OVF E2E VIV Technical & Management Proposal
PUBLIC VERSION

Proposal Cover Sheet

Galois Proposal Code	OVF-E2E-VIV-2014
Technical Areas	Project Management and System Specification and Report Authoring/Editing
Proposal Title	End-to-End Verifiable Internet Voting for Overseas Citizens, Overseas Military Voters, and Disabled Voters Worldwide that is Accepted and Supported by Computer Scientists and State Election Officials
Lead Organization	Galois, Inc. 421 SW Sixth Avenue, Suite 300, Portland, OR 97204
Type of Business	Other Small Business
Technical Point of Contact	Joseph Kiniry, Galois, Inc. 421 SW Sixth Avenue, Suite 300, Portland, OR 97204 Phone: 503.626.6616, Email: `kiniry@galois.com`
Administrative Point of Contact	Jodee LeRoux, Galois, Inc. 421 SW Sixth Avenue, Suite 300, Portland, OR 97204 Phone: 503.808.7209, Email: `jodee@galois.com`
Award Instrument Requested	Fixed-fee at reduced rate
Galois R&D Funding	At least $25,000
Place and Period of Performance	Portland, Oregon 06-01-2014 to 05-01-2015
Subcontractor Information	N/A
Proposal Validity Period	05-23-2014 to 08-01-2014
Taxpayer ID Number	93-1278540
Date Proposal Submitted	05-23-2014

Executive Summary

Galois offers to be the technical project manager for the *E2E VIV Project*, whose general project management is performed by the non-profit *Overseas Vote Foundation* (*OVF*), and whose funding derives from a grant obtained by *OVF* from the *Democracy Fund*.

Galois will facilitate the communication and decision-making of the excellent expert teams brought together by *OVF*. *OVF* has convinced the brightest researchers and activists who represent the entire spectrum of attitudes about E2E VIV systems---a ``team of rivals'' in the nomenclature of the original *OVF* proposal---to participate in this project.

Galois will also be the editor and, when necessary, author, of a set of rigorous engineering artifacts fit for refinement into a working election system, and against which third parties can perform independent validation and verification.

The Galois offer of work for the *E2E VIV Project* is as follows:

- *facilitate the communication and decision-making* of the expert teams to drive toward the goals of the project,
- *project management* of matters relating to systems research & specification and demonstrator development,
- *help interface with external parties* who are interested in the technical work of the project and its outcomes,
- have authorship and editorial responsibility for the final *E2E VIV system specification*,
- have authorship and editorial responsibility for the *build/buy recommendation document* for a E2E VIV system development,
- have authorship and editorial responsibility for the *validation/testing recommendation document*, and
- ensure that all *project reports* and supporting *technical artifacts* meet or surpass the definition described in the project *Success Targets* defined in *OVF's Principles and Scope of Cooperation* document [17].

To ensure that the concrete technical claims about existing systems and the design of new technologies are appropriately grounded in reality and demonstrable to all, Galois is *contributing scaled matching funding for the construction of demonstrators* for the E2E VIV project.

1 Introduction

Research and prototype development of end-to-end verifiable internet voting systems (E2E VIV) more or less started nearly two decades ago with Beneloh's PhD dissertation in 1996 [2]. While there are several leading candidate algorithms with exemplar prototypes (e.g., Helios, Zeus, Remotegrity, RIES), there has been little serious effort put into the detailed, justified, peer-reviewed specification of an *E2E VIV election system*. In fact, no system constructed thus far includes traceable evidence for the correctness, security, or usability, particularly for the disabled, of an E2E VIV election system.

Serious consideration of the practical design, development, deployment, and use of an E2E VIV election system has occurred in fits and starts over the past fifteen years. The main reason that earlier efforts have failed are due, in part, to two factors. Firstly, there are fundamental technical challenges in the design of an E2E VIV election system which properly balances security and usability. Secondly, and more importantly, the electronic voting technology research and activist community has been steadfast in its rejection of most of the constructive activity in this area.

Part of the reason that activists are so animated about this topic is political and procedural. Early efforts to force the development and use of an internet voting system for military personnel stationed overseas witnessed little transparency and oversight, resulting in a system that, at first blush, fulfilled the functional requirements of overseas voters. But upon careful inspection by security experts, the system fulfilled none of the most fundamental mandatory security properties of such a critical system [11].

Another reason why activists are so agitated by this topic is that vendors regularly abuse the precise terminology of the research area and make broad, sweeping, strong claims about the correctness and security properties of their products with little-to-no evidence. Moreover, no vendor provides the necessary transparency to their design decisions, architecture, or development for the public, or even election officials under NDA, to come to any deep and just understanding of the system that they are paying for.

