

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	9
3.3.1 Use of Communication/Internet	9
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 [18]	13
4.4.2	Prêt à Voter [11]	14
4.4.3	Punchscan [21, 22]	15
4.4.4	Scantegrity II [9, 10]	15
4.4.5	Helios [1, 2]	15
4.4.6	Introduction	16
4.4.7	Core Architecture & Operation	16
4.4.8	Security	17
4.4.9	Auditability	18
4.4.10	Norwegian System [15]	18
4.4.11	Remotegrity [26]	19
4.4.12	Introduction	19
4.4.13	Core Architecture & Operation	20
4.4.14	Security	21
4.4.15	Infrastructure required	23
4.4.16	Shortcomings	23
4.4.17	Wombat [17]	23
4.4.18	DEMOS [13]	23
4.5	Limitations of Existing Systems	24
5	Required Properties of E2E Systems (Dan) (100%)	25
5.1	Technical Requirements	25
5.1.1	Functional	25
5.1.2	Usability	26
5.1.3	Accessibility	27
5.1.4	Security and Authentication	27
5.1.5	Auditing	28
5.1.6	System Operational	29
5.1.7	Reliability	29
5.1.8	Interoperability	30
5.1.9	Certification	30
5.2	Non-functional Requirements	30
5.2.1	Operational	30
5.2.2	Procedural	32
5.2.3	Legal	32
5.2.4	Assurance	33
5.2.5	Maintenance and Evolvability	33
6	Crypto Specification (Joe K./Dan) (15%)	34
6.1	Ideal Functionality of an E2E System— \mathcal{F}_{e2e}	34
6.1.1	Claims Regarding \mathcal{F}_{e2e}	36
6.1.2	Security Properties Not Captured by \mathcal{F}_{e2e}	36
7	Architecture (Joe K./Dan) (15%)	37
8	System Specification (Joe K./Dan) (15%)	38
9	Verification and Validation (Joe K./Dan/Adam) (20%)	39
9.1	Requirements and Scenarios	39
9.2	Methodology	39
9.3	Technologies	39
9.4	Interpreting Results	39
10	Feasibility (Unassigned) (25%)	40
10.1	Threats and Security Risks	40