found at /home/saes/.ssh/authorized_keys:1
Aug  9 18:38:29 appc01srv05 sshd[1368699]: Postponed publickey for saes from 192.168.95.64 port 4173
8 ssh2 [preauth]
Aug  9 18:38:29 appc01srv05 sshd[1368699]: Accepted key RSA SHA256:+G/bFNLMg30UgfQ2ZJtlyOUEes3Y9EB+J
2Q7HDfMn/w found at /home/saes/.ssh/authorized_keys:1
Aug  9 18:38:29 appc01srv05 sshd[1368699]: Accepted publickey for saes from 192.168.95.64 port 41738
 ssh2: RSA SHA256:+G/bFNLMg30UgfQ2ZJtlyOUEes3Y9EB+J2Q7HDfMn/w
Aug  9 18:38:29 appc01srv05 sshd[1368699]: pam_unix(sshd:session): session opened for user saes by (
uid=0)
Aug  9 18:38:29 appc01srv05 systemd-logind[1349]: New session 680655 of user saes.
Aug  9 18:38:29 appc01srv05 sshd[1368699]: User child is on pid 1368703
Aug  9 18:38:29 appc01srv05 sshd[1368703]: Starting session: command for saes from 192.168.95.64 por
t 41738 id 0
Aug  9 18:38:29 appc01srv05 sshd[1368703]: Received disconnect from 192.168.95.64 port 41738:11: dis
connected by user
Aug  9 18:38:29 appc01srv05 sshd[1368703]: Disconnected from user saes 192.168.95.64 port 41738
Aug  9 18:38:29 appc01srv05 sshd[1368699]: pam_unix(sshd:session): session closed for user saes
Aug  9 18:38:29 appc01srv05 systemd-logind[1349]: Session 680655 logged out. Waiting for processes t
o exit.
Aug  9 18:38:29 appc01srv05 systemd-logind[1349]: Removed session 680655.
Aug  9 18:38:29 appc01srv05 sshd[1368706]: Connection from 192.168.95.64 port 41740 on 192.168.95.63
 port 22 rdomain ""
Aug  9 18:38:29 appc01srv05 sshd[1368706]: Accepted key RSA SHA256:+G/bFNLMg30UgfQ2ZJtlyOUEes3Y9EB+J
2Q7HDfMn/w found at /home/saes/.ssh/authorized_keys:1
Aug  9 18:38:29 appc01srv05 sshd[1368706]: Postponed publickey for saes from 192.168.95.64 port 4174
0 ssh2 [preauth]
Aug  9 18:38:29 appc01srv05 sshd[1368706]: Accepted key RSA SHA256:+G/bFNLMg30UgfQ2ZJtlyOUEes3Y9EB+J
2Q7HDfMn/w found at /home/saes/.ssh/authorized_keys:1
Aug  9 18:38:29 appc01srv05 sshd[1368706]: Accepted publickey for saes from 192.168.95.64 port 41740
```

Unexplained access by user called "saes"

(9) IEBC refused to provide a security walkthrough of their system to highlight key security controls to determine whether Form 34As could be tampered with during transmission and at what point.

(10) Despite some limited access, IEBC effectively refused to provide access to the actual servers that ran the 2022 general election. Instead of granting access to the forensically imaged server(s), the System Administrator projected a workstation to demonstrate the access to the servers. The properties of the virtual workstation (EMP04), which was used for demonstration, indicated that the virtual RTS server was created and modified on 31st August 2022 at 10:30am. Therefore, access to the live server used for results transmission was not provided as ordered by court.

(11) The IEBC only partially provided the documentation requested under Orders 1, 3 and 4, 36 hours from the time of the court order. This extensive delay cannot be explained or justified other than as a deliberate and willful frustration of court orders.

(12) It was noted that the ICT Policy Document contains numerous pages that have been inserted, breaking the sequential numbering of other pages. Curiously, the said insertions introduce a list of users 'National Returning Officers' led by Dickson Kwanusu. This was observed as an attempt to legitimize unexplained logins by Dickson Kwanusu on the server. This list of 41 National Returning Officers is not included in the Gazette Notice dated 28th April 2022, Vol. CXXIV-No. 79.

(13) It was agreed between the petitioner's agents, the judiciary's representatives and the IEBC that the dispute over the interpretation of the words 'forensically imaged' servers would be submitted to court for directions, after which the judiciary's representatives would revert on the way forward on 1st September at 9 a.m. This did not happen. Instead directions were given by the court to the effect that the scrutiny exercise had ended.

(14) Over 6 hours after the aforesaid ruling, the IEBC purported to deliver to the Agents an image of Form 34C from the public portal, and not the image of the server. This was in defiance of the court order.