This poor state of affairs has led to not just a great deal of distrust between vendors and activists, but also between election officials and activists. Consequently, the adoption of a trustworthy E2E VIV election system is as much a socio-political challenge as a technical one.

Galois's leadership on *Overseas Vote Foundation*'s *End-to-end Verified Internet Voting Project* (or *OVF E2E VIV Project*, or simply the *project*, for short) will change this state-of-affairs, socially and technically.

On the social front, Galois will facilitate the communication and decision-making of the excellent expert teams brought together by *OVF*. *OVF* has convinced the brightest researchers and activists who represent the entire spectrum of attitudes about E2E VIV election systems---a ``team of rivals'' in the nomenclature of the original *OVF* proposal---to participate in this project.

On the technical side, Galois will be the editor and, when necessary, author, of a set of rigorous engineering *artifacts* fit for refinement into a working election system, and against which third parties can perform independent validation and verification.

Galois believes that it will be the social and technical catalyst and glue to keep the project lively, on track, and ensure that it meets the expectations of both *OVF* and the *Democracy Fund*.

The main reasons that Galois has this belief are twofold. First, as a company, Galois has an outstanding professional reputation as a company in the high-assurance R&D space, particularly with demanding clients such as the U.S. Department of Defense. Second, and more personally, Galois believes that the Galois Principal Investigator in this area, Dr. Joseph Kiniry, has the appropriately strong and broad reputation, collegial relationships, and technical expertise in the electronic voting research area to lead this project to a successful conclusion beyond the expectations of its originators.

The main aspects of this project that will engender success are process, project management, and a results-driven focus. By using a tuned combination of processes, methods, and artifacts, Galois will ensure that the end result of this project is trustworthy and approachable by the layperson.

Additionally, to ensure that the concrete technical claims about existing systems and the design of new technologies are appropriately grounded in reality and demonstrable to all, Galois is *contributing matching funding for the construction of demonstrators* for the *E2E VIV Project*. The kind and nature of *demonstrators* will be determined, for the most part, by the experts involved and the digital election systems against which new E2E VIV election systems are judged.

2 Process

The *E2E VIV Project* is (1) framed by several *project documents*, (2) potentially has *positive and negative result outcomes*, and (3) outcomes are objectively determined by the active participation of *many actors, both internal and external*.

2.1 Framing Documents

The main project framing documents are as follows.

1. The *Democracy Fund Proposal*, or simply the *DF Proposal* for short. This proposal is entitled ``Proposal for a Paradigm Shift: Online Voting for U.S. Overseas and Military Voters Accepted and Supported by Computer Scientists and State Election Officials''. We call the project summarized in this proposal the *E2E VIV Project*, for short.
   The *DF Proposal* provides sufficient background to describe the *E2E VIV project* at a high level at its inception. The project's history, social and political framing, goals, strategy, participants, potential outcomes, and deliverables are all summarized therein. The *DF Proposal* was submitted by *OVF* to the *Democracy Fund* in 2013 in order to obtain the funding necessary to execute Phase I of the *E2E VIV Project*.

2. The *Principles and Scope of Cooperation*, or *PSC* for short. This document was written by *OVF* to explicitly frame contributions to the *E2E VIV Project* by stating the principles and scope of the project and, subsequently, the roles and activities of the parties involved in the project.
   The *PSC* provides a template for not only the statement of work for participating actors, but also the intended intellectual property and use rights of the outcomes of the *E2E VIV Project*.

2.2 Outcomes

While *E2E VIV Project* project will produce a *System Specification Development and Documentation* (or *technical report* for short), including a *Whole Product Solution Specification* (or simply *specification* for short), for an *E2E VIV Election System* (or just *election system* for short), the assessment of that system by the expert team has two possible outcomes.

Positively, the majority of the expert team may decide that the specified *election system* meets all of the requirements set forth by the charter of the group, as described in the *DF Proposal*. This outcome indicates that *OVF* may potentially move forward with Phase II funding proposals to ensure that the *election system* is developed and, potentially, deployed.

Negatively, the majority of the expert team may decide that the specified *election system* **does not** meet all of the requirements set forth by the charter of the group. This outcomes indicates that further funding to design or construct such an *election system* is, for the moment, unwise and that the community believes that designing a usable and secure *election system* is still an open scientific, not engineering, challenge.

Note that, as discussed in subsubsection 4.2.2 below, fulfilling the usability and security requirements sketched out in the original *Democracy Fund Proposal* is *not* sufficient for a positive assessment by the expert team. A full system specification that is usable and secure may be, for example, far to expensive to build, too difficult to deploy and manage, or mandate too much expertise from election officials to operate. Social non-functional requirements may trump technical functional requirements.

