Vero Select 3rd party Digital Signature

# Revision History

|  |  |  |  |
| --- | --- | --- | --- |
| Version | Date | Summary of Changes | Author |
| 1.0.0 | 11/15/2023 | Initial draft | Abe Barberenagil |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

# Table of Contents

[1 Revision History 2](#_Toc150941307)

[2 Table of Contents 3](#_Toc150941308)

# System Architecture

Level 0 Data Flow

ToDo: DFD0 diagram



# Deployment model and strategy

Certificates

ECDSA public and private.

Add notes from Figure

Create a prototype tool for QA to verify the validity of the key.

Framework Version 4.7.1

Workflow

Investigate the validity of the certificate.

Possible testing scenarios:

\*Renew a Cert before it expires, usually 30 days

Test with an invalid (expired or revoked) certificate.

Rotate the private and public key

Action Items

1. Create a console application to
2. Pramod will help to figure out where to place the code/library.
3. Coordinate the purchase of the Prod certificate
4. Use a self-signed private and public key in the meantime
5. Elaborate a high level of LOE
6. New VeroSELECT version will be 8.23
7. Define follow up meeting schedule

# References

1. [RFC 8785: JSON Canonicalization Scheme (JCS) (rfc-editor.org)](https://www.rfc-editor.org/rfc/rfc8785)
2. [OpenSSL Man - ECDSA](https://www.openssl.org/docs/man1.0.2/man3/ecdsa.html)
3. [Command Line Elliptic Curve Operations - OpenSSLWiki](https://wiki.openssl.org/index.php/Command_Line_Elliptic_Curve_Operations)
4. [PowerShell - Create X.509 Certificate with Private and Public Key (compilemode.com)](https://veros.sharepoint.com/development/veroselect/Shared%20Documents/Developer%20Notes/Digital%20Signature/verify-java-sample)