ACT Electoral Commission

Election Management System Modernisation

OSEV System Design

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
21/02/2020	Drafted	Draft 2.1	Ewen Cameron
24/02/2020	Update	Draft 2.2	Ewen Cameron
25/02/2020	Edits	Draft 2.3	Ewen Cameron
29/03/2020	Design Updates	Draft 2.4	Ewen Cameron
13/04/2020	Design Updates	Draft 2.5	Ewen Cameron
14/04/2020	Minor edits	Draft 2.6	Ewen Cameron
15/05/2020	Updated appendix	Draft 2.7	Ewen Cameron
27/05/2020	Process updates	v2.8	Ewen Cameron
21/08/2020	Updated – Desktop Application and other modifications	V2.9	Ewen Cameron
09/09/2020	Updated – to match final 2020 implementation.	V3.0	Ewen Cameron

Table of Contents

Introduction

About this document

This document describes a proposed draft design of the OverSeas Electronic Voting (OSEV) system for review and comment prior to further design works.

The design described here is a new design which differs from previously proposed designs and a summary of the differences are described in this document.

Following further discussion and design activities, updated versions of this document may be produced.

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

Design Overview

The OverSeas Electronic Voting (OSEV) system design considers system security, process integrity and vote integrity. The design considers the way information is collected, shared, stored and connected.

The system will be cloud hosted with restricted access and all data will be encrypted in transit and at rest.

The system includes four main cloud components, each with their own responsibilities. The components have restricted interfaces to communicate with the other and only relevant data is sent and stored by each component. Additionally, a desktop application is used for vote decryption in isolation from the cloud hosted components.

See OSEV Architecture diagram (appendix: diagram 1) for further context.

System Components

1. **OSEV Web Application** - This component provides public facing web interfaces for applicants to register for overseas voting and submit their votes. The component's responsibilities include:
    a. Verifying that an applicant has authenticated with the auth and identity service.
    b. Gather verified information about the applicant from the identity service.
    c. Managing the registration process including forwarding personal details to OSEV Verify but does not store any identifying applicant details.
    d. Managing the submission of vote preferences.
    e. Encrypts the vote preferences and forwards the encrypted vote preferences to the Vote Storage System but does not store any preferences itself.
2. **OSEV Verify** - This component is an API server with the following responsibilities:
    a. Acts as an intermediary between where applicant personal information is stored (OSEV Check) and where vote preferences are stored (Vote Storage System) so that neither has a direct link to the other.
    b. Applicant personal information is forwarded by this component but not stored.
    c. Vote preferences are never seen by this component.
3. **OSEV Check** - This component is a restricted web application for use by Elections ACT staff with the following responsibilities:
    a. Stores Ballot Paper variations ready for use.
    b. Stores Applicant authentication identifiers with registration information (isolated from vote preferences).
    c. Stores the Ballot Paper assignment for an applicant.
    d. Provides a restricted portal for Election Officers.
    e. Exports OSEV registration records for TIGER to match to the electoral roll.
    f. Imports Electoral roll matches from TIGER.
    g. Election Officers can approve or deny declaration vote submissions.
4. **Vote Storage System** – This component is a restricted web application for use by Elections ACT staff with the following responsibilities:
    a. Stores encrypted vote preferences.
    b. Verifies registration approval through OSEV verify before votes are downloaded using the Desktop Application.
5. **Authentication and Identification Service** – This is a third party service which will provide both identification of applicants and authentication. Identification will include the requirement for submission of identity documents. Authentication service will be through a single sign on authentication model.
6. **Desktop Application –** This is used to generate the vote encryption keys and also to download the vote preferences, decrypt them and create the encrypted vote preferences output for counting. This is the only component that utilizes the vote decryption key.
7. **Azure Active Directory –** This authentication service is used to authenticate OSEV administration users of the OSEV Check web portal and the Desktop application.

Process Descriptions

The following describes how various processes are undertaken using the OSEV system. It is recommended that these descriptions are read in conjunction with the corresponding process sequence diagrams (see appendix).

Election Preparation

These activities are undertaken prior to the Election period.

1. Ballot Papers are exported from TIGER and imported into OSEV Check.
2. A copy of the electoral roll will be exported from Tiger and imported into OSEV Check.
3. The OSEV Check web Application will be configured with the election closing dates and times.
4. The encryption and signing keys and certificate are created in the desktop application.
5. The vote encryption public certificate is uploaded in the OSEV Check Web Application.
6. The election is manually opened in the OSEV Check web application.