The *Whole Product Solution Specification* will be written in one or more specification languages that cover the technical needs of the *E2E VIV Project*, particularly with regards to third party high-assurance verification and validation of implementations. Galois recommends using Alloy [10], RAISE [9], or PVS [18] to codify a formal domain model, BON [21] to specify the *election system's informal domain model, requirements, architecture, and design, and F* [8] and Cryptol [4] to specify *election system* protocols.

2.3 Actors

There are several *actors* relevant to the project that Galois and *E2E VIV Project participants* must explicitly reflect upon and with which we will interact.

The actors directly involved with the project, which we call *internal actors* or *E2E VIV Project participants*, are:

- members of *experts teams*, including the *technical*, *usability*, *testing*, and *research* teams,
- the project *advisory council*,
- *local election officials* involved in the the project, and
- the *OVF project management team*.

The *external actors* with whom we must interact include, but are not limited to the following classes:

- the *election activism community*, particularly those that have strong positions on internet voting. The primary actors in this community that we must be aware of include the Election Verification Network (*EVN*) [7], the Verified Voting Foundation (*VVF*) [20], and voter outreach efforts like Rock the Vote [19].
- *external election experts* that are not on the expert teams, including organizations such as the Caltech/MIT Voting Technology Project [3].
- *external local election officials* not represented on the project.
- the National Institute of Standards and Technology (*NIST*) [14], as they are the primary federal organization tasked via the 2002 Help America Vote Act (HAVA) for helping realize improvements in U.S.A. election systems.
- the U.S. Election Assistance Commission (*EAC*) [5], as the organization responsible for, in some sense, all things election-related in the U.S.A.
- companies and non-profits working in the internet voting space (e.g., major U.S. vendors like Dominion Voting and the non-profit OSET Foundation [16]), which we will generically call *evoting vendors*.
- individuals and teams that have designed or constructed E2E VIV election systems, either as academic or hobbyist projects, which we will call *E2E vendors*.

Note that some specific are potentially members of several actor classes. Also, the nomenclature ``vendor'' is not meant to be a pejorative; it is only indicative of the fact that an actor has constructed an operational system of some kind, not that the system is meant to be commercially sold or licensed.

2.4 Timeline

The timeline of the *E2E VIV Project* is 1 June 2014 to 1 May 2015. Galois will actively work on the project during this time frame. Galois will continue to support *OVF* after the time frame has ended in a manner similar to current relationships with the *EVN*, *VVF*, and the *OSET Foundation*. This means that some fraction of Dr. Kiniry's time is spent supporting these initiatives as a scientist-activist to further the agenda of transparent, trustworthy, auditable elections.

It is expected that active work on the project will be at a fairly constant moderate rate every week with occasional bursts of full-time activity. Systems engineering work on *demonstrators* will likely happen in bursts, while engineering work on libraries or solutions will span longer time frames and will likely continue after the *E2E VIV Project* formally ends.

2.5 Engagement and Communication

Galois will be highly engaged with all aspects of the project relevant to our offered outcomes. Communication will be regular, transparent, and high-bandwidth with all *internal actors*. Communication with *external actors* will be periodic and transparent.

Galois advocates that all communication within the project and between project members and external actors be stored in a searchable, traceable, archived format. Permitting external actors access to all communication for the purposes of auditing enormously enhances the transparency and trustworthiness of the project and its outcomes. While the decision to witness this degree of transparency can impact the manner in which experts communicate about sensitive topics (e.g., explicitly stating their expert opinion on specific commercial technologies), Galois believes that, on the balance, the increase in trustworthiness and traceability is well worth this trade-off.

Non-digital communication, like face-to-face meetings, should have minutes produced or, if feasible, be digitally recorded. Likewise, capturing text chat logs, archiving critical multiparty audio/videochat conversations, etc. is all worth considering in the light of the trustworthiness of outcome.

2.6 Drive Towards Decisions

To keep the project moving forward with momentum, the main mechanism Galois will use to take action each day on the activities of the *E2E VIV Project* is a project-bespoke version of David Allen's *Getting Things Done* methodology (*GTD*) [1].

Concretely, all goals of the *E2E VIV Project* will be decomposed into GTD tasks, each of which will be tracked and prioritized using the project collaboration system(s). Thus, every *goal* will have a *tree of tasks* and every task will have a concrete *next action*. Associated with every goal, task, and action is a set of metadata including, but not limited to, creation date, deadline, creator, owner, priority, dependencies, completion date, and update log.

Galois has a highly efficient process for creating, updating, and maintaining GTD projects and their artifacts. Galois will interface that process with the technology currently in use by the *E2E VIV Project*.

