ACT Electoral Commission

Overseas Electronic Voting System

Security Summary

by Digital Elections Pty Ltd
4/935 Station Street, Box Hill North,
Victoria, Australia

and Blitzm Systems
Level 1, 285 Lennox Street
Richmond, VIC 3008

info@blitzm.com
1300 211 248
www.blitzm.com.au

Revision History

Date	Description	Version	Author
29/05/2020	Drafted	Draft 1.0	Blitzm Systems
29/05/2020	Reviewed	Draft v1.1	Digital Elections
31/05/2020	Updated	v1.2	Blitzm Systems
31/05/2020	Final Review	V1.3	Digital Elections
11/11/2020	Updated	V1.4	Blitzm Systems

Table of Contents

About this document

An of the security considerations and approaches taken for the OverSeas Electronic Voting System (OSEV) is provided in this document.

Project Stakeholders

- Digital Elections Pty Ltd ("DE") ABN: 46 623 821 483
  4/935 Station Street, Box Hill North, Victoria, Australia

- Blitzm Systems Pty Ltd ("Blitzm") ABN: 94 153 627 644
  Level 1, 285 Lennox Street, Richmond, Victoria 3121

- The ACT Electoral Commission ("Elections ACT")
  Level 6, 221 London Circuit, Canberra City, Australian Capital Territory

Other Stakeholders:

- ACT Electors
- ACT Legislative Assembly and election candidates

[redacted]

Security Approach Summary

The security of the OSEV system is addressed through many different aspects which are described below in terms of design, voter authentication, technology, infrastructure, service monitoring, web security, data management and encryption, third party testing and auditing and user advice and information. These approaches provide mitigation to common system security risks where possible within the context of the technology and requirements of the system.

System Design

To summarise the security features of the OSEV system design:

1. Personal information is separated from vote preferences.
2. Votes are encrypted and the decryption key is isolated from the system.
3. System architecture has been designed to minimise security risks.

The security features are achieved through the following design features:

1. System components are separated with segregated environments with restricted interfaces between them: .
    a. The following core functions are segregated:
        i. Web application for applicants to register and submit votes.
        ii. Electoral Roll and voter verification.
        iii. Storage of encrypted vote preferences.
    b. A component can only access the resources such as a database that is designated for its use and can't access the data of other components.
2. Interfaces between OSEV components are restricted in the following ways:
    a. The Application Programming Interfaces (APIs) expose the specific functions required for another component to use.
    b. The APIs are restricted by whitelists to only accept connections from the expected OSEV component.
    c. The connecting components also require an authentication key to interact with the API.
3. The OSEV web application where an applicant can register and vote has the following security related features:
    a. The public access point to the OSEV web application is restricted to only allow connections over a TLS secured connection.
    b. The web application does not have a database and so only has the ability to perform limited functions offered by other components.
    c. The web application does not store or persist any vote preferences because they are sent to the vote storage system as soon as they are submitted and encrypted.
    d. The web application does not store personal details and instead requests them from other components where required.

4. The OSEV interfaces to be used by the ACT Electoral Commission have the following security features:
    a. Restricted to only be accessible from the ACT Electoral Commission.
    b. Only allows connections over a TLS secured connection.
    c. Require two factor authentication of the permitted Electoral Commission staff.
5. The system design maintains the secrecy of the vote through the following means:
    a. Votes are encrypted when they are received by the system and are never decrypted within OSEV itself
    b. Votes are decrypted for counting using an offline device
    c. The link to the electoral roll is a two-step process so that system components holding applicant personal information with a VoterToken, do not have sufficient information to link to the vote.
    d. The system components that process vote preferences do not know the VoterToken and instead only have a RegToken which is not stored with any personal information.

Voter Authentication

A third party identification and authentication system will be used to identity applicants. This system will use Australian government document verification services to verify the identity of applicants. The third party service will authenticate the user before they are able to register or vote using OSEV.

Technology

Overseas voters interact with OSEV using their own device with a web browser.

The OSEV website makes use of server rendered pages to avoid any active content (i.e. javascript) in the client's browser. OSEV does not include any 3rd party runtime dependencies within the voter's browser.

[redacted]

Client to server communication occurs using HTTPS. Client interactions are authorised by the server using HTTP Sessions via Browser Cookies. No personal information is stored in the HTTP Session. No information related to the user's vote preferences is stored in the HTTP Session. Cookies are only used to enable to HTTP sessions as per standard web authentication standards and are not used to track user activity.

[redacted]

[redacted]

[redacted]

