

Contents

Note: Names following chapter titles are the currently-assigned writers; percentages following writer names are very rough estimates of the approximate percentage of completion. Some material factored into the percentages may not yet appear in the generated report because it needs to be brought in from external sources.

List of To Do Items	4
1 Executive Summary (Joe K./Susan) (0%)	5
2 Introduction (Joe K./Susan) (25%)	6
2.1 The E2E VIV Project	6
2.2 Goals	6
2.3 People	6
2.4 Methodology	6
2.5 Outcome	6
2.6 Next Steps	6
3 Remote Voting (Philip) (30%)	7
3.1 Rationale	7
3.1.1 Geographic Dispersion	7
3.1.2 Accessibility	7
3.1.3 UOCAVA	7
3.1.4 Early Voting	7
3.1.5 Expectations	7
3.2 History	7
3.3 Current Practice	7
3.3.1 Integration with Local Elections	7
3.4 Shortcomings of Current Practice	7
3.4.1 Use of Communication/Internet	7
3.4.2 Accessibility and Usability	7
3.4.3 Auditing	7
4 E2E VIV Explained (Philip/Daniel/Adam) (25%)	8
4.1 IV, VIV, E2E	8
4.2 E2E Election Rituals	8
4.2.1 Pre-Election Phase	8
4.2.2 Voting	8
4.2.3 Post-Election Phase	8
4.3 Shortcomings and Expectations of E2EVIV	8
4.3.1 Access to Communication/Internet	8
4.3.2 Accessibility	8
4.3.3 Usability	8

4.4	E2E VIV in Practice	8
4.5	Limitations of Existing Systems	8
5	Required Properties of E2E Systems (Dan) (100%)	9
5.1	Technical Requirements	9
5.1.1	Functional	9
5.1.2	Usability	10
5.1.3	Accessibility	11
5.1.4	Security and Authentication	11
5.1.5	Auditing	12
5.1.6	System Operational	13
5.1.7	Reliability	13
5.1.8	Interoperability	14
5.1.9	Certification	14
5.2	Non-functional Requirements	14
5.2.1	Operational	14
5.2.2	Procedural	16
5.2.3	Legal	16
5.2.4	Assurance	17
5.2.5	Maintenance and Evolvability	17
6	Crypto Specification (Joe K./Dan) (15%)	18
6.1	Ideal Functionality of an E2E System— \mathcal{F}_{e2e}	18
6.1.1	Claims Regarding \mathcal{F}_{e2e}	20
6.1.2	Security Properties Not Captured by \mathcal{F}_{e2e}	20
7	Architecture (Joe K./Dan) (15%)	21
8	System Specification (Joe K./Dan) (15%)	22
9	Verification and Validation (Joe K./Dan/Adam) (20%)	23
9.1	Requirements and Scenarios	23
9.2	Methodology	23
9.3	Technologies	23
9.4	Interpreting Results	23
10	Feasibility (Unassigned) (25%)	24
10.1	Threats and Security Risks	24
10.2	Availability	24
10.3	Usability	24
10.4	Legal Frameworks and Politics	24
10.5	LEO Considerations	24
10.6	Cost	24
10.6.1	Design and Development	24
10.6.2	Operational	24
10.6.3	Integration with Local Election Systems and Processes	24
11	Conclusion (Joe K./Susan) (0%)	25
11.1	Results	25
11.2	Recommendation (YES or NO???)	25
11.3	Next Steps	25
11.3.1	Political/Legal Challenges	25
11.3.2	Research Challenges	25
11.3.3	Engineering Challenges	25
11.3.4	Business Opportunities	25