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 [16] . . . 13
4.4.2 Prêt à Voter [10] . . . 14
4.4.3 Punchscan [19, 20] . . . 15
4.4.4 Scantegrity II [8, 9] . . . 15
4.4.5 Remotegrity [23] . . . 16
4.4.6 Helios [1, 2] . . . 17
4.4.7 Norwegian System [13] . . . 17
4.4.8 Wombat [15] . . . 18
4.4.9 DEMOS [11] . . . 18
4.5 Limitations of Existing Systems . . . 18

5 Required Properties of E2E Systems (Dan) (100%) 19
5.1 Technical Requirements . . . 19
5.1.1 Functional . . . 19
5.1.2 Usability . . . 20
5.1.3 Accessibility . . . 21
5.1.4 Security and Authentication . . . 21
5.1.5 Auditing . . . 22
5.1.6 System Operational . . . 23
5.1.7 Reliability . . . 23
5.1.8 Interoperability . . . 24
5.1.9 Certification . . . 24
5.2 Non-functional Requirements . . . 24
5.2.1 Operational . . . 24
5.2.2 Procedural . . . 26
5.2.3 Legal . . . 26
5.2.4 Assurance . . . 27
5.2.5 Maintenance and Evolvability . . . 27

6 Crypto Specification (Joe K./Dan) (15%) 28
6.1 Ideal Functionality of an E2E System—$\mathcal{F}_{\mathsf{e2e}}$ . . . 28
6.1.1 Claims Regarding $\mathcal{F}_{\mathsf{e2e}}$ . . . 30
6.1.2 Security Properties Not Captured by $\mathcal{F}_{\mathsf{e2e}}$ . . . 30

7 Architecture (Joe K./Dan) (15%) 31

8 System Specification (Joe K./Dan) (15%) 32

9 Verification and Validation (Joe K./Dan/Adam) (20%) 33
9.1 Requirements and Scenarios . . . 33
9.2 Methodology . . . 33
9.3 Technologies . . . 33
9.4 Interpreting Results . . . 33

10 Feasibility (*Unassigned*) (25%) 34
10.1 Threats and Security Risks . . . 34
10.2 Availability . . . 34
10.3 Usability . . . 34
10.4 Legal Frameworks and Politics . . . 34
10.5 LEO Considerations . . . 34
10.6 Cost . . . 34
10.6.1 Design and Development . . . 34
10.6.2 Operational . . . 34
10.6.3 Integration with Local Election Systems and Processes . . . 34