By using this method, project managers can instantly see the status of the project in a summary view of goals, tasks, and actions. Moreover, if desired, such artifacts can be coupled to more traditional project management artifacts such as Gantt charts and project management tools such as Microsoft Project and OmniPlan.

Additionally, and perhaps more importantly, project participants---particularly expert team members that are preoccupied with their other duties---can instantly see the status of those facets of the project that they are responsible for, or to which they are contributing.

3 Project Management

Successfully ensuring that this project meets its goals critically dependent upon quality project management, given the distributed nature of the team and the fact that team members are uncompensated for this work and have day jobs.

3.1 Galois' Role

The main technical project management role of Galois is to facilitate the communication and decision-making of the expert teams.

Activities for which Galois is responsible include, but are not limited to:

- triggering and fostering dialogs on all topics,
- creating, triaging, updating, and ensuring the resolution of tickets relating to project management, *election system* research and specification, and *demonstrator* development, and
- helping organize and conduct online, telephone, and face-to-face meetings among expert team members to drive toward transparent decisions about *election system* and *demonstrator design*.

This technical management capacity is complemented by Galois's role in concretizing the (likely high-level) specification of the *election system* created by the expert teams.

More specifically, Galois will be the editor and, when necessary, author, of a set of rigorous engineering *artifacts* fit for refinement into a working *election system*, and against which third parties can perform independent validation and verification. The expected nature of these specifications are discussed later in
section 5.

Galois also plays a supporting role in several aspects of this project. In particular, Galois will:

- *interface with the OVF project management team* in a completely transparent, timely, and open fashion, from day-to-day updates to formal reporting,
- *support the CMU/Heinz Capstone projects*, via email and telephone, on technical and strategic matters that relate the E2E VIV project,
- *support the OVF's approach to potential Phase II and Phase III funders* in the event the project is deemed worthy of further phases of work and *OVF* has identified potential paths, and
- *support the OVF in crafting intermediate reports and a final summary statement* to the *Democracy Fund* regarding the promised *Success Targets* in the *PSC*.

3.2 *OVF* Role

OVF, via the *OVF support team*, will continue to act as overall project manager, as they are responsible to *Democracy Fund* for the overall outcome of this project.

The *OVF* was and is responsible for Phase I, part 1 *Identify/Recruit Team Members*, and part 3 *Business Plan* components of the project. Galois welcomes the opportunity to contribute their contacts and expertise within these sub-deliverables, but *OVF* will remain responsible for their execution.

Consequently, *OVF* is delegating management of the whole of Phase I, part 2 *System Specification Development and Documentation*, including the technical components relating to the *Whole Product Solution Specification*, *Technical Specifications and Considerations*, *Build/Buy Recommendation*, and *Testing* chapters of said deliverable to Galois.

3.3 Experts' Roles

The *expert team members* are responsible for making timely and appropriate contributions within their areas of expertise including, but not limited to:

- contributions to dialog via email, hosted discussion forums, and telephone, online, and face-to-face meeting about key decisions in the requirements, architecture, and design of the *election system*,
- contributing to dialog in a similar vein about *demonstrators*,
- the authoring of specific subsections of a draft of the *Final E2E VIV Project Report* (or *project report* for short),
- *potentially* editing drafts of (parts of) the *project report*,
- the authoring of specific subsections of a draft of the *System Specification Development and Documentation* (or *technical report* for short),
- *potentially* providing feedback on, or editing drafts of (parts of) the *technical report*,
- *potentially* contributing research and engineering expertise to the development of supporting *technical artifacts* of the *technical report*,
- *potentially* contributing engineering expertise to the design and development of *demonstrators*,
- contributing to the design and execution of the definition and execution of *usability testing*, particularly from the point-of-view of the *disabled voter*, for the *election system*,
- contributing to the design and execution of the definition and execution of *security validation and verification* for the *election system*, and
- contributing to the design and execution of the definition and execution of *correctness validation and verification* for the *election system*.

It is to be expected that many experts will not have the resources to take a leading role in the authoring of either the *final report*, the *technical report*, or its supporting *artifacts*. Consequently, those aspects of the project are mentioned as *potential*, rather than *mandatory* contributions above.

3.4 Community Interaction and Support

There are several communities relevant to the *E2E VIV Project* outside of those represented on the expert teams. We, the *E2E VIV Project* participants, must expect to have interactions with members of these communities.

Advocates. The most vocal of these communities is that of elections advocates of various stripes. Highly active, high-volume members of this community are members of EVN, and thus will hear about and comment upon this project. We must be prepared to interact with them, both individually and en mass. We must be transparent with them in our process and with our *artifacts*, and we must give them an opportunity to provide structured input on the *E2E VIV Project* at the appropriate time.