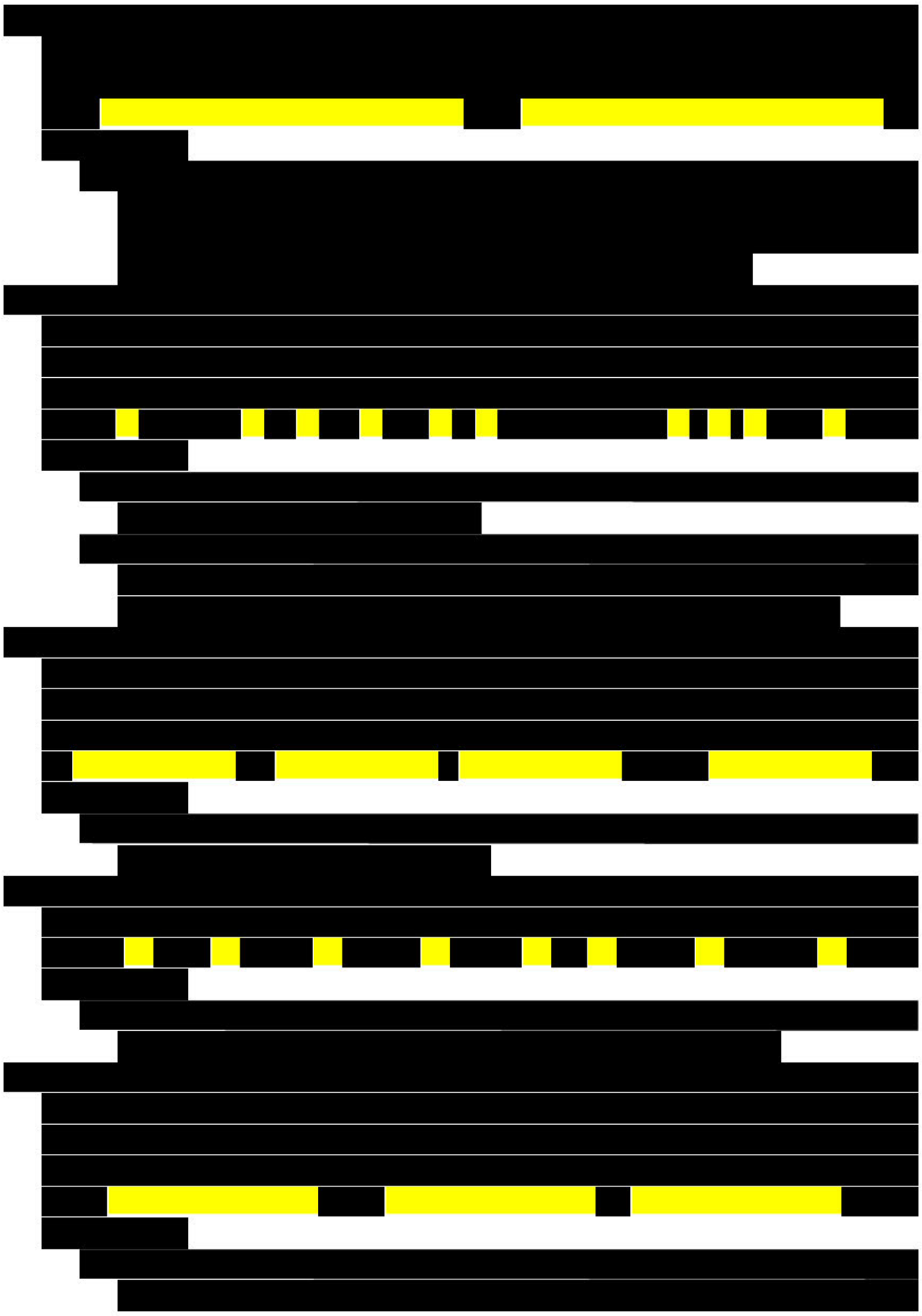
[redacted]

Service Monitoring

[redacted]

Web Security

[redacted]



Data Management and Encryption

1. Throughout all the OSEV components data is encrypted both in transit and at rest.
2. Encryption and signing using ASD approved algorithms.
3. Votes are individually encrypted.
4. The vote storage system does not have access to either the encryption of decryption keys.
5. The OSEV cloud system does not store the vote decryption key and so the votes cannot be decrypted until they are exported.
6. The vote preferences will be encrypted by the eVACS voting system key before they are exported.

Third Party Testing and Auditing

The OSEV system will be tested and audited by third parties to verify it has been implemented according to the specifications and without defect. This will include:

1. System penetration testing.
2. Source code auditing.
3. IRAP certification

User Advice and Information

The system will advise users on best practices for use of the service where it is feasible including:

1. Encouragement to use trusted networks and avoid using open or unencrypted wi-fi networks.
2. Encouragement to use trusted devices.
3. Encouragement to use up to date operating systems and internet browsers.
4. Encouragement to disable javascript and browser plugins.

Vulnerabilities and Mitigations

Fraudulent Registrations

This vulnerability relates to the possibility of malicious actors falsely registering as persons through the use of personal information.

Mitigation Strategies:

1. A third-party identity service is used to identify applicants including the use of document verification services.
2. Registrations are matched to the electoral roll.
3. Checks are undertaken to identity if a person has voted elsewhere.
4. All registrations will be reviewed by a ACT Elections official before votes are submitted to the count.

Authentication and System Access

This relates to administrative access to the system or supporting infrastructure.

Mitigation Strategies:

1. Multi-factor authentication.
2. Source white listing for administrative system access.
3. Limiting authorisation rules for needs-based access.
4. Access logging for administrators.

Web System Penetration

This type of vulnerability relates to an attacker attempting to gain unauthorised access to systems or data, such as through code injection-based attacks.

Mitigation Strategies:

1. Firewall restricting access to the system.
2. All user inputs sanitised and validated.
3. Server side rendered web pages.
4. No javascript used to avoid scripting-based attacks.
5. Third party penetration testing.

DDOS

A Distributed Denial Of Service (DDOS) attack would attempt to render the service inaccessible by "overloading" the service with requests.

Mitigation Strategies:

[redacted]

2. System monitoring.
3. DDOS response plan.

Client-Side Based Vulnerabilities

[redacted]

[redacted]