(15) On 1st September the IEBC wrote to the Registrar of the Supreme Court enclosing a letter dated 31st August 2022, from Smartmatic International BV in which the latter stated that "the image of ETC servers contained software owned and copyrighted by Smartmatic and thus IP protected. Providing full access would infringe our intellectual property rights". The production of this letter confirmed that IEBC had no intention at all of complying with Order 2. We consider this justification for denying access evasive and unfounded for the following reasons:

(a) IEBC had been accused of refusing to give access to the servers in 2017. It therefore appeared IEBC planned a response for such requests in 2022 by having redundant servers, or cloning the production server and setting it up in an isolated network subnet.

(b) No software can be retrieved from an image. Software is always installed on hardware in order to operationalize applications (programs) and other corresponding digital elements such as images. As such, no software will be lost, gained or given away.

(c) The claim of IP protection does not arise in this case, as IP protection simply means technological guarantee provided by law to patents, copyright and trademarks, which enable people to earn recognition or financial benefit from what they invent or create.

(d) In any event, Intellectual Property Rights cannot be elevated above Articles 1, 2, 10, 38, 81 and 86 of the Kenya Constitution.

Summary of Observations on Order 2

Failure to provide access to the server, and to provide the server forensically imaged to capture a copy of the Form 34C, which is the total votes cast, made it impossible to determine whether the technology deployed by the IEBC for the conduct of the general elections met the standards of integrity, verifiability, security and transparency to guarantee accurate and verifiable results.

Additionally, it was impossible to determine whether there was interference with the uploading and transmission of Forms 34A from the polling stations to the IEBC Portal.

User access controls is weak. The virtual server which was used for demonstration by IEBC server had contractors' user accounts. There was no user access request form to support the creation of the aforementioned accounts. There was no way of verifying if these were bona fide IEBC staff. This raises compliance issues.

The design of RTS, which is a critical component, presented a Single Point of Failure (SPoF). The server was not highly available given that it was a single server. In layman's language, the foregoing means that if the RTS server failed or crashed, then the capability of electronic transmission of results would have been disrupted. This is against the assurance by IEBC that their systems were reliable.

Interference with technology during election was confirmed. Authorization logs confirmed that outsiders accessed the server before, during and after elections. For instance, the commands history confirmed that the system logs were actually deleted.

COURT ORDER 3:

Overview

This order required IEBC to hand over reports on penetration tests, which are done by cybersecurity professionals who simulate a hostile attack to see how the election technology system can withstand it. It is required by law to be done by a reputable firm before the election, and is evidenced by certified copies detailing the level of pass or fail, and areas of concern. The Court ordered the IEBC to produce "certified copies of penetration tests conducted on the IEBC election Technology System prior to and during the 2022 General and Presidential Election", including certified copies of all reports prepared relating to the relevant regulations.

It was extraordinary that the IEBC produced only 2 out of 16 penetration test reports listed in their policy documentation, with the most significant ones missing. As noted above, a possible reason for not including the remaining 14 test certificates could have been that they failed those penetration tests, which would have constituted incriminating evidence against them. These tests are legally mandatory and must be conducted six months before the election.

ICT Expert Observations on Order 3

(1) Only 2 out of the listed 16 penetration test reports were provided, with the most significant reports not provided.

(2) The penetration testing report does not demonstrate the requisite certification according to the Regulation 10(2) of Election Technology Regulations, 2017.

Summary of Observations on Order 3

Penetration Testing pursuant to Regulation 10 of Election (Technology) Regulations, 2017 is not evidenced for the following reasons:

Only 2 out of 16 Penetration Testing Reports were provided, highlighting significant system security weaknesses and vulnerabilities.

The most significant reports required by the scrutiny team to confirm the existence and effectiveness of system security controls in the electoral systems were conspicuously missing.

The Penetration Testing report does not demonstrate the requisite Certification minimum requirements according to the Regulation 10(2) of Election Technology) Regulations, 2017.

There is no evidence of ISO 27001:2013 Certification of the ICT systems; the ISO standards certification methodology, processes, mandatory requirements and milestones were not provided. These standards ensure that an institution is following international best practices as far as information systems governance and risk is concerned.

It was not possible to determine, for this order, whether the technology deployed by the IEBC for the conduct of the general elections met the standards of integrity, verifiability, security and transparency to guarantee accurate and verifiable results.

COURT ORDER 4:

Overview

This order required the IEBC to reveal the companies it is dealing with, and the agreements it has with them. It was also directed to provide a list of users in the system that belong to technology partners rather than IEBC staff, and admin access to provide clarity on the IEBC systems and their usage for review and verification.