Applicant Authentication Process

This is the first process an applicant must undertake.

1. The Applicant navigates to the OSEV Web Application site.
2. The Applicant is redirected to the Authentication and Identification Provider site.
3. The Applicant authenticates with the Auth Provider.
4. If user is not already registered to that service, they will be required to provide identification documents to verify their identity with that service.
5. The Applicant is redirected back to the OSEV Web Application and:
    a. Their authentication is verified as being from the provider.
    b. Their registration and vote status are checked against records in OSEV Check via OSEV Verify.
    c. OSEV can check if a record for the applicant already exists in OSEV by using the identifier from the authentication service (“IdentityProviderSubject”) which is recorded in OSEV Check.
    d. A VoterToken is created by OSEV Check if it does not already exist for this applicant and returned to OSEV Verify.
    e. A RegToken is created by OSEV Verify if it does not already exist for this applicant and returned to OSEV Web Application.
6. The Applicant is registered if not already registered and then can vote if not already voted.
7. The system uses the AuthToken from the authentication provider to validate the user has authenticated.

Registration Process

This process can be started after the applicant has successfully undertaken the authentication process.

1. The Applicant confirms that they want to proceed and register.
2. Information about the applicant is gathered from the identity provider and forwarded through OSEV Verify to be saved by OSEV Check. Including: (name, address, email, phone, DoB). For more information about why information is forwarded via OSEV Verify see section *Design Features: 2. Not allowing vote preferences to be linked to a voter*.
3. OSEV Check attempts to match the information to the electoral roll.
4. Where are match is not found, the Applicant is given the option to provide an alternate address to match the roll.
5. If after three attempts by the Applicant to provide an alternative address, there is still no match found to the roll, they will have the option of continuing to vote by providing the suburb to determine an electorate.
6. The Applicant completes the registration form including confirming the country that they are voting from and making a declaration that they are in that country.
7. The additional information is forwarded through OSEV Verify to be saved by OSEV Check. Including: (Country Where Voting and Electorate).
8. Once this information is saved, the applicant can proceed to vote. If they leave the site before voting, the system will permit them to authenticate again and continue to vote.

Voting Process

This process can be started after the applicant has successfully undertaken the registration process.

1. The applicant confirms that they want to proceed to vote.
2. The Web Application requests a ballot paper from OSEV Check through OSEV Verify.
3. If a ballot paper has not already been allocated for the applicant, OSEV Check will return the next ballot paper in the robson-rotation iteration for the applicant electorate.
4. OSEV Check saves the allocated ballot paper for the applicant and returns it to the OSEV Web Application via OSEV Verify.
5. The Web Application presents the ballot paper to the Applicant in their web browser.
6. The Applicant fills in their vote preferences in their web browser and after reviewing them submits their vote.
7. The OSEV system will accept the applicant's submission regardless of whether they have submitted an informal vote.
8. The OSEV Web Application combines some random data with the vote preference data to act as a salt for encryption and signing purposes. This means that any signature of the data or encrypted package cannot be used to identify the vote by simply comparing to vote preference and ballot paper combinations.
9. The vote is encrypted using the public certificate of an asymmetric encryption algorithm and the private decryption key is not held within the system.
10. The encrypted vote and RegToken are sent to the vote storage system.
11. The vote storage system saves the encrypted vote and RegToken.

12. The OSEV Web Application informs the Applicant that their vote has been submitted and that no further action is required.

OSEV Check Process

This process would be undertaken after the election closes in order to have complete records of whether a person has voted elsewhere.

1. An Election Officer logs in to the restricted OSEV Check Web portal.
2. The Election Officer can see there are declaration vote submissions to be reviewed. (this does not include any actual vote preferences).
3. The Election Officer exports the names, dates of birth and addresses of the voters along with a digital signature of the data created by OSEV Check.
4. The Election Officer imports the voter information into TIGER and TIGER validates the digital signature of the data to provide assurance it was not edited and was created by OSEV Check.
5. The voter is matched to the electoral roll where possible.
6. TIGER will also check if a match on the electoral roll is already marked as voting elsewhere.
7. The Election Officer exports the electoral roll matching information along with a digital signature created by TIGER.
8. The Election Officer imports the match information back into OSEV Check and the signature is checked to provide assurance it was not edited and was created by TIGER.
9. The Election Officer can see which voters match the electoral roll and whether they are known to have voted elsewhere along with the person's information.
10. The Election Officer will perform authenticity checks and review records for voting elsewhere.
11. The Election Officer performs further roll history checks against returned "not on rolls".
12. The Election Officer either marks each declaration vote submission as admitted or invalid.