Standards Bodies. There are also likely to be interactions with several other parties who are invested in elections, including the EAC, NIST, and existing election systems vendors.

We should transparently communicate and coordinate with the EAC and NIST as they will, in the end, have the authority to permit binding elections and certify election apparatus, including, eventually, remote voting systems. Galois expects to be visiting both organizations in the coming months on matters relating to elections and cryptographic algorithm standardization.

Vendors. Vendors, of course, will claim that their internet voting products are comparable or superior to the *election system* specified by virtue of this project. Moreover, eventually a robust implementation of this *election system* needs to be built, audited, certified, maintained, deployed, and evolved. It is highly likely that existing vendors will want to perform that work. Consequently, vendors are going to be extremely interested in tracking the progress of---and perhaps even influencing the content of---the E2E VIV specification. They are welcome to follow the development of the *E2E VIV Project* and reflect upon its related *artifacts* as any other citizen.

Hackers. The information security community is also very interested in this project. This community has two overlapping sub-communities.

First, white hat hackers, like those that work in universities and with organizations like the CCC, are interested in showing that election systems are flawed and should not be used. As such, members of this community must be included in the project as active project members, and this requirement is satisfied by the current expert team's membership.

Secondly, in the longer term, members of the hacktivist community (e.g., members of *Anonymous*) have shown interest in security problems relating to election systems, both DRMs and remote.

Galois recommends that an active approach must be taken with this second community. The *specification*, *technical artifacts*, and *demonstrators* should be transparently shared with hackers and hacktivists. Moreover, *E2E VIV Project* participants should *actively recruit* members of this community to perform security analyses, code audits, penetration testing, etc.

©2014 Galois, Inc. PUBLIC VERSION.

Election Officials. Outreach to the primary stakeholders responsible for running elections---election officials that are external actors---is critical to the success of this project. Even if all internal actors are in support of the system design, without the support of a broad swath of external election officials, obtaining resources for the next stage in system development and deployment will be at serious risk. As such, communication to, and receiving feedback from, election officials via the NASED [13], NACRC [12], the Election Center [6], and similar organizations is critical to our success.

Citizens. The general public must also be engaged with this project as they are the final arbiter of the subjective trustworthiness of the project, its participants, and the final *election system*.

It is to be determined what the appropriate timing is with regards to widespread promotion of the *E2E VIV Project* and solicitation of feedback on its reports and artifacts. Galois will, with other *E2E VIV Project participants*, contribute to the decision for the timing of such and the mechanism by which such input is collected, though the final decision rests with *OVF project management*.

3.5 Coordination Technologies

Several coordination technologies are appropriate for communication within the E2E VIV project. Undoubtedly, several are in use at the moment, setup and managed by *OVF*. Galois understands that a Redmine instance is in use, for example.

Highlighted below are those technologies that Galois thinks are most relevant for use in a project with this size, visibility, import, and given the range of technical expertise of the expert participants. We especially reflect upon the fact that expert team members are participating voluntarily, thus their time and attention are at a premium.

3.5.1 Mailing Lists

We believe that the primary means by which expert team members communicate is via email. Many experts do not have the interest in interfacing with web-based communication tools like collaborative development environments such as Redmine and wikis.

Consequently, we suggest that an email gateway to all of the other communication mechanisms mentioned below is necessary. An email gateway permits team members to simply send or respond to emails and their contributions are automatically inserted into the CDE.

3.5.2 Google Docs

Google Docs is a reasonable choice for the shared authoring of documents for non-technical experts and for obtaining feedback from non-technical interested parties.

Virtually all of the technical expert team members will be comfortable with using LaTeX, various markup languages, and version control systems. We suggest that the final project

©2014 Galois, Inc. PUBLIC VERSION.

write-up will be written in LaTeX or a markup language that generates attractive, maintainable output.

But because the expert team includes several non-technical members, we need to facilitate the authoring and editing of *non-technical artifacts* using a more approachable means that facilitates interactive collaboration, thus the need for Google Docs or some similar service.

3.5.3 Redmine

Redmine is a *Collaborative Development Environment*, or *CDE* for short. Most CDEs provide several different subsystems to facilitate asynchronous online collaboration, including wikis, ticket trackers, version control systems, mailing lists, web forums, etc. CDEs are a popular and effective means by which to run distributed projects.

Galois's extensive experience with such systems is that: (a) only those subsystems that are actively being used should be enabled and visible, (b) an email gateway to actions in the system is mandatory for enabling expert team member participation, (c) all *artifacts*, both *technical* and *non-technical* should be treated in the same fashion by being stored and tracked within the CDE, and (d) traceability to *artifacts* stored within the CDE must be carefully done so as to not be fragile in the face of evolving URLs, CDE versions, etc.

