Report

Security Review Status Report

Online Voting Working Party

Report

Dimension Data Contact Details

We welcome any enquiries regarding this document, its content, structure or scope. Please contact:

Jaco Grobler - Principal Security Consultant, Mobile Phone: +64 9 356 5680

Dimension Data New Zealand Limited
Cnr Market Place and Customs St West
Viaduct
Auckland 1010
New Zealand
☎ 09 356 5680
🖷 09 356 5698
✉ Jaco.Grobler2@dimensiondata.com

Document Author and Reviewers

Action	Name	Title	Date
Prepared by:	Peter Benson	Principal Security Consultant	12/11/2018
Reviewed / Approved by:	Peter Benson	Principal Security Consultant	14/11/2018

Document Release Versions

Version	Date Released	Change Notice	Remarks
V1.00	14/11/2018	Auckland Council	1st Draft
V2.00	16/11/2018	Auckland Council	Final Version
V3.00			

Document Contribution (C) and Distribution (D) List

Name	C/D	Organisation	Title
Peter Benson	C	Dimension Data	Principal Security Consultant
	C	Dimension Data	
Jenny Botton	D	AUCKLAND COUNCIL	Information Security Manager
Marguerite Delbet	D	AUCKLAND COUNCIL	General Manager, Democracy Services
Gaik Lim	D	AUCKLAND COUNCIL	Head of Business Systems

Report

Contents

List of Figures

List of Tables

Version 1.00 18 April 2018
{Document Reference Number}

1. Executive Summary

The Online Voting Working Party have requested Dimension Data to review the security aspects of the On-Line Voting trial, to confirm that appropriate security measures have been addressed.

Given that the trial is still at a relatively early stage, we are unable to provide full and independent assurance that all aspects of security have been addressed through to a production ready instance. However we can confirm that appropriate security measures and decisions have been made to the extent possible within the RFP and vendor selection process, and business case development.

The vendor selection process has been robust, and the selected vendor and project team have the capability to deliver an on-line voting platform within the levels of security and risk as outlined in the initial objectives, i.e. at least as secure as the postal voting equivalent. The technologies involved provide a high degree of assurance of the voting process, and auditability, within the confines of the identified requirements.

The short time frames for development, design, and implementation do pose significant risks, and appropriate controls will be required to ensure that security considerations are addressed appropriately, given the aggressive nature of the project.

In terms of the overall project, there are a number of security considerations and steps still to be undertaken, so this report should not be taken as approval or assurance that the final delivered solution is either fit for purpose or sufficiently secure. At this stage, we would consider this project to be at high risk but being managed appropriately.

The author of this report has been involved in providing advice and guidance to the project, and hence, this is not a fully “independent” assessment, and should be tempered by the notion of involvement, and advice provided during the project to date.

The following sections describe observations and issues identified from the level of engagement available within the project.

1.1. Conclusion

The project has developed and designed an RFP for the purposes of selecting an end-to-end service provider for the provisioning and management of an on-line voting solution.

In addition, the project has been working with the Department of Internal Affairs with respect to the voting regulations to enable the progression of the on-line voting technology in conjunction as a “trial” only at this stage.

As of the time of report development, the RFP process has been completed, the vendor (and hosting provider) have been selected as preferred supplier, and a business case has been developed to enable decision making by the Working Party to proceed as required.

Appropriate security measures and decisions have been made to the extent possible into the RFP and vendor selection process.

The vendor selection process has been robust, and the selected preferred vendor and project team have the capability to deliver an on-line voting platform with the levels of security and risk as outlined in the initial objectives of the project.

2. Introduction

Central Government is currently progressing legislation to enable a trial of online voting in the local authority elections in October 2019. On the basis that the necessary changes will be made to the regulatory framework governing local authority elections, nine local authorities have formed an Online Voting Working Party ("Working Party"), to provide an online voting option as part of the 2019 local authority elections.

Local Government New Zealand (LGNZ), representing all local authorities, supports the Working Party's initiative to offer a trial of online voting, and is working with them to increase community understanding and identify lessons arising from the trial.

Provided the enabling legislation is enacted in time, the Working Party intend to trial an online voting option for the 2019 local authority elections only, to demonstrate that online elections will work in the New Zealand local government context.

This report is based on the initial phase of the project only, i.e. the RFP process, preferred vendor selection, and business case development.