OSEV Export Process

This process would be undertaken after the OSEV Check process.

1. The Election Officer opens the Desktop application.
2. The Election Officer requests votes to be downloaded.
3. The Election Officer logs in using their OSEV Active Directory credentials.
4. The Election Officer must provide the vote decryption key to the system.
5. The Election Officer must provide the eVACS encryption key to the system.
6. The Vote Storage System will for all votes:
    a. Ask OSEV Verify if the vote should be admitted using the RegToken.
    b. OSEV Verify will forward the request to OSEV check using the VoterToken.
    c. OSEV Check will reply with the registration approval state of being admitted/approved, invalidated/rejected or neither yet.
    d. If a registration is approved, then the vote is downloaded, otherwise it will be ignored.
    e. The encrypted votes for approved registrations are all downloaded to the computer hosting the desktop application.

   f. The votes are decrypted on the local computer using the decryption key provided by the Election Officer.
   g. The vote preferences are compiled into a single file suitable for importing into the eVACS system for counting.
   h. This vote preference file is encrypted using the eVACS encryption key.
7. The Election Officer exports the votes and stores in a secure location ready for counting.
8. The Election Officer can review the number of votes downloaded and compare to the number of approved OSEV applications in Tiger.
9. The vote preferences are transferred from local computer hosting the OSEV desktop application to eVACS for counting.

Design Features

The design has the following features:

1. Separation of system components into segregated environments so that:
    a. access control and maintenance can be managed independently and appropriate to the needs of each environment.
    b. risk management through isolation so that no one environment provides complete access.
    c. The following core functions are segregated:
        i. Web application for applicants to register and submit votes. (See Further Discussion section for discussion on level of separation of these functions).
        ii. Integration to the electoral roll and vote integrity verification.
        iii. Declaration vote review
        iv. Storage of vote preferences
2. Not allowing vote preferences to be linked to a voter by:
    a. The link to the electoral roll is a two-step process so that TIGER or OSEV Check which hold applicant personal information with a VoterToken, do not have sufficient information to link to the vote.
    b. The OSEV Web Application and Vote Storage System do not know the VoterToken and instead only has a RegToken and uses OSEV Verify as an intermediary.
    c. Votes are also only stored with encryption so are only readable at the point of exporting for counting.
3. Vote integrity is supported through the following features:
    a. Vote preferences cannot be read by an unauthorised party because they are encrypted using an RSA asymmetric algorithm so that they can only be decrypted by a key not stored by the system and instead held by Elections ACT.
    b. Vote preferences cannot be secretly edited or changed on the vote storage system because the votes are already encrypted before reaching it and the vote storage system does not have access to the encryption key.
4. Process integrity is supported through the following features:
    a. Verify an applicant's identity through a third-party identification service.
    b. Authenticate an applicant for registration and voting through a third-party authentication service.
    c. Declaration vote review and approval process by Elections ACT.
    d. Ensure declaration votes are approved before being downloaded for counting.
    e. Checking the applicant has not already registered with OSEV at registration.
    f. Checking the applicant has not already voted with OSEV at vote submission.
5. Ballot paper variations are pre-loaded into the system for simplicity and performance. OSEV Check will deliver the ballot paper according to the electorate and robson-rotation number and delivered to the applicant via the OSEV Web Application.
6. There is no direct link to TIGER to maintain OSEV isolation considering security and operational reasons. Instead ballot papers and electoral roll matches are imported by an election official into OSEV after exporting them from TIGER.

7. Elections ACT functions will be performed on isolated and restricted interfaces including:
    a. the OSEV Check Web Portal which is used to upload ballot papers and process declaration vote submissions.
    b. the OSEV Desktop Application which is used to download votes.
8. The cloud system has no access to the vote decryption key and so there is no way to view the stored vote preferences through the OSEV cloud systems.

System Interfaces

The following outlines the approach to system interfaces. See OSEV Architecture diagram (appendix: diagram 1) for further context.

1. Public access to web application will include:
    a. Enforced HTTPS.
    b. DoS attack protection.
2. Interfaces between system components will include:
    a. TLS encryption.
    b. API secret key authentication.
    c. Authorisation control to only functions required by connecting system.
    d. Connection control to known source (IP whitelist).
3. Elections ACT Access to internal portals including the Vote Storage Portal and the OSEV Check portal will include:
    a. Enforced HTTPS.
    b. Username/password authentication (according to ACT Government standards).
    c. Connection control to known source (IP whitelist).