3.5.4 GitHub

GitHub is the most popular, high-profile CDE in the world today. We highly recommend that the project and all of its *artifacts* are made public and maintained on GitHub at an appropriate point in time.

This recommendation is mainly based upon the social aspects of the community that is interested in the topic of E2E VIV elections and the Open Source community's perspective of transparency and visibility of open projects like this one.

4 Results

The main classes of *artifacts* produced by this project is a *set of reports* and a *set of demonstrators*. Furthermore, *artifacts* are either *non-technical* (thus requiring no specific competencies to understand) or *technical*. Complementing artifact creation is the critical social dimension of *community engagement*. Finally, all results must be *SMART*[1].

[1] Galois contends that all project results should be *SMART*: *Specific*: the determination of whether a result is accomplished is as objective as possible; *Measurable*: major results have a tracking dashboard on the project website and are updated and reviewed weekly; *Attainable*: *E2E VIV Project* participants believe they can achieve the results they propose; *Relevant*: results contribute to the priorities, goals, or on-going; operation of the project, and offer clear value to the project; and *Trackable*: progress toward the achievement of a result is monitored, including project budget. Moreover, each result must have a *customer*. A customer is an individual or group with whom performers, such as Galois, negotiate a result and who will be actively engaged with Galois as a performer. That is, they will really care that the result is achieved and work to make us all successful in doing so.

4.1 Reports

Galois suggests that the *E2E VIV Project Reports*, which are, in the main, but not entirely, *technical artifacts*, have the following properties:

- drafts of reports are public *while under discussion* and *while being authored*, preferably by putting drafts into a public version control system within a tracker (e.g., a *E2E VIV GitHub Organization* or a *OVF GitHub Organization*[2]),
- contents are cross-referenced, and thus traceable to and from, all *specification* aspects (from domain models to behavioral design specifications),
- Copyright is held on each document by the specific authors that contribute that contribute to the document in question, and
- reports are all licensed under a Creative Commons license appropriate for the work.

The *project reports* are a non-technical *Final E2E VIV Project Report* (or *project report* for short) and the *System Specification Development and Documentation* (or *technical report* for short). Galois understand that internal actors and OVF project management desires that drafts of reports are private to participants and only made public when participants deem them ready for public review.

4.2 Technical Artifacts

Several technical artifacts must be created to elucidate the *Whole Product Solution Specification*, particularly its *Technical Specifications and Considerations* chapter, and support the conclusions and process described in the *Testing* chapter.

4.2.1 Domain Model

The foundational *artifact* that must be produced for the *E2E VIV Project* is a domain model of the project. The domain model of the management side of the project is defined informally in this document. Every term defined with a term in *italics* is a concept in this domain model.

A complementary domain model will be formulated for the terminology of *election systems*, particularly those concepts central to *E2E VIV election systems*. The domain model will be expressed in English as part of the *technical report* summarized in the below *Offer of Work* (subsection 5.1), and Galois expects to formalize them as well in an appropriate technology. It is our recommendation that this informal specification is written in BON [21].

The focus of having an informal domain model (effectively, an *E2E VIV Project* glossary) is to ensure that communication within and about the project is clear, concise, traceable, and unambiguous.

[2] A *GitHub Organization* is a structuring concept at GitHub that permits multiple owners and administrators to manage multiple repositories for a business or large open source projects.

The point of formalizing the domain model is to enable a *high-assurance validation and testing methodology*, one of our other offers. Only by having a domain model with a lightweight formal semantics can we ensure that project requirements are sensible and are fulfilled by the *specification*.

4.2.2 Requirements

Requirements for the *project* and *election system* will be written in a standard style using English structured syntax. Project requirements are outlined in the *DF Proposal* and the *PSC* and are specified within this document (see section 4). *Election system* requirements are specified using industry-standard nomenclature for requirements (as used by, e.g,. the IETF) and Galois recommends that they are embedded within a BON system specification (see below) as scenarios.

By having a formal *domain model* and a structured set of *election system requirements* the community has a means by which to not only provide traceable evidence as to the soundness of the arguments behind the technical decisions of the *E2E VIV Project* architecture and design, but Galois can also automatically and manually generate traceable verification artifacts useful for third party validation. These artifacts are directly relevant to the *Testing* section of the final deliverable.

4.2.3 Architecture

The *architecture* of the *election system* describes the high-level architectural style(s) of the system, its subsystems, and their inter-dependencies. Galois recommends specifying the system using BON, as it includes an architecture specification language and is translatable to other architecture specification languages with domain-specific tool support like AADL, SDL, Microsoft's ``layers'', and UML models.