IEBC simply refused to comply with Order 4.

ICT Expert Observations on Order 4

The IEBC declined to avail the Partnership agreements, which govern their relationships with e.g. suppliers, service providers, contractors, including Smartmatic and Safaricom.

The IEBC declined to avail the list of users, trail, and admin access[6] to provide clarity on the IEBC systems and their usage for review and verification with the claim that this would risk the lives of those who had admin access.

Summary of Observations on Order 4

The failures to avail the partnership agreements made it impossible to understand and evaluate the Service Level Agreements (SLA) in order to determine the involvement of the technical partners in the supply, management and support of the electoral technology.

The failures to provide the list of users, trail, and admin access made it impossible to provide clarity on the IEBC systems and their usage for review and verification of the standards of integrity, verifiability, security and transparency to guarantee accurate and verifiable results.

[6] There are different levels of access possible to the system; admin have full unfettered access. Read-only access is the least privileged

The claim by Smartmatic that the forensic images requested contain software owned and copyrighted by them and is thus IP protected raises serious concerns about Intellectual Property (IP) infringement claims which should not be left unchallenged because:

(1) It is not a technical challenge to provide the forensic images without Smartmatic's IP being compromised.

(2) Access was previously granted without claims of breach.

(3) The required access was for the apex court legal process, not for commercial purposes.

(4) It propones the denial of access to information.

(5) It challenges the sovereignty of Kenya for the vendor company to control what Kenyans can do with their data. Contrary to what happened in this case, Kenyan law allows IP to be infringed in the case of on-going litigation with the appropriate strictures against misuse.

CONCLUSION

When the Supreme Court ordered the IEBC on 30th August 2022 to allow scrutiny of its servers and election technology system, it was with the intention of investigating the integrity of the IEBC's system in transmitting, receiving and calculating the presidential results. The extensive non-compliance by the IEBC meant it was impossible to determine whether the technology deployed by the IEBC for the conduct of the general election met the standards of integrity, verifiability, security and transparency to guarantee accurate results.

The findings of this team have been detailed comprehensively, and demonstrate how the lack of compliance of IEBC with the court orders hindered the process of conducting an objective and professional scrutiny of the systems.

Nevertheless, the exercise, within its limited context and frustrations, was able to establish various information security control weaknesses, vulnerabilities and compromises within the Electoral Technologies used by IEBC, which cannot eliminate the possibility of election malpractices or the fact that the systems may have been compromised.

Acknowledgements

AfriCOG thanks team members Lucy Ngumo, Fred Lusasi, Isaac Njoroge, Charles Kigwe, Jane Nunga, and James Gondi.

AfriCOG and KPTJ would like to thank their partners at Open Society Initiative for Eastern Africa (OSIEA), Open Society Foundation, and the Ford Foundation for the support that makes their work possible.

The opinions presented in this report are those of AfriCOG/KPTJ alone.

Kenyans for Peace with Truth and Justice (KPTJ) is a coalition of citizens and organisations working in the human rights, governance and legal fields that came together after the crisis over the disputed results of the 2007 presidential election. Members include: Africa Centre for Open Governance (AfriCOG), Bunge La Mwananchi, Centre for the Development of Marginalized Communities (CEDMAC), Centre for Law and Research International (CLARION), Centre for Multiparty Democracy (CMD), Centre for Rights, Education and Awareness for Women (CREAW), The CRADLE – The Children's Foundation, Constitution and Reforms Education Consortium (CRECO), East African Law Society (EALS), Fahamu, Gay and Lesbian Coalition of Kenya (GALCK), Haki Focus, Hema la Katiba, Independent Medico-Legal Unit (IMLU), InformAction (IFA), International Commission of Jurists (ICJ-Kenya), International Centre for Policy and Conflict, Inuka Trust Kenya, Katiba Institute, Kenya Human Rights Commission (KHRC), Kituo cha Sheria, Mazingira Institute, Muslim Human Rights Forum, Release Political Prisoners Trust, Sankara Centre, Society for International Development (SID), The 4 Cs, Urgent Action Fund (UAF) – Africa and Youth Agenda.

December 2022.

Editorial:

Africa Centre for Open Governance - AfriCOG
P.O Box 18157 - 00100 Nairobi, Kenya.
+254 - 20 - 444 3707 | +254 737 463 166
admin@africog.org | www.africog.org | http://kptj.africog.org

Design and Layout by Lugaka Eric

africog
Africa Centre
for Open Governance

KPTJ
KENYANS FOR PEACE WITH TRUTH & JUSTICE