3. Purpose

Dimension Data had been requested to provide a resource to deliver security consulting work for the online voting project.

The purpose of this document is to provide observations and commentary on the effectiveness and outcomes of the first phase of the project, i.e. RFP process and vendor selection / recommendation, and business case development,

4. Scope of Review

The scope of this work was to:

1. Evaluate the vendor responses to the RFP

    a. Provide support to the Auckland Council tender evaluator for reviewing the submissions from respondents to the RFP

    b. Assess the information security aspects of the submissions and identify any gaps, weakness and key differences between the short-listed responses.

2. Support Auckland Council's Information Security Manager in developing the security related aspects and costs for input into the business case that will be submitted to the Governing Bodies for approval to proceed with the chosen technology for the trial.

Deliverables:

3. Provide feedback on the responses and make recommendations for the technology to select based on how closely the responses match the requirements in the RFP and subsequent amendments.

4. Costs of the security related work are estimated for inclusion in the business case.

5. Approach to Review

The process has involved a committee of 9 local councils ("Online Voting Working Party"), working together as a steering committee, providing governance and direction to the project. The project team has included an evaluation team, supported by a "technical support" team to evaluate technical aspects of the RFP and responses.

Our approach to the vendor selection / RFP process focused on four key areas as outlined below:

Focus Area	Description / Objective
Vendor selection process	Assure quality of RFP process and preferred vendor selection.
Security Architecture	Assure that the technology, people, processes and described architectures are fit for purpose for performing online voting in local government elections.
Communication	Determine that input and communication within and external to the project is appropriate based on criticality of the deliverable.
Risk Management and risks	Identify and highlight key risks that need to be mitigated or considered in future project phases.

6. Results of the Review

The results of our review are outlined below:

6.1. Vendor selection process

The vendor selection / RFP process has been well managed, with clear management of governance, process, probity, and analysis.

The RFP was developed using reasonable practice and based on threat modelling and advice from DIA and others to ensure that any vendor selection has met minimum standards and expectations from a security standpoint.

While a number of the proposals were lacking in both quality and security capability, the final two candidates clearly demonstrated they have been involved in delivering successful on-line voting projects globally and could demonstrate they met the minimum quality and security levels required by this project.

The overall security was improved during the short-listing process through the decision to require the vendor to host the solution in an All of Government (AoG) IaaS certified Data Centre, within the commercial space, but with security levels equivalent to All of Government certification.

From a security perspective, the probity process was well enforced in order to help the technical support team make recommendations outside of any potential bias introduced by commercial considerations. Independence issues were addressed throughout the course of the RFP process, and managed appropriately.

The decisions / recommendations were based largely on whether the vendors both had credibility in the industry space being considered, whether they had sufficiently robust processes and controls to have a level of confidence that they could build an appropriate solution, and a clear understanding that they could achieve the required processes and conditions outlined in the RFP, subsequent follow up changes, and flexibility to deliver to requirements in the time frame.

Technically, the preferred vendor has demonstrated strong security and cryptographic controls, consistent with the requirements for protection of the voting process and vote collection, storage, and processing. Strong audit controls along with vote verification systems have been identified based on proven technology. The preferred vendor has also demonstrated sufficient flexibility to provide a level of assurance they can meet local customisation requirements without compromising overall security.

Please note however that vendor selection is only one stage in the security journey; due to time frames, there was insufficient time to perform a full and detailed threat analysis or security architecture / design prior to the vendor selection. These processes will be required to be undertaken in subsequent phases of the project.

6.2. Security Architecture

Overall the security architecture described by the selected vendor is "fit for purpose" in relation to the voting process, the vote collection and tabulation, and the auditing functions required to ensure an accurate voting count. Further detail concerning the security architecture is provided below:

- The election management technical controls provide a level of confidence in the collection, storage, decryption of the votes, and strong audit controls to ensure provable processes.
- The voting process includes double encryption (client and communication), which provides a level of confidence that votes cannot be intercepted and / or changed over the network communication.
- A separate vote verification system has been included, to provide assurance that vote manipulation in the user's (voter's) device has been addressed.
- A reasonable level of assurance has been achieved in the vendor having appropriate internal controls and processes to develop and maintain secure voting application systems.

The project has established sufficient confidence in the overall security at this stage of the project to progress forward. This includes agreement to use hosting services providers that are compliant with AoG security requirements, as well as a compliance requirement with the New Zealand Information Security Manual (NZISM).