System Technology

[redacted]

Data Formats

The following details how different data will be formatted in the system:

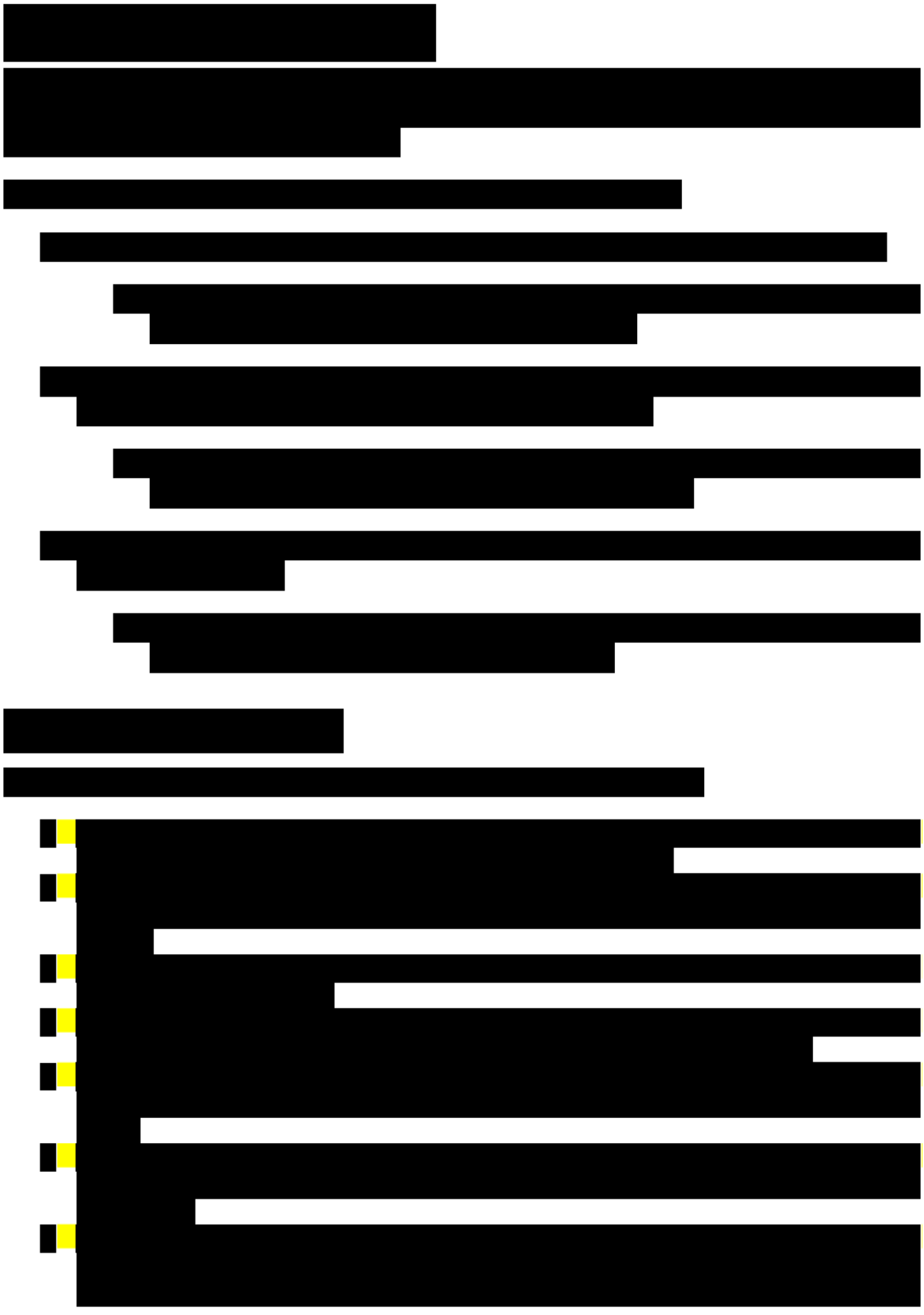
1. **Tokens**
   The system will generate and use “tokens” to provide a component or actor with a reference back to an object or piece of information but without providing any part of that information.

Each token will be a random and unique string, [redacted] Examples include voter token, registration token, unique URL token.