By having a formal architecture specification Galois can more precisely and concisely explain the overall structure of the system, reason about the consistency and clarity of the overall architecture, and the community can check that implementations conform to the architecture and do not experience architecture drift or erosion. This latter capability is important to third party validation and verification.

4.2.4 Technical Design

The *technical design* of the *election system* describes the medium-level types and behavioral properties of the system, its subsystems, and their inter-dependencies. Galois recommends specifying the system using BON, as BON designs are translatable to other design languages such as UML and formal methods like Event-B, Z, and VDM.

Like having a formal architecture specification, by having a formal design specification Galois can reason about the overall consistency and clarity of the design, check that implementations conform to the design, and even automatically generate validation artifacts critical to third party validation and verification.

4.2.5 User Interface Design

The *user interface* (or *UI* for short) of the E2E VIV election system is **the** critical factor in ensuring that the system is both *usable* **and** *secure*. Consequently, a detailed *UI design* that is informed by *usability testing*, facilitated via Galois-funded demonstrators, is a mandatory component of the system specification.

Galois recommends that the E2E VIV election system's UI behavior be specified in a combination of BON and UI mock-ups. Moreover, we recommend that the expert team, working with Galois, prioritize the design and development of UI demonstrators for usability testing. Our thoughts on this are documented in the *Example Demonstrators* document.

Furthermore, Galois believe that usability testing must focus on the dual challenges of: (1) *comprehensibility* and *transparency* of the underlying *mechanisms of verifiability*, and (2) *basic usability* for the disabled (broadly speaking), and disabled voters worldwide are the critical first-order users of the E2E VIV election system. Designing an E2E VIV election system that is *comprehensible* **and** *usable* by the disabled, in which the main challenging populations are the blind and the severely physically disabled, is an open *scientific* **and** *engineering* challenge.

Future Proofing The choice of BON as a specification language is a strategic one. By choosing a programming language-neutral specification language that lacks the baggage of its heavyweight (and, some would say, semantic-less) competitors such as UML one ends up with a smaller, more precise, more useful specification.

Moreover, by starting with firm type and behavioral foundations, translating (fragments of) the BON specification into other specification, reasoning, and implementation languages is a straightforward process. Performing a similar translation from a higher-order language (such as PVS) or a ambiguous language (such as UML) removes any such capability.

Thus, such a specification is ``future proof'' as there is no dependency upon specific versions of complex and expensive tools (in the case of UML) nor is the specification relegated only to the hyper-experts (in the case of PVS or similar).

Finally, and most importantly, non-technical *actors* interested in the *artifacts* produced by the *E2E VIV Project* will be able to efficiently read and understand the specifications the *E2E VIV Project* produces, thereby increasing the trustworthiness and transparency of the project and its outcomes.

4.3 Demonstrators

Demonstrators are *technical artifacts* from the point of view of definition and constructions, but *non-technical artifacts* from the point of view of demonstration. Galois suggests that all *demonstrators* developed using Galois IR&D funding are:

- developed in a *completely transparent* and *public* fashion within the *Galois GitHub Organization*,

- cross-referenced, and thus traceable to and from, all specification aspects (from domain models to behavioral design specifications),
- are replicated into the *E2E VIV GitHub Organization*,
- are licensed under either a mainstream Open Source license with a strong community (e.g., Apache License 2.0, BSD 3-Clause ``New'' or ``Revised'' license, BSD 2-Clause ``Simplified'' or ``FreeBSD'' license, GNU General Public License (GPL), GNU Library or ``Lesser'' General Public License (LGPL), MIT license, Mozilla Public License 2.0, Common Development and Distribution License, Eclipse Public License [15]) or a domain-specific license like the OSET license [16].

4.4 Community Engagement

As discussed in subsection 2.3, Galois must actively engage with the *actors* relevant to the *E2E VIV Project*, both internal and external. All interactions must be transparent, archived, and traceable.

The primary reason for such is to ensure the trustworthiness of the project and its outcomes. The mechanism by which this trust is earned is traceability between discussions as evidence for transparent and objective decision making.

5 Project Specifications

The main goal of this part of the *E2E VIV Project* is the development of a *``whole product solution'' specification* (or simply *specification* for short) for a *trustworthy E2E VIV election system*.[3]

The only *acceptable specification* is one that is:

- **[EXPERTS_SUPPORT]** supported by the vast majority the *experts teams*, including the *technical*, *usability*, *testing*, and *research* teams,
- **[ADVISERS_SUPPORT]** endorsed by the vast majority of the *advisory council*, and
- **[LEO_SUPPORT]** endorsed by the major stakeholders in elections administration as represented by the project's *local election officials*.