Due to the tight time frames of the project, a range of detailed security architecture and design activities related to the hosting providers and hosted solution have yet to take place, and it is essential that additional tasks are required in the next phase to perform and agree the following:

- Detailed threat analysis and mapping
- High level security architecture
- Detailed security architecture and design, including all areas of the solution:
  - People
  - Process
  - Technology (including network, application, server, etc.).

6.3. Communication

Given the nature of the project and the aggressive time frames of the project, communications at this stage have been very good, with high levels of engagement by both the stakeholders and the project team.

The next stages of the project will require similar levels of communications to ensure that all parties and interests are adequately represented, particularly related to security concerns.

The nature of the time frames are to some extent dictating the outcomes of the project, and while every project has a trade off between time, cost, quality, it is essential that quality and time are considered the primary concerns to ensure a successful outcome.

External communications, including with interest groups has been reasonable, with public submissions around the draft regulation changes and mediated forums with interested parties including DIA, disability groups, Maori, various universities, and democratic representation.

Within this type of disruptive technology introduction, and the potential impact / implications for public trust and democratic process, it is highly recommended that external communication and input is sought to ensure the robustness of the process, and to ensure that all threats are identified and mitigated appropriately. With this type of technology, the more security and risk experts that provide input to the process, the better. This will help with both risk identification, and to help with confidence building outside the immediate project team.

On-line voting is considered high risk in the media, and there is a lot of “Fear, Uncertainty, and Doubt” (FUD) in the public domain as to whether there is sufficient trust in the technology to proceed. Irrespective of the notion that the objectives of the trial are to be “at least as secure as postal voting”, the degree of public scrutiny on the project should not be underestimated. This is particularly relevant in the face of state sponsored election manipulation fears, such as the purported Russian interference in the US election process.

It is highly recommended that the project consider a proactive and positive communications strategy to establish engagement and comfort / confidence in the project, as opposed to a reactive communication strategy which only reacts to negative media reports.

6.4. Risk Management and Risks

The following are risks that have been identified by the author that should be given consideration in the following phases of the project. There is a level of comfort that all appropriate steps have been taken to date. The following are additional considerations for the next phases of the project that should be addressed.

1. **Trial vs production** – While this project is a “trial” of online voting, the intent is to implement and install this into a fully production environment, with use going forward for additional elections / by-elections. There is a potential for thinking that, as this is a “trial”, that the environment, systems, security, etc., are temporary.

   In reality, the project needs to ensure the designs, implementation and operation, are suitable for a 3-5 year time frame, i.e. standardised production and operation.

   The second consideration is that the requirements and system designs have been considered for the purposes of Local Body Elections only, and not for National Elections. While stated in the original purpose of the Trial, it should be reinforced that the selected systems and designs should be considered fit for existing purposes only, and subject to full and complete reviews prior to any consideration for any other purposes.

2. **Vendor risk** – a range of detailed design requirements are yet to be ratified and confirmed, due to the draft regulations not either finalised or approved at this stage. This limits the time within which to perform detailed requirement design and system development.

   There are risks associated with this that, while assurances have been provided by the Vendor, it may impact on project delivery or costs. Implications of changes to requirements have yet to be confirmed and therefore are unknown in scope and implications.

3. **Security design** – As previously discussed, while there is confidence in the vendor’s solution from a security perspective, the overall (end to end) security design has yet to be formalised and ratified through the process of detailed threat modelling, high level security architecture, detailed security architecture, implementation and operation.

   Threat Modelling is an essential part of this process, i.e. it is essential that a detailed threat and risk assessment be undertaken to determine as many threats as possible to the infrastructure, operational processes, technology, and voting methodologies. Once the detailed threat landscape and risks have been understood to the extent possible, appropriate controls and mitigations can be designed and implemented.

It is essential that this work be performed as early as possible, once the detailed requirements have been identified, and the regulations ratified.

4. **Time vs quality** – The project is working to reasonably aggressive time frames. The vendor has identified that the time frames are currently achievable, however it is recommended that there is sufficient effort applied to ensure that quality (security) is not compromised as a result of the time pressures to deliver the outcome.

5. **Costs / Business Case** – At this stage of the project, reasonable consideration has been given to security requirements, however as detailed requirements have not been fully identified or detailed design undertaken, the final and full costs of implementation and operation of security may not be fully identified.

