

# 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.**

<b>List of To Do Items</b>	<b>4</b>
<b>1 Executive Summary (Joe K./Susan) (0%)</b>	<b>5</b>
<b>2 Introduction (Joe K./Susan) (90%)</b>	<b>6</b>
2.1 The E2E VIV Project . . . . .	6
2.1.1 Situation . . . . .	6
2.1.2 A Proposed Solution . . . . .	7
2.1.3 Definition . . . . .	7
2.2 Goals and Objectives . . . . .	8
2.2.1 Shared Goals . . . . .	8
2.2.2 Project Goal . . . . .	8
2.2.3 Additional Objectives . . . . .	8
2.2.4 Deliverables . . . . .	8
2.2.5 A First Step . . . . .	9
2.2.6 Success . . . . .	9
2.2.7 Scope . . . . .	9
2.3 People . . . . .	10
2.3.1 Team Members . . . . .	10
2.3.2 Stakeholder Groups . . . . .	12
2.4 Methodology . . . . .	13
2.5 Outcome . . . . .	13
2.5.1 Deliverables Produced . . . . .	14
2.5.2 User Interface Design . . . . .	14
2.6 Next Steps . . . . .	15
<b>3 Remote Voting (Philip) (100%)</b>	<b>16</b>
3.1 Rationale . . . . .	16
3.1.1 Accessibility . . . . .	16
3.1.2 UOCAVA . . . . .	16
3.1.3 Domestic Absentee . . . . .	16
3.1.4 Expectations . . . . .	18
3.2 History . . . . .	18
3.2.1 Armed Forces Voting . . . . .	18
3.2.2 Remote Civilian Voting . . . . .	19
3.2.3 Disabled Civilian Voting . . . . .	19
3.2.4 Modern Remote Voting . . . . .	19

3.3	Shortcomings of Current Practice . . . . .	20
3.3.1	Use of Communication Technologies . . . . .	20
3.3.2	Accessibility and Usability . . . . .	20
3.3.3	Auditing . . . . .	20
<b>4</b>	<b>E2E VIV Explained (Philip/Daniel/Adam) (75%)</b>	<b>22</b>
4.1	Goals . . . . .	22
4.2	Shortcomings and Expectations of E2EVIV . . . . .	24
4.3	E2E VIV in Practice . . . . .	24
4.3.1	RIES . . . . .	24
4.3.2	Prêt à Voter . . . . .	25
4.3.3	Punchscan . . . . .	25
4.3.4	Scantegrity II . . . . .	26
4.3.5	Remotegrity . . . . .	26
4.3.6	Helios . . . . .	27
4.3.7	Norwegian System . . . . .	27
4.3.8	Wombat . . . . .	28
4.3.9	DEMOS . . . . .	28
4.4	Limitations of Existing Systems . . . . .	28
4.4.1	Voter Secrecy . . . . .	28
4.4.2	Ballot Stuffing . . . . .	29
4.4.3	Infrastructure & Equipment . . . . .	29
4.4.4	Usability . . . . .	30
4.4.5	Accessibility . . . . .	30
4.4.6	Social & Political . . . . .	31
<b>5</b>	<b>Required Properties of E2E Systems (Dan) (100%)</b>	<b>32</b>
5.1	Technical Requirements . . . . .	33
5.1.1	Functional . . . . .	33
5.1.2	Usability . . . . .	34
5.1.3	Accessibility . . . . .	34
5.1.4	Security and Authentication . . . . .	35
5.1.5	Auditing . . . . .	36
5.1.6	System Operational . . . . .	36
5.1.7	Reliability . . . . .	37
5.1.8	Interoperability . . . . .	38
5.1.9	Certification . . . . .	38
5.2	Non-functional Requirements . . . . .	38
5.2.1	Operational . . . . .	38
5.2.2	Procedural . . . . .	39
5.2.3	Legal . . . . .	40
5.2.4	Assurance . . . . .	41
5.2.5	Maintenance and Evolvability . . . . .	41
<b>6</b>	<b>Crypto Specification (Joe K./Dan) (15%)</b>	<b>42</b>
6.1	Ideal Functionality of an E2E System— $\mathcal{F}_{e2e}$ . . . . .	42
6.1.1	Claims Regarding $\mathcal{F}_{e2e}$ . . . . .	44
6.1.2	Security Properties Not Captured by $\mathcal{F}_{e2e}$ . . . . .	44
<b>7</b>	<b>Architecture (Joe K./Dan) (95%)</b>	<b>45</b>
7.1	Non-Functional Requirements Forcing Architectural Factors . . . . .	45
7.1.1	Certification . . . . .	45
7.1.2	Abstraction . . . . .	46
7.1.3	Deployment . . . . .	46
7.1.4	Threats . . . . .	46