Additionally, the *E2E VIV Project* expects to receive support and endorsement from many members of the electronic voting activism community, as represented by key members of the *Election Verification Network* and the *Verified Voting Foundation*.

The *specification* will be of a form with sufficient detail such that the following *requirements* are fulfilled:

[3] Each *requirement* on *Galois project management* or on the outcomes and deliverables of the *E2E VIV Project* are tagged with a *requirements tag* of the form **[TAG_SHORT_NAME]**. Such tag names provide the means by which to cross-reference and provide traceable evidence of the trustworthiness of requirements satisfaction.

- **[INDEPENDENT_IMPLEMENTATION]** The specification must be of sufficient detail and clarity that an implementation of the *election system* must be possible by an independent party without extensive dialog with participants in the project.
- **[INDEPENDENT_VALIDATION]** It must be possible for a moderately proficient IT expert to objectively determine, in a reasonable time frame with reasonable cost, if any *election system* constructed which claims to fulfill the specification.
- **[EVIDENCE_BASED_DECISIONS]** Every decision made in the crafting of the specification must be objectively justifiable and the evidence for the decision must be traceable.

5.1 Offer of Work

The *Galois Offer of Work* for the *E2E VIV Project* is as follows:[4]

- **[FACILITATOR]** *facilitate the communication and decision-making* of the expert teams to drive toward the goals of the project,
- **[MANAGEMENT]** *project management* of matters relating to *election system specification* and *demonstrator* development,
- **[COMMUNICATION]** *help interface with external parties* who are interested in the work of the project and its outcomes,
- **[SPECIFICATION_DELIVERABLE]** have authorship and editorial responsibility for the *Whole Product Solution Specification chapter* of the *System Specification Development and Documentation*,
- **[BUILD_BUY_DELIVERABLE]** have authorship and editorial responsibility for the *Build/Buy Recommendation chapter* for *election system* development within the *System Specification Development and Documentation*,
- **[VALIDATION_DELIVERABLE]** have authorship and editorial responsibility for the *Testing* chapter within the *System Specification Development and Documentation*, and
- **[DELIVERABLE_EXCELLENCE]** ensure that all *project reports* and supporting technical artifacts meet or surpass the definition described in the project *Success Targets* defined in the *Principles and Scope of Cooperation* document.

5.2 Performers

The project lead at Galois is Dr. Joseph Kiniry. Several other performers within Galois have appropriate expertise in matters relevant to E2E VIV election systems (e.g., applied cryptography, distributed systems, HCI for secure systems, high-assurance systems, etc.). They will be pulled onto the project as needed to assist.

[4] Each offer is a requirement on the *E2E VIV Project* as a whole, thus they have requirement tags.

6 Bibliography

References

[1] David Allen. *Getting Things Done: The Art of Stress-Free Productivity*. Penguin Books, 2002.

[2] Josh Beneloh. *Verifiable Secret-Ballot Elections*. PhD thesis, Yale University, 1996.

[3] Available via `http://www.vote.caltech.edu/`.

[4] Available from `http://cryptol.net/`.

[5] Available via `http://www.eac.gov/`.

[6] Available via `https://www.electioncenter.org/`.

[7] Available via `http://www.electionverification.org/`.

[8] Available from `http://research.microsoft.com/en-us/projects/fstar/`.

[9] The RAISE Language Group. *The RAISE Specification Language*. BCS Practitioner Series. Prentice--Hall, Inc., 1992.

[10] Daniel Jackson. *Software Abstractions: Logic, Language, and Analysis*. The MIT Press, 2012.

[11] David Jefferson, Aviel D. Rubin, Barbara Simons, and David Wagner. A security analysis of the secure electronic registration and voting experiment (SERVE), 2004.

[12] Available via `http://www.nacrc.org/`.

[13] Available via `http://www.nased.org/`.

[14] Available via `http://www.nist.gov/itl/vote/`.

[15] Available from `http://www.opensource.org/`.

[16] Available via `http://www.osetfoundation.org/`.

[17] Principles and scope of cooperation (PSC). Written by Overseas Vote Foundation and shared with all consultants associated with the E2E VIV Project.

[18] The PVS specification and verification system. Available via `http://pvs.csl.sri.com`.

[19] Available via `http://www.rockthevote.com/`.

[20] Available via `http://verifiedvoting.org/`.

[21] Kim Waldén and Jean-Marc Nerson. *Seamless Object-Oriented Software Architecture - Analysis and Design of Reliable Systems*. Prentice--Hall, Inc., 1995.