   There is a risk that the required costs of security may require a cost review at some stage in the project. The earlier that detailed designs can be undertaken, the earlier any cost variances can be identified. At this stage, recommendations have been made to include additional costs in the business case for "yet to be identified" security requirements.

6. **Transparency** – Online voting is a significant change from postal ballot voting, and is significantly more complex. While reasonable attempts have been made to ensure security experts have been engaged and security requirements have been addressed, this is one area where involvement and engagement of appropriate interest groups and open experts is recommended to the extent possible. This particularly applies to the threat modelling to ensure that threats have been identified and mitigated to the extent possible.

7. **Threat modelling** – The initial RFP work was developed based on threat models that were developed in 2014, which was fit for purpose for the process of vendor selection.

   The threat landscape and technology capabilities and risks have changed since then, with additional risk factors and issues needing to be taken into consideration when developing and operating the online systems. In addition, while the existing threat models are sufficient for a general vendor selection process, they are insufficiently detailed to ensure that all appropriate threats and risks have been covered off in a detailed sense.

   The next phase of the project should include a detailed threat assessment / modelling exercise to ensure that all appropriate threat mitigations and safeguards are designed into the project prior to implementation.

7. Conclusion

Overall we found the process to be robust and time bound in terms of decision making and managing the vendor process. Democracy Services representation has been strong within the project, and it is paramount that this continues. There are always risks with technical projects that objectives can be missed, and a detailed level of engagement with the democratic services and voting processes is paramount to the success of the project from the perspective of ensuring the delivered capability meets the democratic requirements.

We did note the following concerns that need to be carefully managed in the next stage of the project:

1. Draft Regulation design and interpretation is creating a strain on the project, as the draft regulations are still undergoing change, are subject to a level of interpretation, and are not guaranteed to be passed into regulation. This is creating pressure on the vendor implementation, as a range of detailed design and development requirements will only be understood once the regulation has been passed, with tight time frames following that date for implementation. There is nothing to suggest at this stage however that the timing cannot be achieved.
2. The on-line voting Draft Regulations (and interpretation of the same) are of some concern. While there is an intent to provide equivalency of service between on-line voting and postal voting, technology for on-line voting provides a significantly different threat posture to voting processes, and there are risks that the draft regulations may "water down" or affect the quality of the overall on-line voting process. An example is the authentication process being necessarily limited due to the authentication method; less of an issue with postal (physical) ballot handling, but has a different risk posture for on-line voting systems.
3. In addition, the DIA interpretation of vote verification methodology, while technically feasible, will impact on (lessen) the amount of actual vote verification undertaken by voters, and increase the operational delivery costs. Noted however that these decisions are outside the scope of the project, and are technically manageable within the time frames.
4. The project time frames are necessity aggressive in order to meet the objectives of the October 2019 elections. Given the strong security requirements of the trial, it is essential that there is sufficient time to perform appropriate testing, including source code review, penetration testing, and security audits. This is a substantial piece of work, and the importance of stringent testing (and time to perform) cannot be understated.

Appendix A Software suppliers review

Five vendors were invited to respond to the closed RFP process, these being:

- Digital Elections
- Link Market Services
- Scytl
- Smartmatic
- Votem

Each of the vendors was compared in a number of areas:

- RFP response completeness and compliance
- Security controls and technical details
- Fitness for purpose in meeting requirements for local government elections
- Vendor robustness, commercial maturity, success in similar use cases
- Other.

From the responses provided by the vendors, the following were discounted by the Technical Support team as being inadequate in a number of areas, including fitness for purpose, quality of controls and security, ability to meet the RFP requirements. The vendors dismissed included Votem, Link Market Services, and Digital Elections.

It should be noted that each provide a commercial offering which may be appropriate for digital elections under specific circumstances, however these were determined as not meeting the objectives of usability or security within a local government election process, or did not meet the requirements of this RFP.

The two remaining candidates, Smartmatic and Scytl, were invited to respond to additional questions / requirements, and to demonstrate their capabilities to a team representing both the Working Party, and the Technical Support team.

Both Smartmatic and Scytl meet the objectives and requirements of the RFP and security requirements, and either are reasonable candidates for selection as the preferred supplier.

From an observation perspective, Smartmatic demonstrated stronger flexibility in meeting changing requirements and demonstrated a stronger level of commitment to meeting tight objectives and time frames.