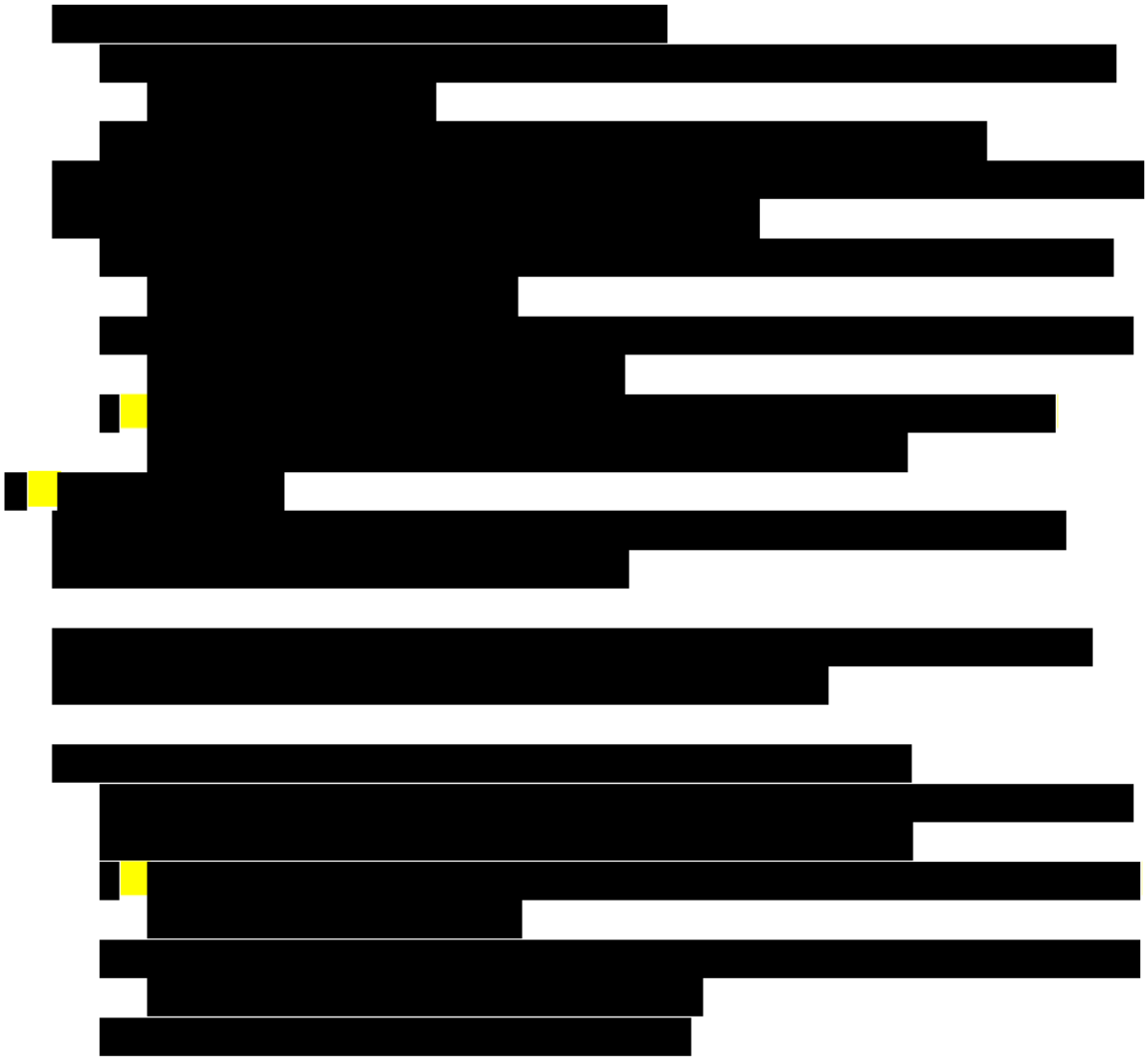
2. **Ballot Paper**
   The ballot paper is proposed to be delivered from TIGER in JSON format. The ballot paper JSON will encapsulate the information required to render the ballot paper as HTML or a PDF document.

Vote

A "vote" is the combination of vote preferences and the ballot paper. While stored in the system, the vote may be stored as either json or html. The "Vote" will encapsulate all information to render the vote in a web browser or PDF. When encrypted [redacted]t will be done with a salt so that the vote cannot be identified by comparing to another [redacted]r encrypted package of the same vote preferences.



[redacted]



4. External Decryption Key

This design includes the use of a private decryption key that is not known by the system. Previous design iterations have included encryption and decryption methods internal to OSEV system components. This new approach means that once votes are submitted, they are not readable or editable until Elections ACT processes them by providing the decryption key.

Appendix

This design document is intended to be read in conjunction with the following design diagrams:

1. OSEV Architecture Diagram v1.1