

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) (45%)	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	8
3.1.5 Expectations	8
3.2 History	8
3.2.1 Integration with Local Elections	9
3.3 Shortcomings of Current Practice	10
3.3.1 Use of Communication/Internet	10
3.3.2 Accessibility and Usability	10
3.3.3 Auditing	10
4 E2E VIV Explained (Philip/Daniel/Adam) (45%)	11
4.1 IV, VIV, E2E	11
4.2 E2E Election Rituals	12
4.2.1 Pre-Election Phase	12
4.2.2 Voting	12
4.2.3 Post-Election Phase	12
4.3 Shortcomings and Expectations of E2EVIV	12
4.3.1 Access to Communication/Internet	12
4.3.2 Accessibility	12
4.3.3 Usability	12
4.4 E2E VIV in Practice	12

4.4.1	RIES [17]	13
4.4.2	Prêt à Voter [11]	14
4.4.3	Punchscan [20, 21]	14
4.4.4	Scantegrity II [8, 9]	15
4.4.5	Remotegrity [26]	16
4.4.6	Helios [1, 2]	16
4.4.7	Norwegian System [14]	17
4.4.8	Wombat [16]	17
4.4.9	DEMOS [12]	18
4.5	Limitations of Existing Systems	18
4.5.1	Voter Secrecy	18
4.5.2	Ballot Stuffing	19
4.5.3	Infrastructure & Equipment	19
4.5.4	Support & Responsiveness	19
4.5.5	Usability	19
4.5.6	Accessibility	20
4.5.7	Social & Political	20
5	Required Properties of E2E Systems (Dan) (100%)	21
5.1	Technical Requirements	21
5.1.1	Functional	21
5.1.2	Usability	22
5.1.3	Accessibility	23
5.1.4	Security and Authentication	23
5.1.5	Auditing	24
5.1.6	System Operational	25
5.1.7	Reliability	25
5.1.8	Interoperability	26
5.1.9	Certification	26
5.2	Non-functional Requirements	26
5.2.1	Operational	26
5.2.2	Procedural	28
5.2.3	Legal	28
5.2.4	Assurance	29
5.2.5	Maintenance and Evolvability	29
6	Crypto Specification (Joe K./Dan) (15%)	30
6.1	Ideal Functionality of an E2E System— \mathcal{F}_{e2e}	30
6.1.1	Claims Regarding \mathcal{F}_{e2e}	32
6.1.2	Security Properties Not Captured by \mathcal{F}_{e2e}	32
7	Architecture (Joe K./Dan) (15%)	33
8	System Specification (Joe K./Dan) (15%)	34
9	Verification and Validation (Joe K./Dan/Adam) (20%)	35
9.1	Requirements and Scenarios	35
9.2	Methodology	35
9.3	Technologies	35
9.4	Interpreting Results	35
10	Feasibility (Unassigned) (25%)	36
10.1	Threats and Security Risks	36
10.2	Availability	36
10.3	Usability	36